

Summary of the Analysis of the T.38 Malformed Packets

1 Initial Call Setup (G.711 Audio Call)

- **Client to Server (SIP INVITE):**
 - The client initiated a call using **SDP** with the **G.711U and G.711A codecs**, indicating an audio call.
 - Media port on client: **10338** (used for sending audio to the server).
 - The server responded with **200 OK** (SIP response) 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 a two-way audio call was established using **G.711 codecs**.
-

2 T.38 Negotiation (Switch from G.711 to T.38 Fax)

- During the audio call, the **server sent a second SIP INVITE** to the client to switch the media type to **T.38 fax protocol**.
 - The server requested to continue using **port 16834** for the T.38 image data (same port used previously for audio).
 - The client responded with **100 Trying** to acknowledge receipt and indicate that it was processing the request.
 - The client then sent a **200 OK** to confirm it was ready to receive T.38 fax data.
 - The client used a new port, **10340**, for receiving T.38 image data.
 - The server acknowledged this change using **ACK**.
-

3 Call Termination

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

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):** The client used different ports for receiving **audio (10338)** and **T.38 image data (10340)**.

2. Why Were T.38 Packets Malformed?

- When the media switched from **G.711 to T.38**, the server kept using port **16834**.
- Since the switch was not instantaneous, some residual **RTP audio packets** were still being sent on **port 16834**.
- As referenced in [this post on the Wireshark Q&A site](#), **Wireshark's telephony analyzer expects an immediate switchover**, assuming the first media packet after renegotiation is

already **T.38**.

- However, when audio RTP packets continue for a short while after the switchover, Wireshark may misinterpret and dissect these as **T.38 packets**, leading to "**malformed packet**" errors.
- Only the first few packets after the renegotiation are malformed; the rest are clean T.38 packets.

Root Cause of the Problem

- **Incorrect Vega Settings:**

The issue occurred because the **Vega gateway was misconfigured** to receive **T.38 signals on the wrong port**.

Instead of properly switching to the port designated for **T.38 fax**, the Vega was still trying to receive **fax data on the audio (RTP) port**.

As a result, the fax data was not properly received, and Wireshark marked the initial T.38 packets as malformed.

Correct Solution

1. Correct Vega Configuration:

- The solution was to configure the **Vega gateway** to receive **T.38 fax data on the audio port** (Port 16834).
- This ensures that the T.38 image data is properly received on the same port as G.711 audio, which is in line with the negotiated media parameters.

2. Avoid Misinterpretation of Ports:

- Avoid changing ports during the switch from **G.711 to T.38** to prevent media confusion.
- If a port change is required, ensure it is clearly signaled during the **SIP re-INVITE**.

Conclusion

- The root cause of the issue was **incorrect Vega gateway settings** that caused it to expect **T.38 signals on the wrong port**, resulting in no fax data being received.
- The **correct solution** was to configure the Vega to **receive T.38 fax data on the same port as the audio (16834)**.
- As referenced in the [Wireshark Q&A post](#), **Wireshark expects a clean and immediate switchover from RTP (audio) to T.38**. Any residual RTP packets on the media port can be misinterpreted as **malformed T.38 packets**, but this issue is often resolved once the correct configuration is applied.