

Requirements & Networking Optimisations

Ports

Telviva One uses port 4433 and your network & firewall should allow traffic on this port.

Port 4433 has to be open for both UDP and TCP protocols.

In addition, your device would have to have full access to <https://one.telviva.com/api> in order to access the required APIs

Routing

Your firewall should allow outgoing & incoming UDP to the public internet
We utilize WebSocket connections, so HTTPS / WebSocket / Secure RTP should be allowed.

Wifi

Local network conditions have the biggest impact on voice quality.
Jitter, latency, and packet loss can be the biggest contributors to voice quality issues in any VoIP network.

Latency	The time it takes the RTP (media) packets to arrive at the destination	Causes media delivery delays, callers may speak over the top of each other.
Packet loss	Packets that don't make it to the final destination	Causes gaps and cut-outs in media, callers may not hear the other side
Jitter	Packets that arrive at the destination out of order	Cause a 'robotic' distortion effect in media, or packet loss when overrunning the jitter buffer

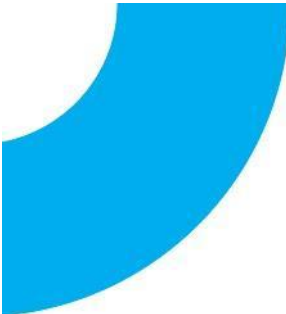
Latency:

High latency can substantially degrade a caller's experience. While there will always be some latency between the codec algorithm, the jitter buffer, and network traversal, the goal is to keep this to a minimum. Callers typically start to notice the effect of latency once it breaches 250ms and find latency above ~600ms to be nearly unusable. Here are some strategies to minimize latency on your network:

- Some lower bandwidth fixed internet connections can often have higher latency. If possible, upgrade your internet connectivity.
- Stick to high-bandwidth connections. Mobile networks such as LTE (mobile 4G Data) can often have high latency.

Jitter:

Packet loss, most frequently jitter-induced packet loss, can greatly impact your VoIP call quality. Wi-Fi can be particularly bad for creating jitter. Here are some strategies to minimize jitter on your network:

- 
- Reduce packet conflicts on Wi-Fi by reducing the number of devices operating on the same channel.
 - Avoid large data file transfers concurrently with voice over the same Wi-Fi environment.
 - Avoid [buffer bloat](#), which can result in high latency, and bursts of jitter. We recommend ensuring your router is configured with the low buffer size, as high jitter cannot be masked by a buffer without introducing artificial delay, and often choppy audio. Note: Not all routers allow for configuring buffer sizes, but some routers ship with defaults that are not optimized for real-time VoIP networks. Open-source routers, enterprise-grade routers, and gamer-oriented routers are good candidates for providing the right configuration options and defaults.

If you have addressed the above issues and continue to have jitter related impact on your voice quality, you may consider configuring your router with QoS rules to prioritize traffic on the above media UDP ports. Given the large range of UDP ports, you should only do this with prior consideration to what other traffic may be flowing in that port range.

Call quality

By following this guide, you can significantly improve the quality of service for wireless voice applications and reduce or eliminate dropped calls, choppy speech, fuzzy speech, buzzing, echoing, long pauses, one-way audio, and issues while roaming between access points.



3 key metrics for voice quality:

- Network MOS – The Network Mean Opinion Score (MOS) is the network's impact on the listening quality of the VoIP conversation. The score ranges from 1 to 5, with 1 being the poorest quality and 5 being the highest quality.
- Packet Loss Rate – The packet loss rate is the percent of packets that are lost during transmission.
- Interarrival Jitter – Interarrival jitter measures the variation in arrival times of packets being received in milliseconds (ms).

Below is a summary of the best practices to provide the best voice quality over wireless.

Perform a pre-install RF survey for overlapping 5 GHz voice-quality coverage with -67 dB signal strength in all areas. (Use Wifi Analyzer App)

If possible, create a new SSID dedicated to your voice over IP devices.

- Set Authentication type to 'Pre-shared key with WPA2'
- Set WPA encryption mode to 'WPA2 only'
- Enable '5 GHz band only'

Enable 'Traffic shaping' on the SSID to prioritize all voice traffic

SIP 5060 UDP / TCP – RTP 10000-20000 UDP – internal Network / UDP 65550 if

Vibe goes via Firewall

- network 197.155.248.128/25
- network 197.155.249.128/25
- network 197.155.250.128/25
- network 197.155.251.128/25

Set DSCP to '46 (EF – Expedited Forwarding, Voice)' for RTP

Video Meetings

What Telviva One needs to be able to access to log in and for a call to work:

- Note the use of WebSockets – both to collect Telviva “events” and for the webrtc for calls. Some customers may have a web proxy running – some older web proxy software is not compatible with WebSockets even though they are standard.
- address 197.155.248.84, TCP port 443: Used for access to the Telviva One backend services – straight HTTP requests used, but also wss (secure websocket) connection for PBX events from Telviva.
- rtcproxies (197.155.250.156/30, 197.155.248.156/30 to follow):
- tcp port 4433: WebRTC connections (this is an encrypted websocket connection carrying SIP packets to and from JSSIP on the client system).
- tcp port 3478: STUN and TURN service, a requirement for WebRTC.

Observations:

1. TCP port 443 is the default port for secure HTTP. It would be very unusual for that to be blocked; if it were blocked most websites wouldn't work.
2. TCP port 4433 is a fairly commonly used secondary port for secure HTTP. But more likely that it is blocked. It might have to be unblocked on the firewall.
3. TCP port 3478 is for STUN/TURN, a requirement for all webrtc and used by modern SIP phones to help deal with NAT. It should be opened.

A customer using a WEB PROXY would need to check that it is compatible with the use of WebSockets. Websockets are a web/internet standard (<https://tools.ietf.org/html/rfc6455>) that should be supported.

