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.

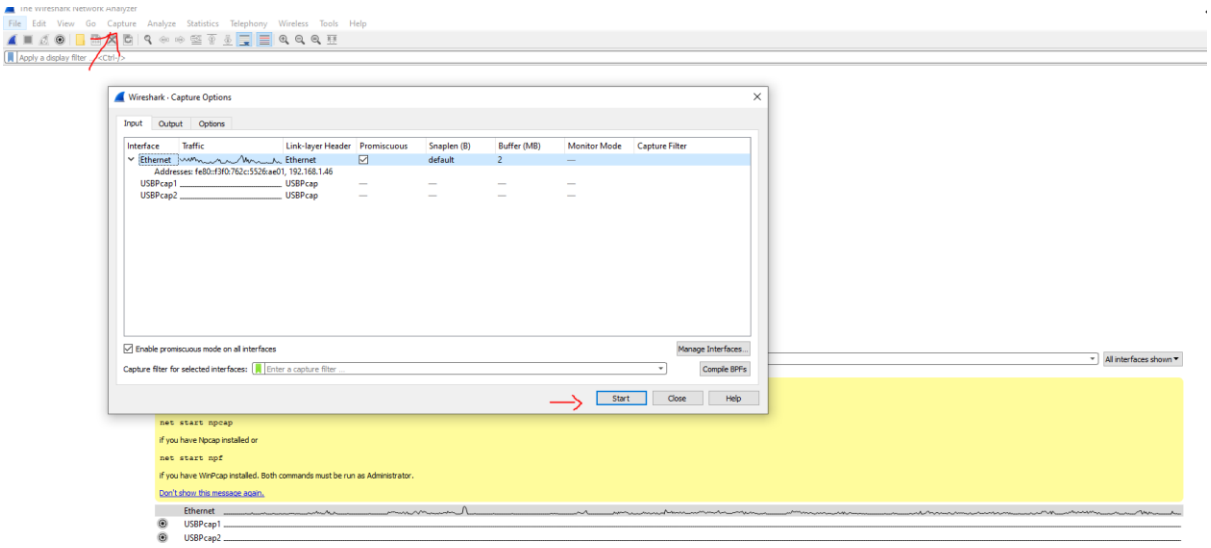
Confirm Connectivity:

- 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).

- 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.



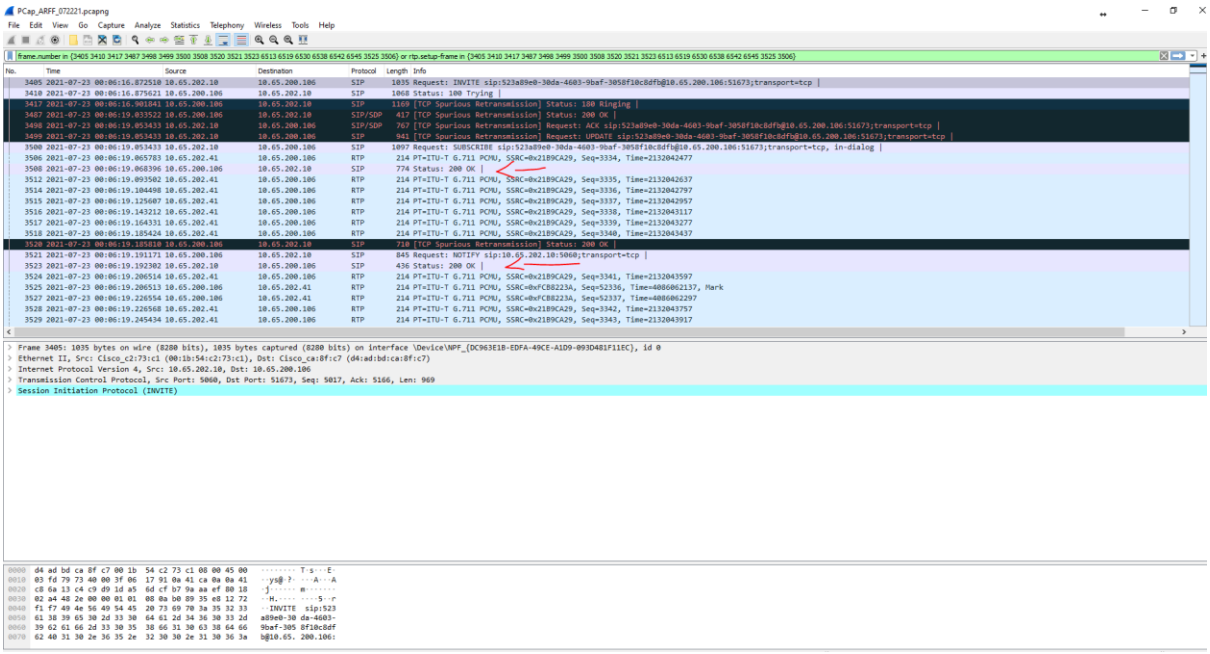
Set the capture buffer size to accommodate the expected duration of the troubleshooting session.

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

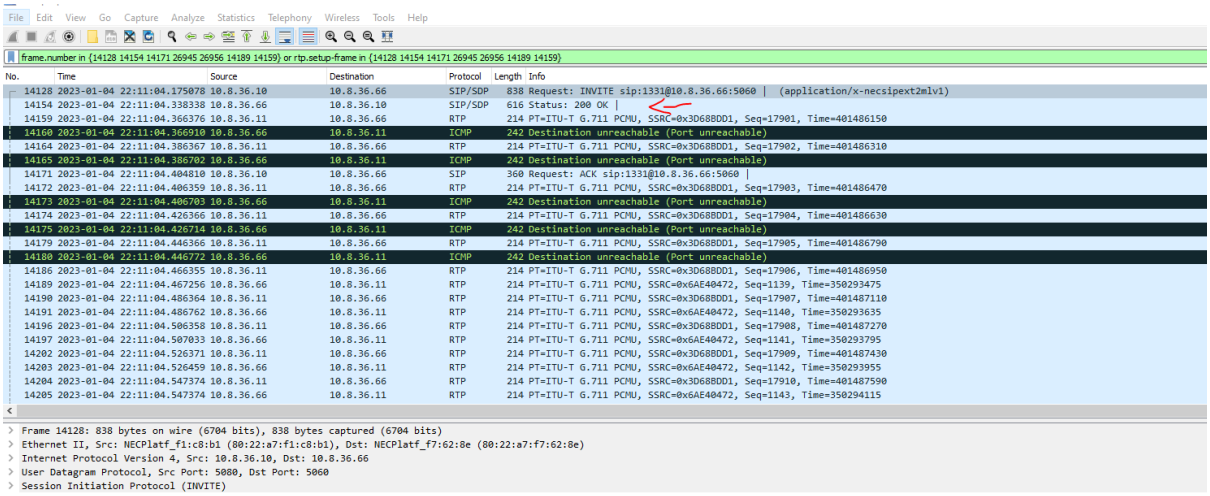
Analyze the Captured Logs:
Check for SIP error codes (4xx, 5xx, etc.) indicating failures in the call setup or registration process.
Examine SIP headers for incorrect or missing information, such as the "Contact," "From," "To," "Call-ID," and "Via" headers.

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:



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.

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.

- 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