

# Настройте захваты пакета на AireOS WLC

## Содержание

[Введение](#)

[Требования](#)

[Используемые компоненты](#)

[Ограничения](#)

[Настройка](#)

[Включите пакет , входящий в WLC](#)

[Проверка](#)

[Преобразуйте пакетную регистрацию вывода в .pcap файл](#)

[Устранение неполадок](#)

## Введение

Этот документ описывает, как выполнить пакетный дамп на Контроллере беспроводной локальной сети (WLC) AireOS. Этот метод отображает пакеты, переданные и/или полученные на уровне процессоров WLC в шестнадцатеричном формате, который тогда можно быть преобразован в .pcap файл с Wireshark.

Полезно в случаях, где связь между WLC и сервером Сервиса RADIUS, Точка доступа (AP) или другие контроллеры должны быть проверены в быстром способе с захватом пакета на уровне WLC, но промежуток порта трудно выполнить.

## Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Доступ интерфейса командной строки (CLI) к WLC, предпочтительно SSH, так как выходные данные быстрее, чем консоль.
- ПК с установленным Wireshark

## Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- WLC v8.3
- Wireshark v2 или позже

**Примечание:** Эта функция доступна начиная с версии 4 AireOS.

## Ограничения

Пакетная регистрация перехватит только двунаправленный Уровень управления (CP) к

пакетам Плоскости данных (DP) в WLC. Те пакеты, которые не переданы от уровня управления к/ота плоскости Данных WLC (т.е. внешний к туннельному трафику привязки, отбрасываниям CP DP и так далее) не будут перехвачены.

Примеры к/ота типов трафика WLC, обработанный в CP :

- Telnet
- SSH
- HTTP
- HTTPS
- SNMP
- NTP
- RADIUS
- TACACS +
- Сообщения мобильности
- Контроль CAPWAP
- NMSP
- TFTP/FTP/SFTP
- Системный журнал
- IAPP

К/от трафика клиент обработан в Плоскости данных (DP) за исключением: управление 802.11, 802.1X/EAPOL, ARP, DHCP и Web-аутентификация.

## Настройка

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в данном документе, были запущены с конфигурацией по умолчанию. Если ваша сеть является оперативной, гарантируйте понимание потенциального воздействия любой команды.

### Включите пакет , входящий в WLC

Шаг 1. Войдите к CLI WLC.

Из-за количества и скорости журналов, что это отображения характеристик рекомендуется войти к WLC SSH а не консолью.

Шаг 2. Примените Список контроля доступа (ACL) для ограничения, какой трафик перехвачен.

В данном примере перехват показывает к/оту трафика интерфейс управления WLC (IP-адрес 172.16.0.34) и сервер 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
```

**Совет:** Для получения всего к/ота трафика WLC, рекомендуется применить ACL, который сбрасывает от к/ота трафика SSH хост, который инициировал Сеанс SSH. Это

команды, которые можно использовать для построения ACL:

```
>acl ip 1 регистрации debug packet запрещает <IP WLC> <IP - адрес хоста> tcp 22
любой
>acl ip 2 регистрации debug packet запрещает <IP - адрес хоста> <IP WLC> tcp любые
22
>debug packet, регистрирующий acl ip 3, разрешает любому любого
```

Шаг 3. Настройте формат, читаемый Wireshark.

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

Шаг 4. . Включите пакетную характеристику входа в систему.

Данный пример показывает, как перехватить 100 полученных/передаваемых пакетов (он поддерживает 1 - 65535 пакетов):

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

**Примечание:** По умолчанию это только регистрирует 25 полученных пакетов с **logging enable** команды **debug packet**.

**Примечание:** Вместо **все**го можно использовать **rx** или **tx** для получения только полученного или передаваемого трафика.

Для получения дальнейшей информации о настройке пакетной характеристики входа в систему консультируются с этой ссылкой:

[Руководство конфигурации контроллера беспроводной связи Cisco, выпуск 8.3, Использование средства отладки](#)

## Проверка

Воспользуйтесь данным разделом для проверки правильности функционирования вашей конфигурации.

Используйте данную команду для проверки текущей конфигурации пакетной регистрации.

```
> 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
```

Воспроизведите необходимое поведение генерировать трафик.

Появляются выходные данные, подобные этому:

```
> 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

```

## Удалите ACL из пакетной регистрации

Для отключения фильтров, примененных использованием ACL эти команды:

```
> 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
```

## Отключите пакетную регистрацию

Для отключения пакетной регистрации, не удаляя ACL, просто используют эту команду:

```
> 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
```

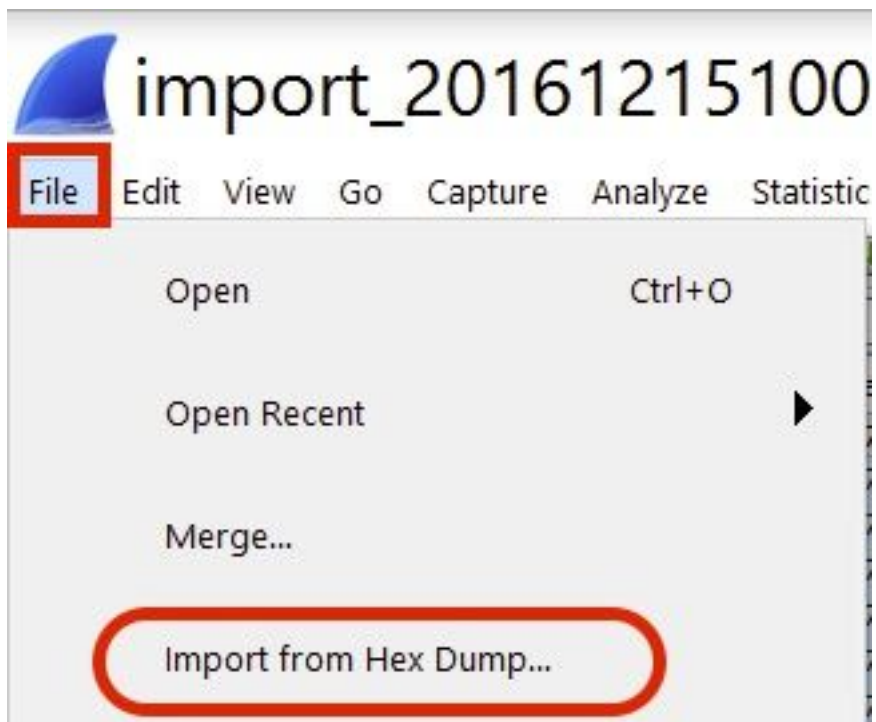
```
[5]: disabled
[6]: disabled
IP ACL:
[1]: permit s=172.16.0.34 d=172.16.56.153 any
[2]: permit s=172.16.56.153 d=172.16.0.34 any
[3]: disabled
[4]: disabled
[5]: disabled
[6]: disabled
EoIP-Ethernet ACL:
[1]: disabled
[2]: disabled
[3]: disabled
[4]: disabled
[5]: disabled
[6]: disabled
EoIP-IP ACL: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

## Преобразуйте пакетную регистрацию вывода в .pcap файл

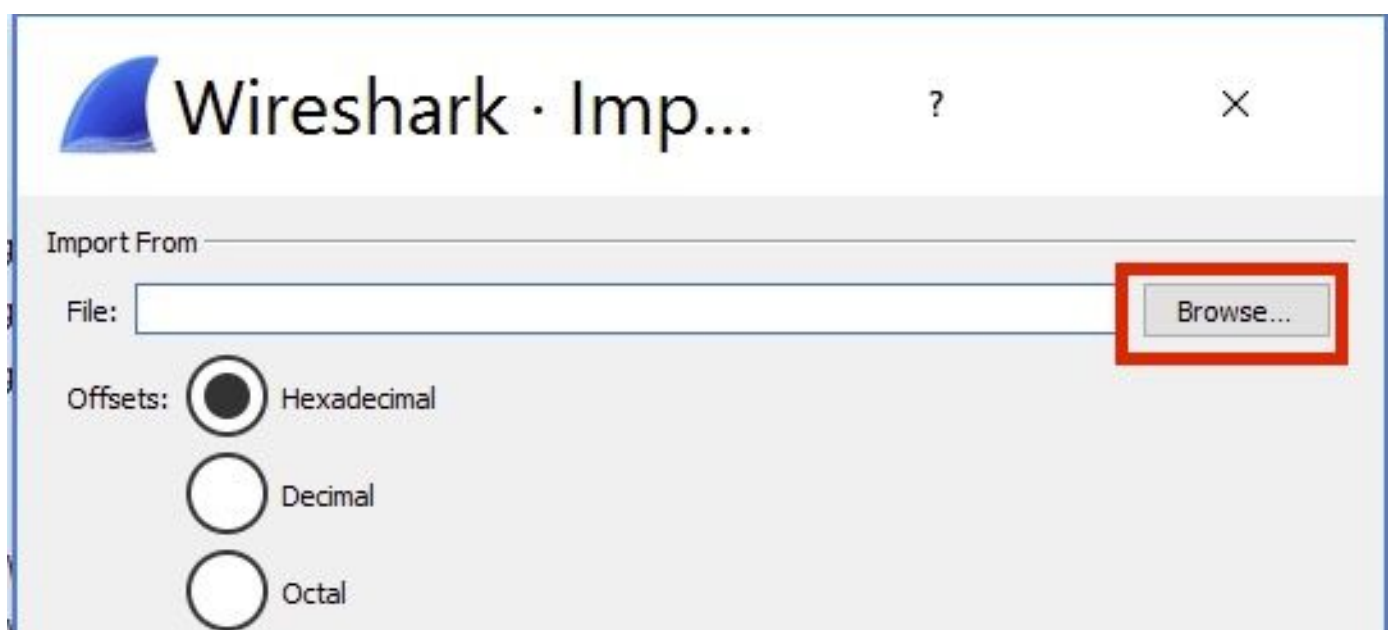
Шаг 1. Как только выходные данные заканчиваются, соберите их и сохраните их к текстовому файлу.

Гарантируйте сбор чистого журнала иначе Wireshark мог бы показать поврежденные пакеты.

Шаг 2. Открытый Wireshark и перешел к **Файлу**> **Импорт от Шестнадцатеричного дампа...**

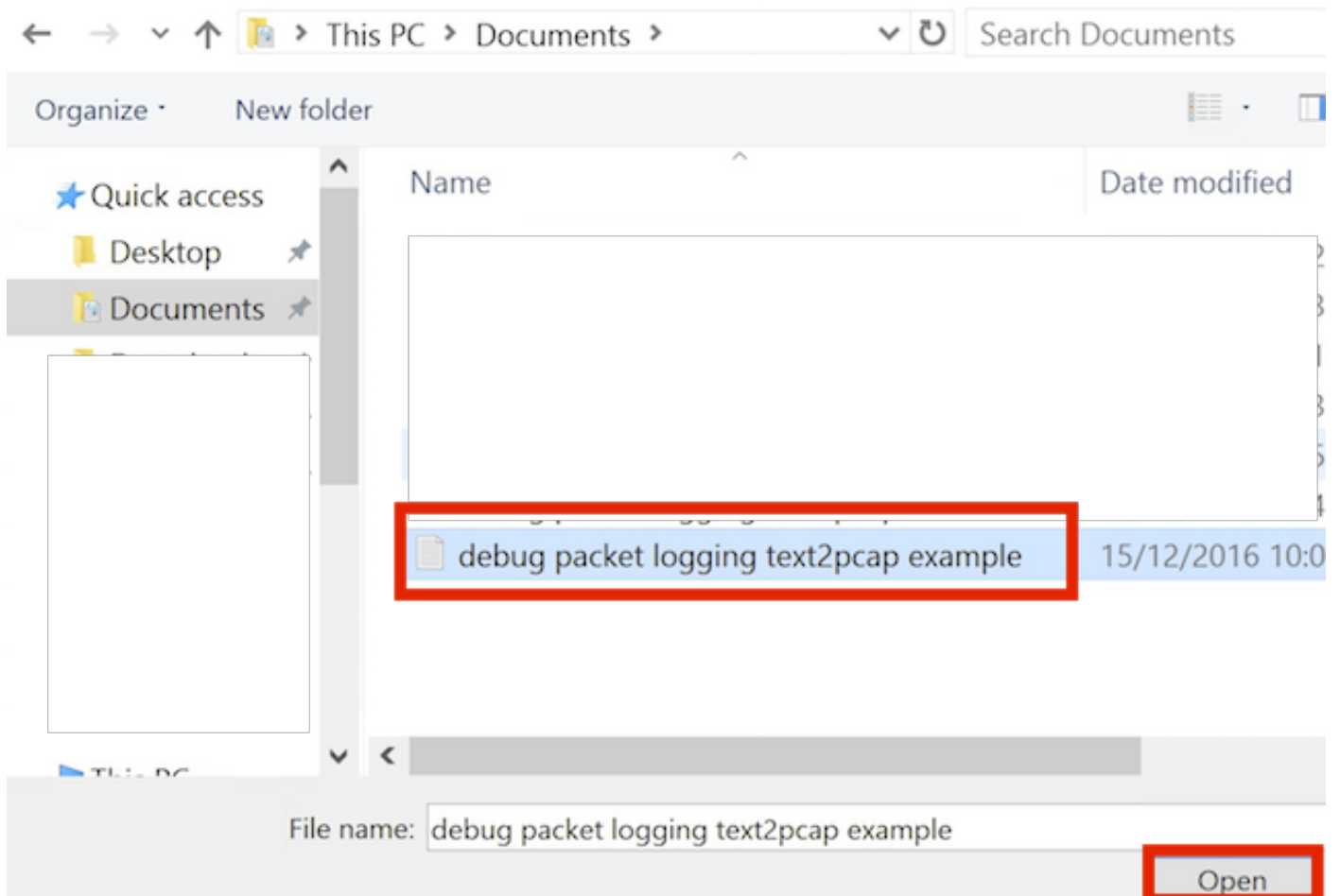


Шаг 3. Нажмите кнопку Browse.

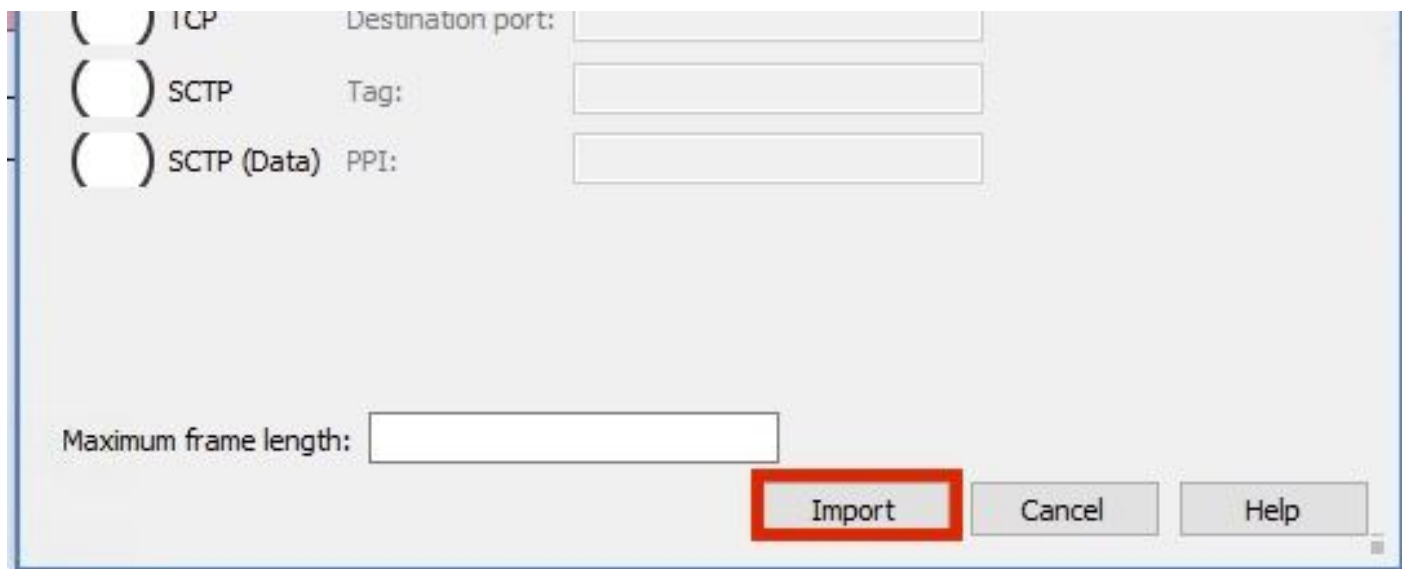


Шаг 4. . Выберите текстовый файл, где вы сохранили пакетную регистрацию вывода.





Шаг 5. . Нажмите кнопку Import (Импортировать).



Wireshark показывает файл как .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) 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
```

**Примечание:** Знайте, что штампы времени не точны, ни временной промежуток между кадрами.

## Устранение неполадок

Для этой конфигурации в настоящее время нет сведений об устранении проблем.

### Дополнительные сведения

- [Пакетный дамп AP](#)
- [Основные принципы сниффинга беспроводных сетей 802.11](#)
- [Cisco Systems – техническая поддержка и документация](#)