### **VoIP Troubleshooting**

Troubleshooting steps for VoIP logger recording through port mirroring, focusing on SIP, H.323, Cisco Skinny, and RAW RTP modes.

#### **Verify Network Configuration:**

- Ensure that the VoIP logger is connected to the appropriate network segment or VLAN.
- Confirm that the port mirroring configuration includes all necessary ports for VoIP traffic.
- Validate that the network infrastructure supports the required protocols and codecs for VoIP communication.

#### **Check Port Mirroring Configuration:**

Double-check the port mirroring configuration on the network switch/router to ensure it is set up correctly.

- Verify that the port mirroring session is configured to capture both incoming and outgoing traffic for the relevant VoIP protocols.
- Confirm that the port mirror destination is correctly set to forward the mirrored traffic to the VoIP logger.

#### **Confirm Connectivity:**

- Validate the connectivity between the VoIP logger and the port mirror destination by performing a ping test or using other network diagnostic tools.
- Ensure that there are no network devices, such as firewalls or security appliances, blocking the traffic between the port mirror destination and the VoIP logger.

#### **Capture Wireshark Logs:**

- Start a Wireshark capture on the interface connected to the VoIP logger.
- Apply appropriate filters to capture only the necessary VoIP traffic based on the protocols (SIP, H.323, Cisco Skinny, RAW RTP).

# **MULTI-MEDIA LOGGING SYSTEMS**



- Go to windows search and type Wireshark, open the app and you will see the following screenshot,
- Go to capture->options and select the nic interface and click start.

<ctrl-></ctrl->	4 ↔ ∞ ≌ ⊉ ₫ 📮 📕	ବ୍ବ୍କ୍⊞								
a w	Vireshark - Capture Options							×		
Inpa	put Output Options									
Int	nterface Traffic	Link-laver Header	Promiscuous	Snaplen (B)	Buffer (MB)	Monitor Mode	Capture Filter			
~	Ethernet mm. Man	C Ethernet		default	2	_				
	Addresses: fe80::f3f0:762c:5526:ae USRP.can1	1, 192.168.1.46	_	_	_	_				
	USBPcap2	USBPcap	_	_	_	_				
	Enable promiscuous mode on all interfaces	3					Manag	ge Interfaces		
Cap	Enable promiscuous mode on all interfaces	ter a capture filter					Manag	compile BPF's		• All interf
Cap	Enable promiscuous mode on all interfaces phure filter for selected interfaces:	ter a capture filter				Star	Manag v Close	pe Interfaces Compile BPFs Help		• ] All interf
Cop	Enable promiscuous mode on al interfaces plure fiter for selected interfaces:	ter a capture filter				→ star	Manag * Close	compile BPFs Help		• Al interf
Cap	Enable promisionus mode on all interfaces plure filter for selected interfaces: () [] [] net: asatt spcap d'you have topcap installed or	s Iter a capture filter				> Star	Manag • Close	pe Interfaces Compile BPFs Help		*) Al interf
Cap	Enable provisionus mode on all interfaces opure filter for selected interfaces: net essats speap if you have topogo installed or net essats spf	tter a capture filter				>Star	Manag • Close	pe Interfaces Comple SPFs Help		• Almer
Cap	Enable promisionus mode on all interfaces phure filter for solected interfaces: net starts reprap if you have hipping installed or net start rep? if you have hipping installed. Both	s ter a capture filter	n as Administrator.				Manag	pe Interfaces Comple BPFs Help		*) Al vierf
Cap	Enable promissionus mode on all interfaces plure filter for selected interfaces: from have bocco installed or net start spc from have bocco installed or net start spc from have workcop installed. Both Doch toknic menseour accord	a ter a capture filter n commands must be ru	n as Administrator.			> Star	Manag	pe Interfaces) Comple BPPs Help		*) Aleard

Set the capture buffer size to accommodate the expected duration of the troubleshooting session.

Voip Filters used in Wireshark IP address : ip.addr == x.x.x.x MAC addres: eth.addr == x:x:x:x SIP: sip, sip.Method == INVITE etc., Cisco Skinny: skinny h.323: h323, h225 RTP: rtp

#### Analyze the Captured Logs:

Check for SIP error codes (4xx, 5xx, etc.) indicating failures in the call setup or registration process.

Examine SIP headers for incorrect or missing information, such as the "Contact," "From," "To," "Call-ID," and "Via" headers.

## **MULTI-MEDIA LOGGING SYSTEMS**



Verify that the SIP messages comply with the relevant RFC specifications. Pay attention to SIP authentication issues, such as incorrect usernames, passwords, or authentication methods.

Examine the SIP 200/OK response packet does have the SDP information encapsulate on it. Check the following screenshots to verify in Wiresharks about the call flows SIP 200 Ok without SDP packet in response to sip invite:

Cao AFF 072221.ocaona											
File	Edit View Go	Capture Analyze Statistics Teleph	onv Wireless Tools Hels								
<u> </u>											
	frame.number in {3405.3	H10 3417 3487 3498 3499 3500 3508 3520 3	521 3523 6513 6519 6530 6538 6	542 6545 3525 :	1906) or rtp.setup-frame in (3405 3410 3417 3487 3498 3499 3500 3508 3520 3521 3523 6513 6519 6530 6538 6542 6545 3525 3506)			×I → I	-1+		
No.	Time	Source	Destination	Protocol	Length Info				<u> </u>		
	3405 2021-07-23	00:06:16.872510 10.65.202.10	10,65,200,106	SIP	1835 Request: INVITE sip:523a89e0-30da-4603-9baf-3058f10c8dfb010.65.200.106:51673:transport=tcp						
	3410 2021-07-23	00:06:16.875621 10.65.200.106	10.65.202.10	SIP	1065 Status: 100 Trying						
	3417 2021-07-23	00:06:16.901841 10.65.200.106	10.65.202.10	SIP	1169 (TCP Spurious Retransmission) Status: 180 Ringing						
	3498 2021-07-23	00:06:19.053433 10.65.202.10	10.65.200.106		767 [TCP Spurious Retransmission] Request: ACK sip:523a89e0-30da-4603-9baf-3058f10c8dfb@10.65.200.106:51673;transport=tcp						
	3499 2021-07-23	00:06:19.053433 10.65.202.10	10.65.200.106	SIP	941 [TCP Spurious Retransmission] Request: UPDATE sip:523a89e0-30da-4603-9baf-3058f10c8dfb@10.65.200.106:51673;transport=tcp						
	3500 2021-07-23	00:06:19.053433 10.65.202.10	10.65.200.106	SIP	1097 Request: SUBSCRIBE sip:523a59e0-30da-4603-9baf-3055f10c8dfb@10.65.200.106:51673;transport=tcp, in-dialog						
	3506 2021-07-25	00:05:19.055783 10.65.202.41	10.65.200.105	RTP	214 PT=TU=T 6.711 PC/NU, SSRC=8x2189CA29, Seq=3334, T1me=2132842477						
	3508 2021-07-23	00:05:19.068395 10.65.200.105	10.65.202.10	SIP	//4 Status: 200 UK						
	3512 2021-07-23	00:00:19.093502 10.05.202.41	10.65.200.100	RIP	214 PT=110-T G./11 PCML, SSNCHWSZ109CA29, S64=3335, 11H==213204230/ 214 DT=111 T G./11 PCML SCHC=210PCA29, S64=3335, 11H==2132042302						
	3514 2021-07-23	00:00:19.104495 10.03.202.41	10.05.200.100	BTD	214 FI-110-10 G/11 FUN, 53K-042105442, 54(=535) 100-21204277						
	3516 2021-07-23	00-05-10 143212 10 65 202 41	10.65.200.105	RTP	214 PT-10-TO TOTAL POWL SCH-MANDARD, SUC-SST, LAMPALADARDY7 214 PT-101LT 6 71 DYML SCH-MANDARD 20 Son-2333 Time-23304317						
	3517 2021-07-23	00:00:19:145212 10:05:202.41	10.65.200.105	RTP	214 0T=THLT 6.711 07ML 500-0021007A29, Seq-3330, Time-213004377						
	3518 2021-07-23	00:06:19,185424 10,65,202,41	10,65,200,106	RTP	214 PT=ITU-T 6.711 PCMU, SSRC=0x2189CA29, Sec=3340, Tim==2132043437						
1	3520 2021-07-23	00:06:19,185810 10,65,200,106	10.65.202.10	SIP	710 [TCP Spurious Retransmission] Status: 200 OK						
	3521 2021-07-23	00:06:19.191171 10.65.200.106	10.65.202.10	SIP	845 Request: NOTIFY sip:10.65.202.10:5060;transport=tcp						
	3523 2021-07-23	00:06:19.192302 10.65.202.10	10.65.200.106	SIP	436 Status: 200 OK						
	3524 2021-07-23	00:06:19.206514 10.65.202.41	10.65.200.106	RTP	214 PT=ITU-T 6.711 PCMU, SSRC=0x2189CA29, Seq=3341, Time=2132043597						
	3525 2021-07-23	00:06:19.206513 10.65.200.106	10.65.202.41	RTP	214 PT=ITU-T 6.711 PCMU, SSRC=0xFC88223A, Seq=52336, Time=4086062137, Mark						
	3527 2021-07-23	00:06:19.226554 10.65.200.106	10.65.202.41	RTP	214 PT=ITU-T G.711 PCMU, SSRC=0xFCB8223A, Seq=52337, Time=4086062297						
	3528 2021-07-23	00:06:19.226568 10.65.202.41	10.65.200.106	RTP	214 PT-ITU-T 6.711 PCMU, SSRC-0x2189CA29, Seq-3342, Time-2132043757						
	3529 2021-07-23	00:06:19.245434 10.65.202.41	10.65.200.106	RTP	214 PT-ITU-T G.711 PCMU, SSRC-0x2189CA29, Seq=3343, Time=2132043917						
<								>	_		
> 1	Frame 3405: 1035	bytes on wire (8280 bits), 1035	bytes captured (8280 b	its) on int	rface \Device\NPF_(DC963E1B-EDFA-49CE-A1D9-093D481F11EC), id 0						
> 1	Ethernet II, Src:	Cisco_c2:73:c1 (00:1b:54:c2:73	:c1), Dst: Cisco_ca:8f:	c7 (d4:ad:b	d:ca:8f:c7)						
>	Internet Protocol	Version 4, Src: 10.65.202.10, 1	Dst: 10.65.200.106								
>	Transmission Cont	rol Protocol, Src Port: 5060, D	st Port: 51673, Seq: 50	17, Ack: 51	66, Len: 969						
>	Session Initiatio	n Protocol (INVITE)									
0.00	a she he he	6 -7 00 1h 64 -7 72 -1 00 00 40	E 00						-		
000	0 04 ad 00 ca a	F C7 00 1D 54 C2 75 C1 00 00 43	a 41								
003	0 c8 6a 13 c4 c	9 d9 1d a5 6d cf b7 9a aa ef 86	0 18 j m								
003	0 02 a4 48 2e 0	0 00 01 01 08 0a b0 89 35 e8 11	2 72 H 5	r							
004	0 f1 f7 49 4e 5	5 49 54 45 20 73 69 70 3a 35 3	2 33 ··INVITE sip:52	3							
005	61 38 39 65 3	a za 33 30 64 61 2d 34 36 30 33	3 2d a89e0-30 da-4603								
007	62 40 31 30 2	e 36 35 2e 32 30 30 2e 31 30 36	5 3a b@10.65, 200.106								
1.000											

SIP 200 OK packet with SDP in response to SIP invite:

REVCORI





File	Edit	View	Go	Capture	Analyze	Statistics	Telephony	Wireless	Tools	Help
1		۲	61.0	🗙 🖸	۹ 👄 🔿	🖻 😨	<b>≹ ⊒</b> ≡	ଭ୍ର୍	a, 🎹	

	frame.number in (14128 14154 14171 26945 26956 14189 14159) or rtp.setup-frame in (14128 14154 14171 26945 26956 14189 14159)												
No	. Time	Source	Destination	Protocol	Length Info								
	14128 2023-01-04	22:11:04.175078 10.8.36.10	10.8.36.66	SIP/SDP	838 Request: INVITE sip:1331@10.8.36.66:5060   (application/x-necsipext2mlv1)								
Т	14154 2023-01-04	22:11:04.338338 10.8.36.66	10.8.36.10	SIP/SDP	616 Status: 200 OK								
	14159 2023-01-04	22:11:04.366376 10.8.36.11	10.8.36.66	RTP	214 PT=ITU-T G.711 PCMU, SSRC=0x3D68BDD1, Seq=17901, Time=401486150								
	14160 2023-01-04	22:11:04.366910 10.8.36.66	10.8.36.11	ICMP	242 Destination unreachable (Port unreachable)								
	14164 2023-01-04	22:11:04.386367 10.8.36.11	10.8.36.66	RTP	214 PT=ITU-T G.711 PCMU, SSRC=0x3D68BDD1, Seq=17902, Time=401486310								
	14165 2023-01-04	22:11:04.386702 10.8.36.66	10.8.36.11	ICMP	242 Destination unreachable (Port unreachable)								
	14171 2023-01-04	22:11:04.404810 10.8.36.10	10.8.36.66	SIP	360 Request: ACK sip:1331@10.8.36.66:5060								
	14172 2023-01-04	22:11:04.406359 10.8.36.11	10.8.36.66	RTP	214 PT=ITU-T G.711 PCMU, SSRC=0x3D68BDD1, Seq=17903, Time=401486470								
	14173 2023-01-04	22:11:04.406703 10.8.36.66	10.8.36.11	ICMP	242 Destination unreachable (Port unreachable)								
1	14174 2023-01-04	22:11:04.426366 10.8.36.11	10.8.36.66	RTP	214 PT=ITU-T G.711 PCMU, SSRC=0x3D68BDD1, Seq=17904, Time=401486630								
	14175 2023-01-04	22:11:04.426714 10.8.36.66	10.8.36.11	ICMP	242 Destination unreachable (Port unreachable)								
1	14179 2023-01-04	22:11:04.446366 10.8.36.11	10.8.36.66	RTP	214 PT=ITU-T G.711 PCMU, SSRC=0x3D68BDD1, Seq=17905, Time=401486790								
÷.	14180 2023-01-04	22:11:04.446772 10.8.36.66	10.8.36.11	ICMP	242 Destination unreachable (Port unreachable)								
	14186 2023-01-04	22:11:04.466355 10.8.36.11	10.8.36.66	RTP	214 PT=ITU-T G.711 PCMU, SSRC=0x3D68BDD1, Seq=17906, Time=401486950								
	14189 2023-01-04	22:11:04.467256 10.8.36.66	10.8.36.11	RTP	214 PT=ITU-T G.711 PCMU, SSRC=0x6AE40472, Seq=1139, Time=350293475								
	14190 2023-01-04	22:11:04.486364 10.8.36.11	10.8.36.66	RTP	214 PT=ITU-T G.711 PCMU, SSRC=0x3D68BDD1, Seq=17907, Time=401487110								
	14191 2023-01-04	22:11:04.486762 10.8.36.66	10.8.36.11	RTP	214 PT=ITU-T G.711 PCMU, SSRC=0x6AE40472, Seq=1140, Time=350293635								
	14196 2023-01-04	22:11:04.506358 10.8.36.11	10.8.36.66	RTP	214 PT=ITU-T G.711 PCMU, SSRC=0x3D68BDD1, Seq=17908, Time=401487270								
	14197 2023-01-04	22:11:04.507033 10.8.36.66	10.8.36.11	RTP	214 PT=ITU-T G.711 PCMU, SSRC=0x6AE40472, Seq=1141, Time=350293795								
	14202 2023-01-04	22:11:04.526371 10.8.36.11	10.8.36.66	RTP	214 PT=ITU-T G.711 PCMU, SSRC=0x3D68BDD1, Seq=17909, Time=401487430								
	14203 2023-01-04	22:11:04.526459 10.8.36.66	10.8.36.11	RTP	214 PT=ITU-T G.711 PCMU, SSRC=0x6AE40472, Seq=1142, Time=350293955								
	14204 2023-01-04	22:11:04.547374 10.8.36.11	10.8.36.66	RTP	214 PT=ITU-T G.711 PCMU, SSRC=0x3D68BDD1, Seq=17910, Time=401487590								
	14205 2023-01-04	22:11:04.547374 10.8.36.66	10.8.36.11	RTP	214 PT=ITU-T G.711 PCNU, SSRC=0x6AE40472, Seq=1143, Time=350294115								
<													
-	Ecomo 14129, 939	huter on wine (6704 hitr) 939 but	ter cantured (6704 bi	+c)									

Frame 14128: 838 bytes on wire (6704 bits), 838 bytes captured (6704 bits) Ethernet II, Scr. IKCPLaff.fic3b1 (80:22:a7:fic3b1), Dat: IKCPLaff\_f7:62:8e (80:22:a7:f7:62:8e) Internet Protocol Version 4, Src: 10.8.36.10, Dst: 10.8.36.66 User Datagema Protocol, Scr. Port: 5080, Dst Port: 5060 Session Initiation Protocol (INVITE)

0000	80	22	a7	f7	62	8e	80	22	a7	f1	<b>c</b> 8	<b>b1</b>	<b>0</b> 8	00	45	00	· " · · b · · "	• • • • • • E •
0010	03	38	60	e6	00	00	40	11	ba	73	0a	<b>0</b> 8	24	0a	0a	08	· 8` · · · @ ·	·s··\$···
0020	24	42	13	d8	13	c4	03	24	d2	bb	49	4e	56	49	54	45	\$B · · · · \$	· · INVITE
0030	20	73	69	70	Зa	31	33	33	31	40	31	30	2e	38	2e	33	sip:133	1010.8.3
0040	36	2e	36	36	3a	35	30	36	30	20	53	49	50	2f	32	2e	6.66:506	0 SIP/2.
0050	30	0d	0a	46	72	6f	6d	3a	20	Зc	73	69	70	3a	74	72	0. From:	<sip:tr< th=""></sip:tr<>
0060	6b	30	32	35	40	31	30	2e	38	2e	33	36	2e	31	30	3a	k025@10.	8.36.10:
0070	35	30	38	30	3e	3b	74	61	67	3d	31	36	44	46	33	32	5080>;ta	g=16DF32

And verify the RTP packet with IP, MAC and udp port references.

#### Investigate H.323-specific issues:

**EVCOR** 

Analyze H.323 messages to identify any call setup failures, such as "Setup" or "Call Proceeding" messages not receiving responses.

Inspect H.245 messages for any negotiation failures related to media capabilities or channel establishment.

Check Q.931 messages for errors or inconsistencies during call establishment, teardown, or redirection.

## **MULTI-MEDIA LOGGING SYSTEMS**



#### Troubleshoot Cisco Skinny issues:

- Examine Skinny protocol messages (SCCP) for any anomalies, such as missing or incorrect message types.
- Validate that the necessary Skinny messages, such as "StationInit," "CallInfo," "CallCtlConnCompl," and "CallCtlTermConn," are exchanged correctly.
- Verify that the devices involved in the call have compatible Skinny protocol versions.
- Resolve RAW RTP mode issues:
- Analize RTP packet headers to check for issues such as incorrect timestamps, sequence numbers, or synchronization source (SSRC) identifiers.
- Identify any RTP packets with packet loss, high jitter, or unusual latency.
- Verify that the correct codecs and payload types are used for audio encoding and decoding.

#### Cross-Referencing with VoIP Logger:

Compare the Wireshark logs with the recorded audio on the VoIP logger.

- Check for discrepancies in timing, such as delays or missing audio segments, between the network traffic and the recorded audio.
- Use the timestamp information in both the Wireshark logs and the audio recordings to identify any synchronization issues.

#### Packet-level Troubleshooting:

- Inspect individual packets in Wireshark to identify abnormalities, such as malformed packets, packet fragmentation, or excessive retransmissions.
- Look for patterns or recurring issues across multiple packets that may indicate underlying problems.

#### **Collaboration and Vendor Support:**

If unable to resolve the issue, escalate the problem to the relevant network or VoIP vendor support team.

• Provide them with the detailed troubleshooting steps you have performed, along with the captured Wireshark logs for their analysis.

# **MULTI-MEDIA LOGGING SYSTEMS**



• Collaborate with the vendor support team to address complex issues that require deeper protocol-specific knowledge.

#### Software/Logger Related configurations:

REVCOR

1. Verify the available VoIP input NIC interfaces and label them properly.

2. Set the static IP by going into the IPV4 NIC properties.

3. Disable the IPV6 option in the NIC properties.

4. Verify that the VoIP channels settings are configured properly and with their respective channel triggers.

5. Verify that the VoIP channel IP/MAC addresses are set up correctly.

6. Select the proper VoIP NIC interfaces in Revconfig and leave the rest of the interfaces unselected.

7. Verify that WinPcap or Win10Pcap is installed on the system.

Once all of these have been verified and are good, proceed to capture Wireshark if there are any problems in recording all VoIP channels or sp

## **MULTI-MEDIA LOGGING SYSTEMS**

