

# Comment obtenir la capture de paquets à partir de la passerelle VXML pour l'analyse de signaux et de voix

## Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Capture de paquets sur la passerelle VXML](#)

[Vérification](#)

## Introduction

Ce document décrit comment obtenir une capture de paquets (pcap) à partir d'une passerelle VXML pour l'analyse du signal et de la voix.

## Conditions préalables

### Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Unified Customer Voice Portal (CVP)
- Passerelle VXML GW (Voice Extensible Markup Language Gateway)
- Outil Whire shark

### Components Used

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

## Capture de paquets sur la passerelle VXML

Vous pouvez obtenir un pcap pour vérifier la signalisation et le support à partir de Cisco VXML GW avec cette procédure pour l'interface **g0/0**. Vous devez remplacer le nom de l'interface dans la commande par le nom approprié.

```

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

```

La passerelle VXML capture le trafic. Effectuez donc un appel de test et arrêtez rapidement la capture de paquets.

```

traffic int g0/0 stop

```

Afin de copier le pcap sur un serveur TFTP, tapez cette commande.

```

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

```

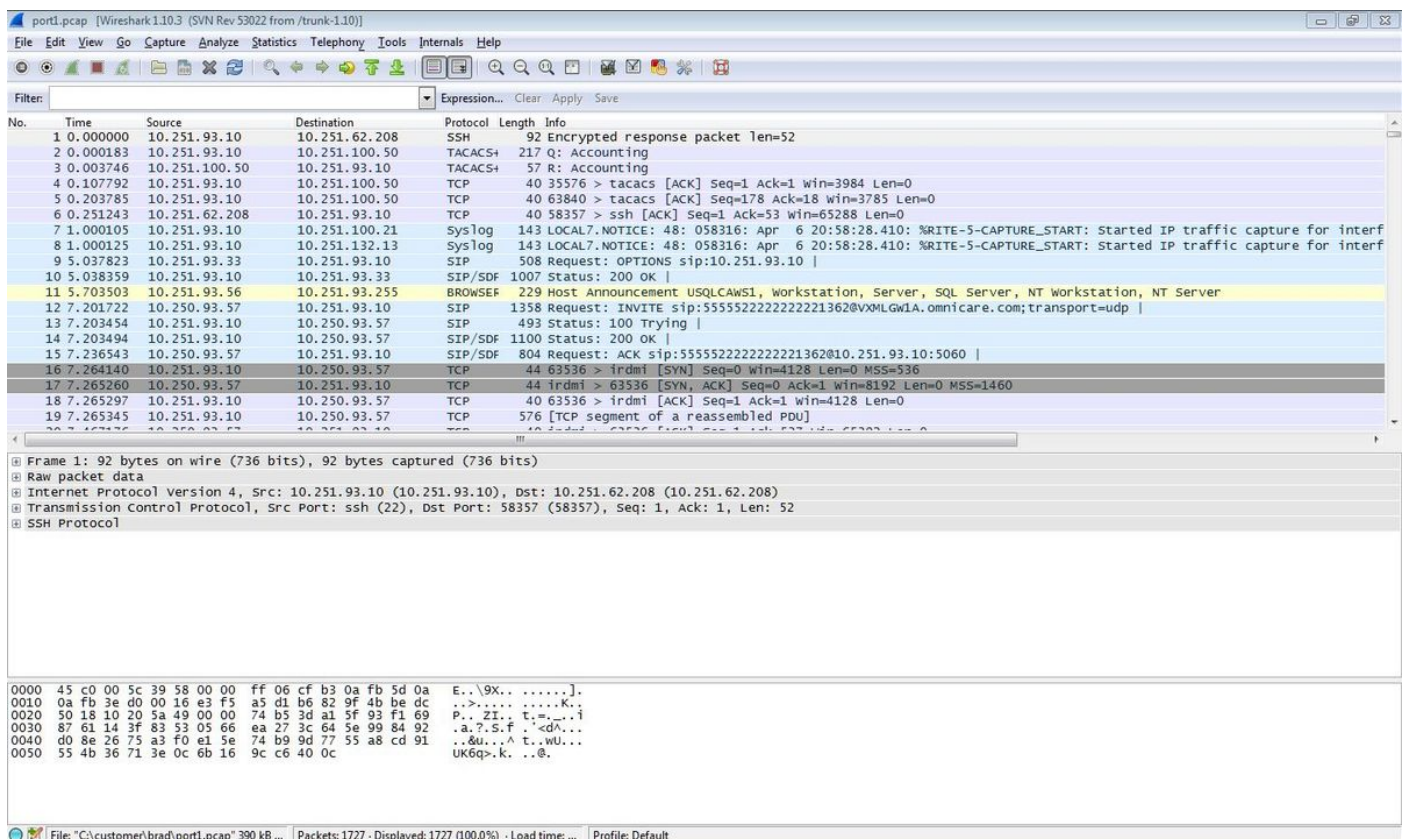
Afin de copier pcap sur un serveur FTP, tapez cette commande.

```

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

```

La capture d'écran montre le fichier pcap **port1.pcap** ouvert avec l'outil Wireshark.



## Vérification

Afin de vérifier que la capture de paquets est valide, utilisez cette procédure.

## Étape 1. Filtrer la signalisation SIP.

Entrez le mot clé **sip** dans la zone de texte **Filter**.

The screenshot shows the Wireshark interface with the filter 'sip' applied. The packet list pane shows the following data:

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:555552222222221362@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:555552222222221362@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:555552222222221362@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:555552222222221363@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:555552222222221363@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	26.078673	10.251.02.57	10.251.02.10	STP	400	Request: BYE sip:555552222222221362@10.251.02.10:5060

The packet bytes pane shows the raw data for the selected packet:

```
0000 45 00 01 fc 77 29 00 00 7f 11 f2 a6 0a fb 5d 21 E..w)...!
0010 0a fb 5d 0a e5 b0 13 c4 01 e8 d5 49 4f 50 54 49 ..].....TOPTI
0020 4f 4e 53 20 73 69 70 3a 31 30 2e 32 35 31 2e 39 0N5 sip: 10.251.9
0030 33 2e 31 30 20 53 49 50 2f 32 2e 30 0d 0a 56 69 3.10 SIP /2.0.vi
0040 61 3a 20 53 49 50 2f 32 2e 30 2f 55 44 50 20 31 a: SIP/2 .0/UDP 1
0050 30 2e 32 35 31 2e 39 33 2e 33 3a 35 38 38 30 0.251.93 .33:5880
0060 30 3b 62 72 61 6e 63 68 3d 7a 39 68 47 34 62 4b 0;branch =z9hg4bk
0070 2d 64 38 37 35 34 7a 2d 63 62 37 38 64 61 31 39 -d8754z- cb78da19
0080 35 63 36 31 62 39 30 66 2d 31 2d 2d 2d 64 38 37 5c61b90f -1---d87
0090 35 34 7a 2d 3b 72 70 6f 72 74 0d 0a 4d 61 78 2d 54z;irpo rt,,Max-
00a0 46 6f 72 77 63 72 64 73 3a 20 37 30 0a 43 6f Forward: 70..co
```

## Étape 2. Ouvrez les flux RTP avec Wireshark Player.

- Accédez à **Téléphonie - Appels IP**
- Choisir l'appel en question
- Sélectionner un **lecteur**

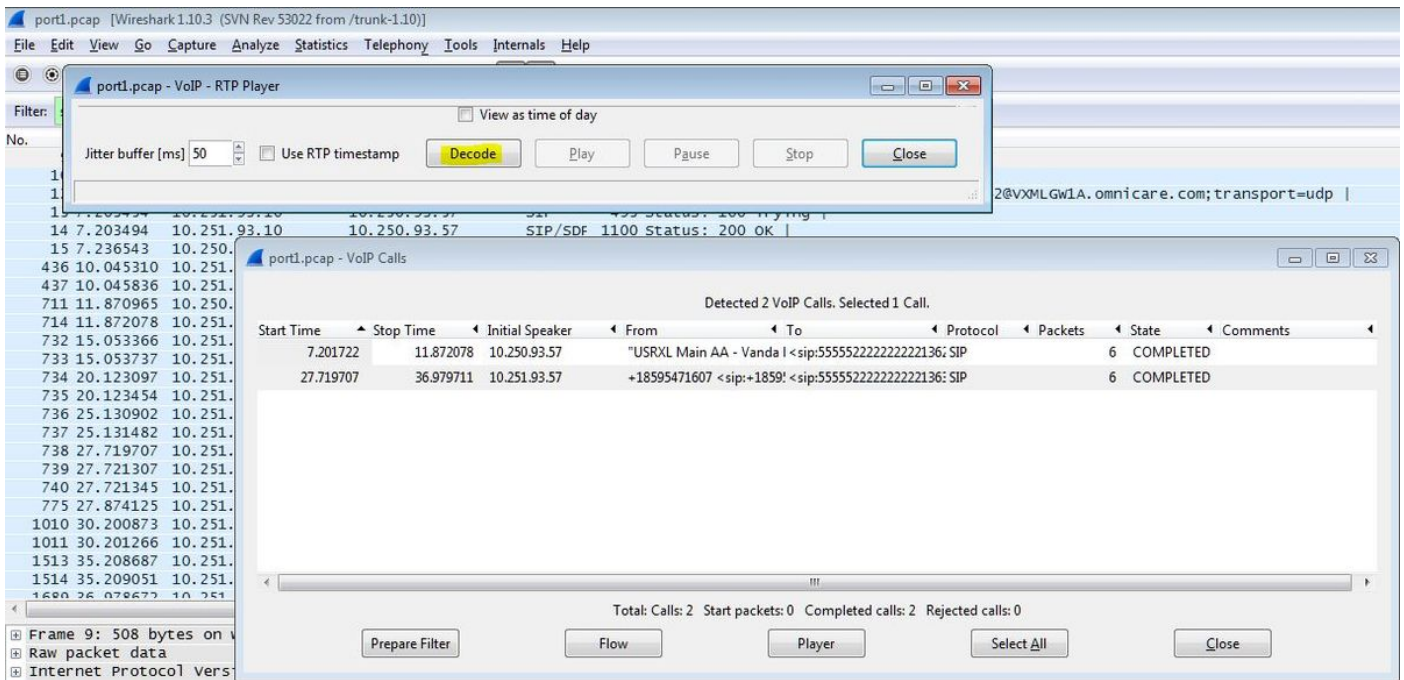
The screenshot shows the Wireshark interface with the filter 'sip' applied. A dialog box titled 'port1.pcap - VoIP Calls' is open, displaying a table of detected VoIP calls:

Start Time	Stop Time	Initial Speaker	From	To	Protocol	Packets	State	Comments
7.201722	11.872078	10.250.93.57	"USRXL Main AA - Vanda I	<sip:55555222222222136; SIP	SIP	6	COMPLETED	
27.719707	36.979711	10.251.93.57	+18595471607 <sip:+1859!	<sip:55555222222222136; SIP	SIP	6	COMPLETED	

The dialog box also shows a summary: Total Calls: 2, Start packets: 0, Completed calls: 2, Rejected calls: 0. The 'Player' button is highlighted.

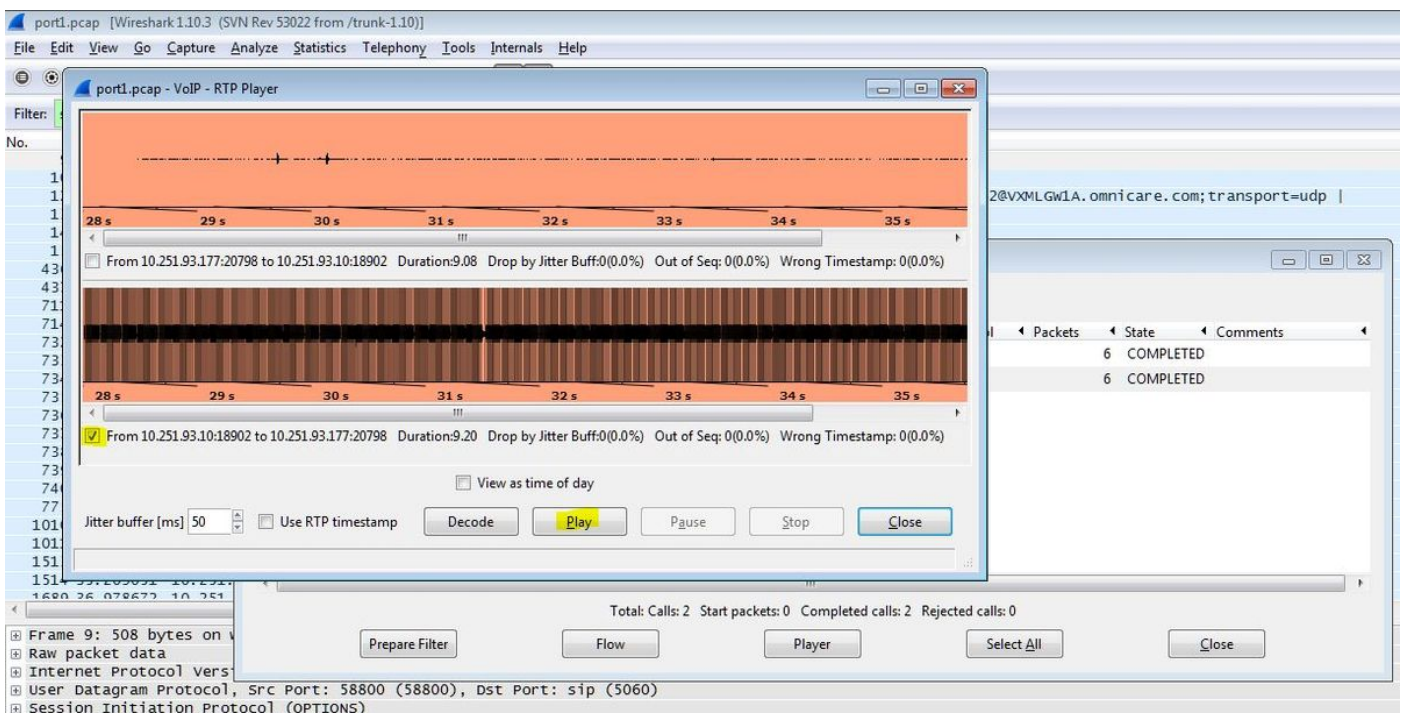
## Étape 3. Cliquez sur **Décodeur**.





Étape 4. Lecture de l'enregistrement.

Afin de lire la conversation enregistrée, sélectionnez le graphique décodé pour l'appel en question et sélectionnez Lire.



La procédure décrite peut être utilisée pour résoudre les problèmes de qualité audio, de qualité audio unidirectionnelle ou d'état d'air mort.

Ces commandes de débogage peuvent être tapées sur la passerelle VXML pour un diagnostic supplémentaire.

```
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
```