

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:

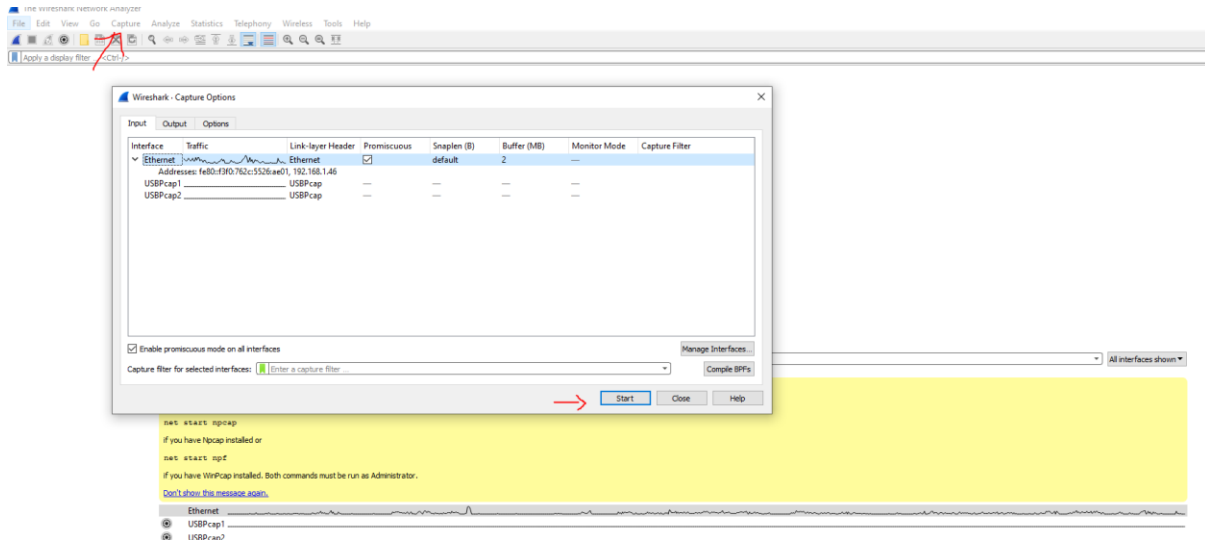
- Validate the connectivity between the VoIP logger and the port mirror destination by performing a ping test or using other network diagnostic tools.
- Ensure that there are no network devices, such as firewalls or security appliances, blocking the traffic between the port mirror destination and the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

KNOWLEDGE BASED ARTICLES

- 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.



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 address: `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:

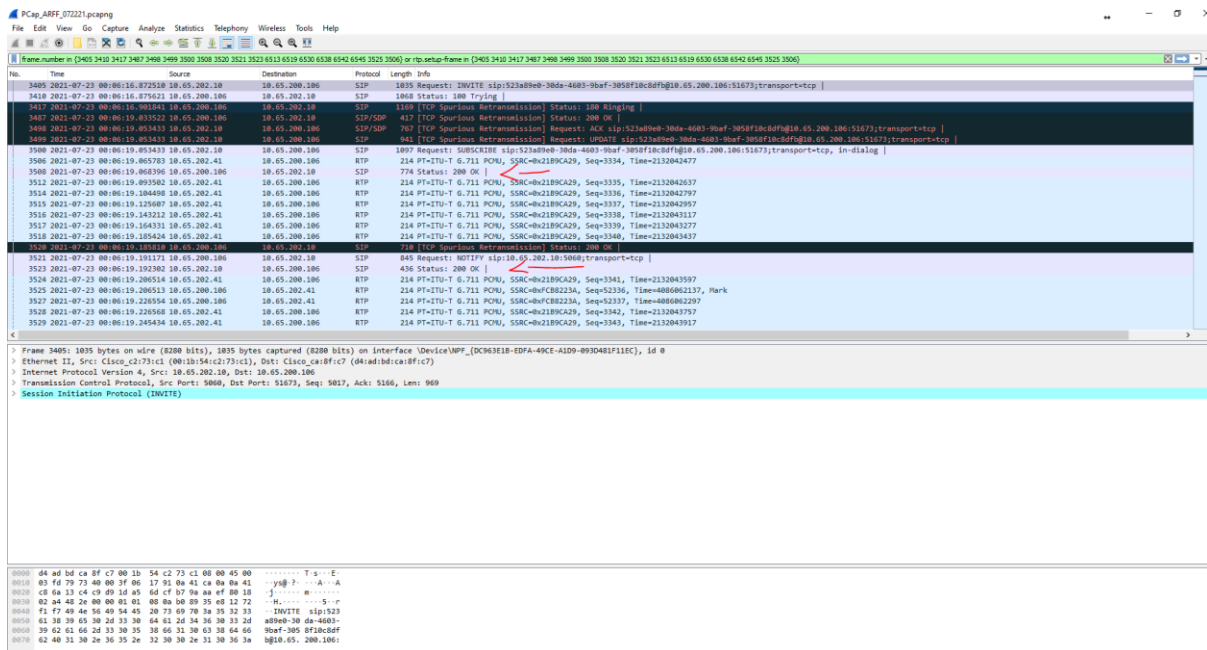
Check for SIP error codes (4xx, 5xx, etc.) indicating failures in the call setup or registration process.

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

KNOWLEDGE BASED ARTICLES

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:



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

KNOWLEDGE BASED ARTICLES

The image shows a Wireshark capture of network traffic. The main pane displays a list of packets with columns for No., Time, Source, Destination, Protocol, Length, and Info. The packets are filtered by 'frame.number in (14128 14154 14171 26945 26956 14189 14199) or rtp.setup-frame in (14128 14154 14171 26945 26956 14189 14199)'. The list includes SIP messages (INVITE, ACK) and RTP packets. Several RTP packets are marked as 'Destination unreachable (Port unreachable)'. Below the packet list, a packet details pane shows the structure of frame 14128, including Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and Session Initiation Protocol (INVITE).

No.	Time	Source	Destination	Protocol	Length	Info
14128	2023-01-04 22:11:04.175878	10.8.36.10	10.8.36.66	SIP/SDP	838	Request: INVITE sip:1331@10.8.36.66:5060 (application/x-ecmascript)
14154	2023-01-04 22:11:04.338358	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=0x30688001, 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=0x30688001, 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=0x30688001, 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)
14174	2023-01-04 22:11:04.406356	10.8.36.11	10.8.36.66	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x30688001, Seq=17904, Time=401486630
14175	2023-01-04 22:11:04.406703	10.8.36.66	10.8.36.11	ICMP	242	Destination unreachable (Port unreachable)
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=0x30688001, 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=0x30688001, 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=0x6AE48472, 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=0x30688001, 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=0x6AE48472, 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=0x30688001, 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=0x6AE48472, 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=0x30688001, 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=0x6AE48472, 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=0x30688001, 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 PCMU, SSRC=0x6AE48472, Seq=1143, Time=350294115

```
> Frame 14128: 838 bytes on wire (6704 bits), 838 bytes captured (6704 bits) on interface 0
> Ethernet II, Src: NECPLatf_f1:c8:b1 (08:22:a7:f1:c8:b1), Dst: NECPLatf_f7:62:8e (08:22:a7:f7:62:8e)
> Internet Protocol Version 4, Src: 10.8.36.10, Dst: 10.8.36.66
> User Datagram Protocol, Src Port: 5060, Dst Port: 5060
> Session Initiation Protocol (INVITE)
```

```
0000  80 22 a7 f7 62 8e 00 22 a7 f1 c8 b1 08 00 45 00  -"-b"-----E:
0010  03 38 60 e6 00 00 40 11 ba 73 0a 00 24 0a 0a 00  -" :g : : $ :
0020  24 42 13 68 13 c4 03 04 d2 10 49 4e 56 49 54 45  -$-----$ INVITE
0030  20 73 69 70 3a 31 33 33 31 40 31 30 2e 38 2e 33  -sip:1331@10.8.3
0040  36 2e 36 36 3a 35 30 36 30 20 53 49 50 2f 32 2e  -6.66:5060 SIP/2.
0050  30 00 0a 46 72 6f 6d 3a 28 3c 73 69 70 3a 74 72  - :From: <sip:tr
0060  60 30 32 35 40 31 30 2e 38 2e 33 36 2e 31 30 3a  -k025@10.8.36.10:
0070  35 30 30 30 3e 3b 74 61 67 3d 31 36 44 46 33 32  -5080;ta g=160F32
```

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

Investigate H.323-specific issues:

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.

KNOWLEDGE BASED ARTICLES

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:
- Analyze 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.

KNOWLEDGE BASED ARTICLES

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

Software/Logger Related configurations:

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