

Как получить захват пакета от шлюза VXML для анализа сигнала и голоса

Содержание

[Введение](#)

[Предварительные условия](#)

[Требования](#)

[Используемые компоненты](#)

[Возьмите захват пакета на шлюзе VXML](#)

[Проверка](#)

Введение

Этот документ описывает, как получить захват пакета (pcap) от шлюза VXML для речевого анализа и сигнала.

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Унифицированный клиентский голосовой портал (CVP)
- Речевой расширяемый язык разметки гипертекста (XML) шлюз (GW VXML)
- Программное средство Whire shark

Используемые компоненты

Настоящий документ не имеет жесткой привязки к каким-либо конкретным версиям программного обеспечения и оборудования.

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.

Возьмите захват пакета на шлюзе VXML

Можно заставить pcap проверять сигнализацию и среды от GW VXML Cisco с этой процедурой для интерфейса g0/0. Необходимо поменять интерфейсное имя в команде к соответствующей.

conf t

```
ip traffic profile test mode capture  
bidirectional  
exit
```

```
int g0/0  
ip traffic apply test size 20000000  
end
```

```
traffic int g0/0 clear  
traffic int g0/0 start
```

Трафик получения шлюза VXML, поэтому сделайте тестовый вызов и быстро остановите захват пакета.

```
traffic int g0/0 stop
```

Для копирования рсар к типу сервера TFTP эта команда.

```
traffic int g0/0 copy tftp://x.x.x.x/g00.pcap
```

Для копирования рсар к типу сервера FTP эта команда.

```
traffic int g0/0 copy ftp://username:password@x.x.x.x/g00.pcap
```

Снимок экрана показывает рсар файл port1.pcap, открытый с программным средством Wireshark.

The screenshot shows the Wireshark interface with the following details:

- Filter:** Expression... Clear Apply Save
- Packet List:**

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.251.93.10	10.251.62.208	SSH	92	Encrypted response packet Len=52
2	0.000183	10.251.93.10	10.251.100.50	TACACS+	217	Q: Accounting
3	0.003746	10.251.100.50	10.251.93.10	TACACS+	57	R: Accounting
4	0.107792	10.251.93.10	10.251.100.50	TCP	40	35576 > tacacs [ACK] Seq=1 Ack=1 win=3984 Len=0
5	0.203785	10.251.93.10	10.251.100.50	TCP	40	63840 > tacacs [ACK] Seq=178 Ack=18 win=3785 Len=0
6	0.251243	10.251.62.208	10.251.93.10	TCP	40	58357 > ssh [ACK] Seq=1 Ack=53 win=65288 Len=0
7	1.000105	10.251.93.10	10.251.100.21	Syslog	143	LOCAL7.NOTICE: 48: 058316: Apr 6 20:58:28.410: %RITE-5-CAPTURE_START: Started IP traffic capture for interf
8	1.000125	10.251.93.10	10.251.132.13	Syslog	143	LOCAL7.NOTICE: 48: 058316: Apr 6 20:58:28.410: %RITE-5-CAPTURE_START: Started IP traffic capture for interf
9	5.037823	10.251.93.33	10.251.93.10	SIP	508	Request: OPTIONS sip:10.251.93.10
10	5.038359	10.251.93.10	10.251.93.33	SIP/SDF	1007	Status: 200 OK
11	5.703503	10.251.93.56	10.251.93.255	BROWSEF	229	Host Announcement USQLCAWS1, Workstation, Server, SQL Server, NT workstation, NT Server
12	7.201722	10.250.93.57	10.251.93.10	SIP	1358	Request: INVITE sip:55555222222222221362@10.251.93.10:5060
13	7.203454	10.251.93.10	10.250.93.57	SIP	493	Status: 100 Trying
14	7.203494	10.251.93.10	10.250.93.57	SIP/SDF	1100	Status: 200 OK
15	7.236543	10.250.93.57	10.251.93.10	SIP/SDF	804	Request: ACK sip:55555222222222221362@10.251.93.10:5060
16	7.264140	10.251.93.10	10.250.93.57	TCP	44	63536 > 1rdmi [SYN] Seq=0 Win=4128 Len=0 MSS=536
17	7.265260	10.250.93.57	10.251.93.10	TCP	44	1rdmi > 63536 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
18	7.265297	10.251.93.10	10.250.93.57	TCP	40	63536 > 1rdmi [ACK] Seq=1 Ack=1 Win=4128 Len=0
19	7.265345	10.251.93.10	10.250.93.57	TCP	576	[TCP segment of a reassembled PDU]
- Packet 11 Details:**
 - Frame 1: 92 bytes on wire (736 bits), 92 bytes captured (736 bits)
 - Raw packet data
 - Internet Protocol Version 4, Src: 10.251.93.10 (10.251.93.10), Dst: 10.251.62.208 (10.251.62.208)
 - Transmission Control Protocol, Src Port: ssh (22), Dst Port: 58357 (58357), Seq: 1, Ack: 1, Len: 52
 - SSH Protocol
- Packet 11 Bytes:**

Offset	Hex	ASCII	
0000	45 c0 00 5c 39 58 00 00	ff 06 cf b3 0a fb 5d 0a	E.. \9X..
0010	0a fb 3e d0 00 16 e3 f5	a5 d1 b6 82 9f 4b be dc	..K..
0020	50 18 10 20 5a 49 00 00	74 b5 3d a1 5f 93 f1 69	P.. ZI.. t:.. ..
0030	87 61 14 3f 83 53 05 66	ea 27 3c 64 5e 99 84 92	.a.?..S.f .<d\...
0040	d0 8e 26 75 a3 f0 e1 5e	74 b9 9d 77 55 a8 cd 91	..&u... ^ t:..w...
0050	55 4b 36 71 3e 0c 6b 16	9c c6 40 0c	UK6q>.k. ..@.

Проверка

Чтобы проверить, что захват пакета является допустимым использованием эта процедура.

Шаг 1. Сигнализация sip фильтра.

Введите ключевое слово **sip** в текстовое поле **Filter**.

The screenshot shows the Wireshark interface with a packet capture filter set to 'sip'. The main pane displays a list of captured packets, all of which are SIP messages. The packet list table is as follows:

No.	Time	Source	Destination	Protocol	Length	Info
9	5.037823	10.251.93.33	10.251.93.10	SIP	508	Request: OPTIONS sip:10.251.93.10
10	5.038359	10.251.93.10	10.251.93.33	SIP/SDF	1007	Status: 200 OK
12	7.201722	10.250.93.57	10.251.93.10	SIP	1358	Request: INVITE sip:5555522222222221362@vxmLgw1A.omnicare.com;transport=udp
13	7.203454	10.251.93.10	10.250.93.57	SIP	493	Status: 100 Trying
14	7.203494	10.251.93.10	10.250.93.57	SIP/SDF	1100	Status: 200 OK
15	7.236543	10.250.93.57	10.251.93.10	SIP/SDF	804	Request: ACK sip:5555522222222221362@10.251.93.10:5060
436	10.045310	10.251.93.33	10.251.93.10	SIP	508	Request: OPTIONS sip:10.251.93.10
437	10.045836	10.251.93.10	10.251.93.33	SIP/SDF	1007	Status: 200 OK
711	11.870965	10.250.93.57	10.251.93.10	SIP	498	Request: BYE sip:5555522222222221362@10.251.93.10:5060
714	11.872078	10.251.93.10	10.250.93.57	SIP	561	Status: 200 OK
732	15.053366	10.251.93.33	10.251.93.10	SIP	508	Request: OPTIONS sip:10.251.93.10
733	15.053737	10.251.93.10	10.251.93.33	SIP/SDF	1008	Status: 200 OK
734	20.123097	10.251.93.33	10.251.93.10	SIP	508	Request: OPTIONS sip:10.251.93.10
735	20.123454	10.251.93.10	10.251.93.33	SIP/SDF	1008	Status: 200 OK
736	25.130902	10.251.93.33	10.251.93.10	SIP	508	Request: OPTIONS sip:10.251.93.10
737	25.131482	10.251.93.10	10.251.93.33	SIP/SDF	1007	Status: 200 OK
738	27.719707	10.251.93.57	10.251.93.10	SIP/SDF	1284	Request: INVITE sip:5555522222222221363@vxmLgw1A.omnicare.com;transport=udp
739	27.721307	10.251.93.10	10.251.93.57	SIP	481	Status: 100 Trying
740	27.721345	10.251.93.10	10.251.93.57	SIP/SDF	1022	Status: 200 OK
775	27.874125	10.251.93.57	10.251.93.10	SIP	488	Request: ACK sip:5555522222222221363@10.251.93.10:5060
1010	30.200873	10.251.93.33	10.251.93.10	SIP	508	Request: OPTIONS sip:10.251.93.10
1011	30.201266	10.251.93.10	10.251.93.33	SIP/SDF	1006	Status: 200 OK
1513	35.208687	10.251.93.33	10.251.93.10	SIP	508	Request: OPTIONS sip:10.251.93.10
1514	35.209051	10.251.93.10	10.251.93.33	SIP/SDF	1008	Status: 200 OK
1690	26.078672	10.251.02.57	10.251.02.10	SIP	400	Request: BYE sip:5555522222222221362@10.251.02.10:5060

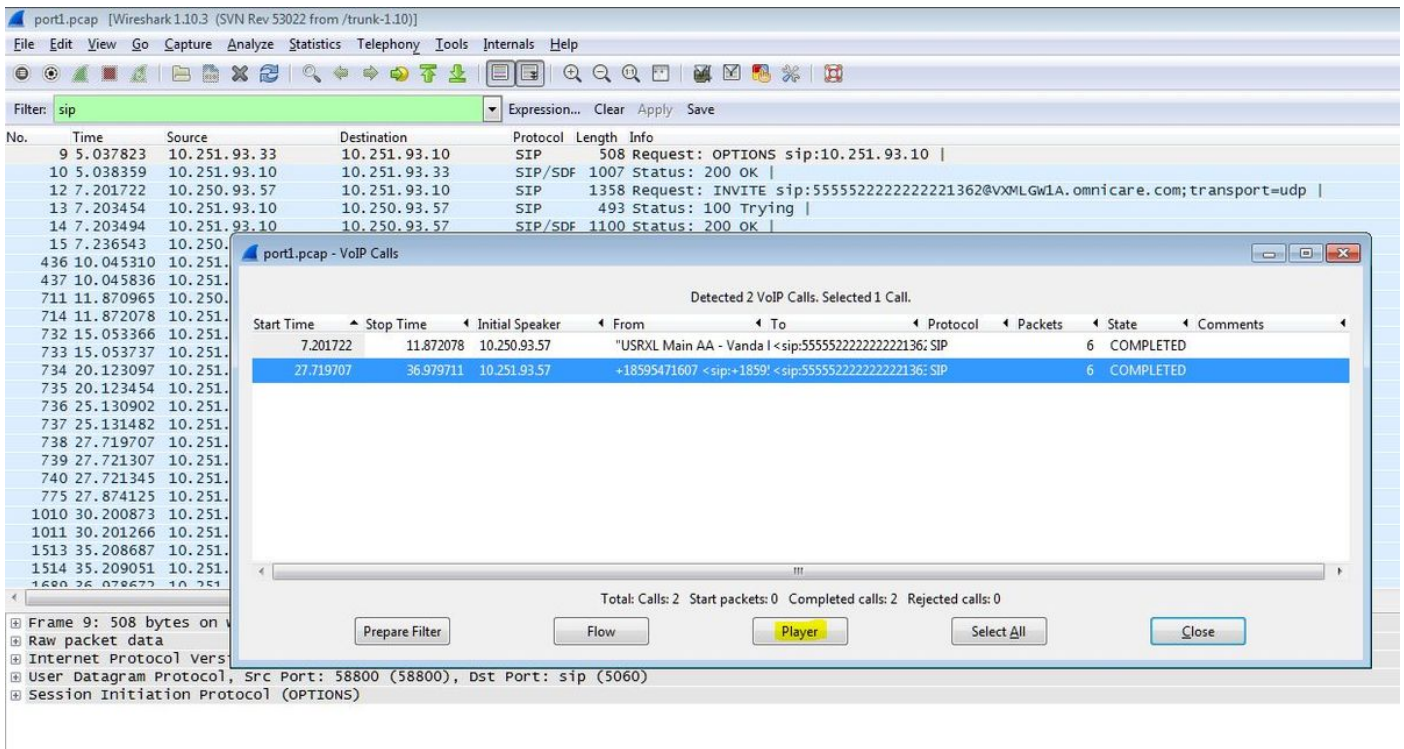
The packet details pane for Frame 9 shows the following structure:

- Frame 9: 508 bytes on wire (4064 bits), 508 bytes captured (4064 bits)
- Raw packet data
- Internet Protocol Version 4, Src: 10.251.93.33 (10.251.93.33), Dst: 10.251.93.10 (10.251.93.10)
- User Datagram Protocol, Src Port: 58800 (58800), Dst Port: sip (5060)
- Session Initiation Protocol (OPTIONS)

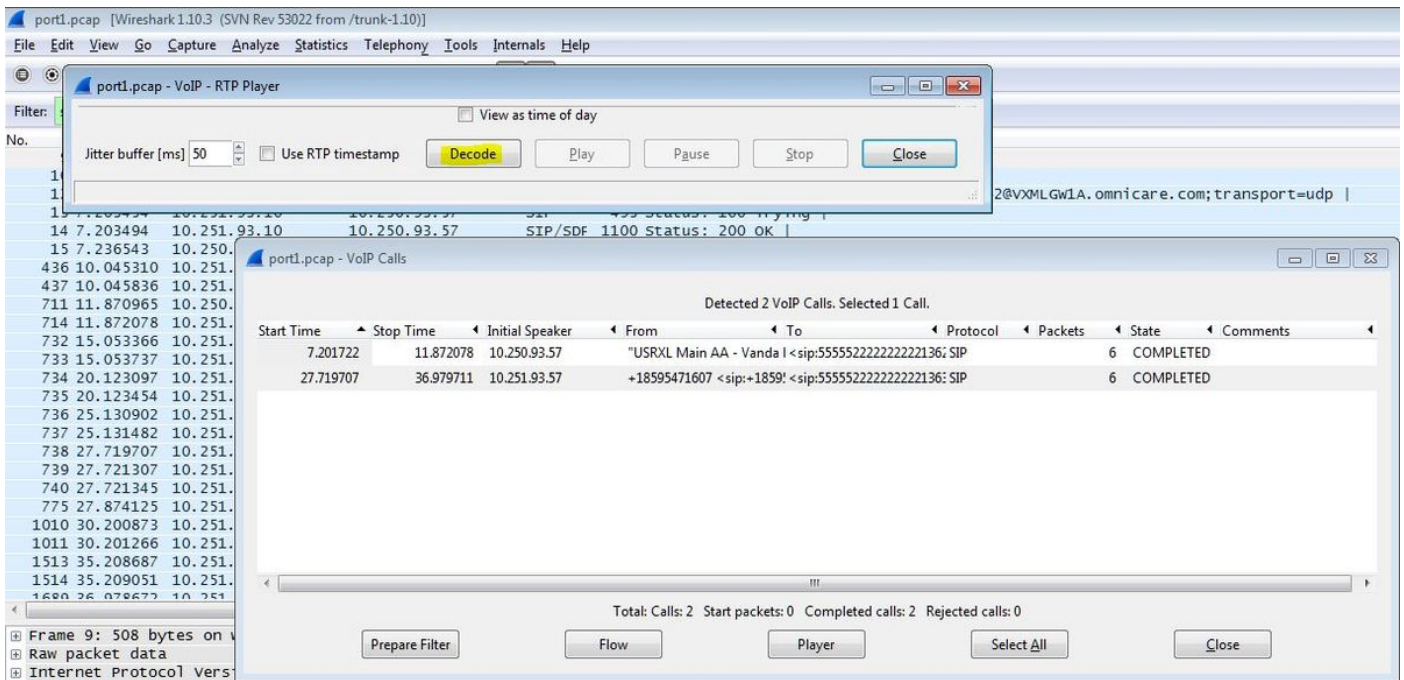
The packet bytes pane shows the raw hex and ASCII data for the captured packet.

Шаг 2. Откройте потоки RTP с Проигрывателем Wireshark.

- Перейдите к **телефонии - вызовы VoIP**
- Выберите рассматриваемый вызов
- Выберите **Player**

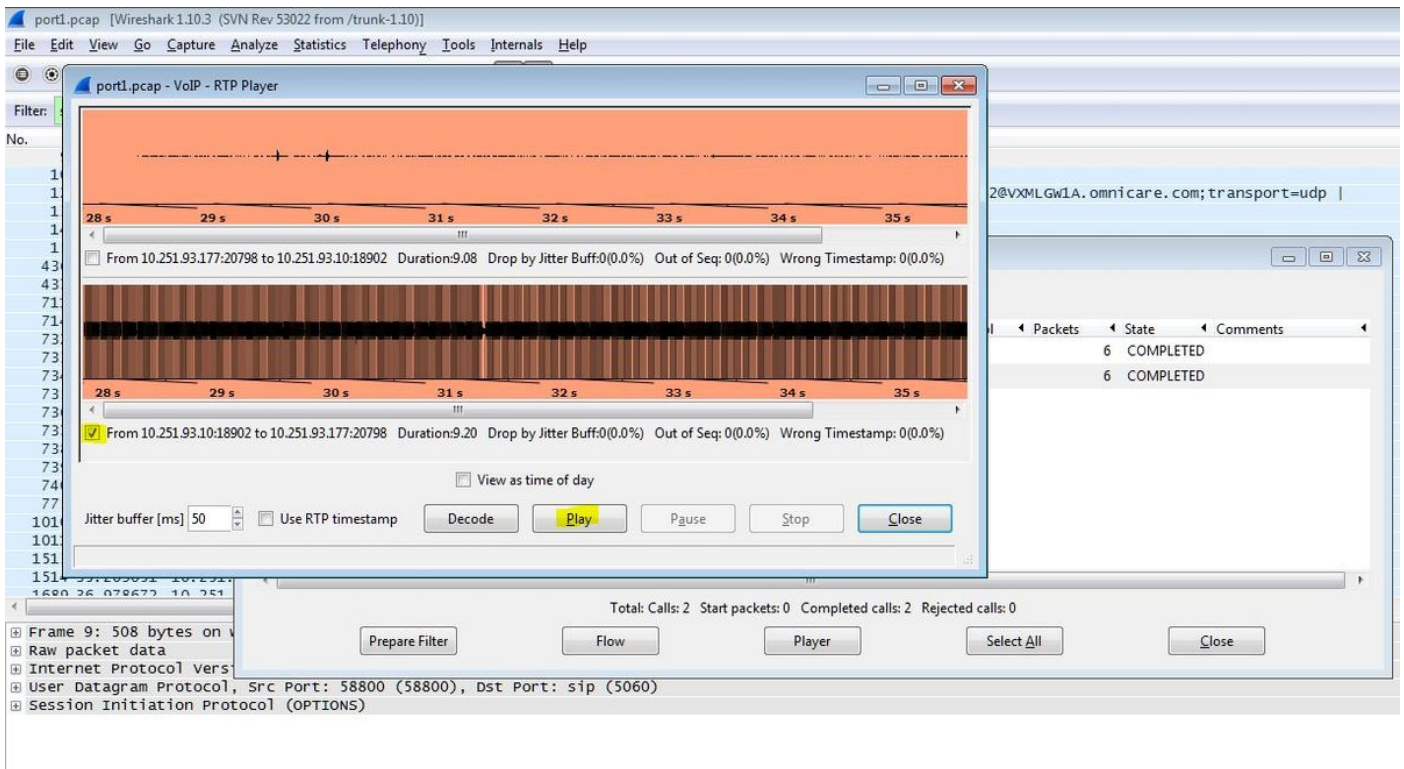


Шаг 3. Нажмите Decode.



Шаг 4. . Воспроизведите запись.

Для воспроизведения зарегистрированного диалога, выбирают декодируемый график для рассматриваемого вызова и выбирают **Play**.



Описанная процедура может использоваться для решения проблем с качеством звука, односторонней передачей аудиоданных или условиями тишины в эфире.

Эти команды отладки могут быть введены на шлюзе VXML для дополнительного диагноза.

```

debug ccsip mess
debug ccsip error
debug voip ccapi inout
debug voip dialpeer inout
debug http client all
debug voip application script
debug voip application vxml
debug voip rtp session named-events
debug voip rtp sess nse
debug voip rtp

```