📋 T.38 Malformed Packet Analysis Report

1️⃣ Initial Call Setup: G.711 Audio Call

- **Client to Server (SIP INVITE)**:
  - The client initiated the call using **SDP** with **G.711U and G.711A codecs**, indicating a **voice call**.
  - **Media port on client**: **10338** (used for sending audio to the server).
  - The server responded with a **200 OK** message to confirm it was ready to receive call data.
  - **Media port on server**: **16834** (used to receive and stream audio).
  - The client sent an **ACK**, and two-way audio was established using **G.711 codecs**.

2️⃣ T.38 Negotiation: Transition from G.711 to T.38 Fax

- During the established G.711 audio call, the **server sent a second SIP INVITE** to switch the media type to **T.38 fax protocol**.
- **Port 16834**: The server requested to continue using this port for **T.38 image data**, maintaining the same media port used for G.711 audio.
- **Client's Response**:
  - The client acknowledged with a **100 Trying** and later a **200 OK** to confirm it was ready to receive **T.38** fax data.
  - The client switched to **port 10340** for receiving T.38 data, while the server continued using **port 16834**.
  - The server acknowledged the new configuration using an **ACK** message.

3️⃣ Call Termination

- After the **fax session** ended, the **client sent a BYE message**, signaling the end of the call.
- The **server responded with a 200 OK**, confirming the successful termination of the session.

📝 Key Observations

1. **Port Usage**
   - **Server's port (16834)**: Used for **both G.711 audio** and **T.38 fax** data.
   - **Client's ports (10338 and 10340)**:
     - Port **10338** for receiving **audio** (G.711).
     - Port **10340** for receiving **T.38 fax image data**.

2. **Why Were T.38 Packets Malformed?**
   - When the media switched from **G.711 to T.38**, the server continued sending RTP audio packets on **port 16834**.
   - **Wireshark Interpretation**:

- Wireshark's telephony analyzer expects an **immediate switch** from **RTP audio** to **T.38 fax**.
- Since audio packets were still sent briefly after the renegotiation, Wireshark mistakenly interpreted them as **malformed T.38 packets**.
- The first few packets after the switch were **incorrectly flagged** as malformed, while the remaining T.38 packets were properly received.

🛠 Root Cause of the Problem

- **Incorrect Vega Configuration**:
  - The **Momentum SBC's** failed to honor the new port (10340) the Vega client opened to receive **T.38 fax data**.
  - The Vega client attempted to use a different port other than the audio port (**16834**) for receiving T.38 data, which caused **no fax data** to be received.
  - **Solution**: Configure the Vega to receive T.38 fax data on the **same port as G.711 audio (16834)**.

☑ Corrective Solution

1. **Correct Vega Configuration**:
   - Update the Vega gateway configuration to receive **T.38 fax data on port 16834**, the same port as G.711 audio.
   - This ensures that **T.38 fax data** is received and processed correctly, in line with the renegotiated media configuration.

📋 Conclusion

- The **root cause** of the T.38 malformed packets was the **incorrect port configuration** on the Vega gateway, where the momentum SBC's were not honoring the new port (10340) for T.38. Instead, the SBC's were honoring the audio port(10338) and this caused the T.38 Port that was opened by the vega client port fail to receive the T.38 fax data.
- **Correct solution**: Configuring the Vega gateway to receive **T.38 fax data on the audio port(10338)** resolved the issue.
- Additionally, as noted in the Wireshark Q&A post, **Wireshark expects an immediate switchover** from audio RTP to T.38, and any residual RTP packets may be misinterpreted as malformed T.38 packets until the correct configuration is applied.

📋 Files and Resources

Wireshark Capture (.cap)

- Review the Wireshark capture for detailed analysis:
  Cloudshark Wireshark Capture

🔍 Live Packet Analysis in MDX using CloudShark

Wireshark Capture (.cap)