Quicklink Studio

WebRTC port allocation

QUICKLINK
Video Over IP Solutions

quicklink.tv

Network info

WebRTC is supported natively in most modern browsers however Quicklink only officially supports Google Chrome. WebRTC usually works without a problem using inbuilt networking technologies (STUN and TURN).

Environments with very restrictive firewalls may require some setup. The details below have further information for your IT-networking department.

WebRTC client connects using the following details:

Component	Address	Client-side port	Server side port	Protocol
Portal	quicklink.network	Any	443	HTTPS
Portal socket I/O	psio.quicklink.network	Any	443	TCP
Signaling	sig.quicklink.network	Any	443	TCP
STUN	global.stun.twilio.com	Any	3478	UDP/TCP
TURN	global.turn.twilio.com	Any	3478	UDP/TCP
Media (SRTP)	Listed below	Any	10,000 - 20,000	UDP
TURN (Network Dependent)	See location table	Any	All outgoing	UDP

The client will select any available port from the ephemeral range. On most machines, these means the port range 1,024 to 65,535. **This means Quicklink recommends in addition to the above rules, all outbound ports above 1024 UDP should be open.**

Video/Voice traffic on an organisation's local area network is similar to data traffic in that it is transmitted as packets over different devices. The main difference between data and video/voice traffic is that data traffic has the ability to resend information if it initially gets lost in transit. Video/ Voice traffic, on the other hand, cannot resend information because the packets must be received in order as a continual stream for the information to make sense. As such, **the way Video packets are treated in your network will have a significant effect on your Video call quality.**

We recommend configuring your network such that voice traffic has a higher priority than data traffic. This will ensure that issues related to voice packets are minimized and that your calls have optimal audio quality without having a noticeable effect on your data traffic. Traffic prioritization can be configured in a variety of ways, but we suggest prioritizing packets based on the IP addresses listed below. Please reach out to your organization's network / IT team to determine the best way to set up traffic prioritization. If you do not have an IT team you can reach out to your internet provider to see if prioritization can be configured on your network.

If you want to prioritise voice traffic on your local area network, you can set up QoS rules using the following media server IP addresses. Doing so is optional, although we do recommend it.

Location	Media server IP address range	CIDR notation
Australia	54.252.254.64 - 54.252.254.127	54.252.254.64/26
Brazil	177.71.206.192 - 177.71.206.255	177.71.206.192/26
Ireland	54.171.127.192 - 54.171.127.255 52.215.127.0 – 52.215.127.255	54.171.127.192/26 52.215.127.0/23
Japan	54.65.63.192 - 54.65.63.255	54.65.63.192/26
Singapore	54.169.127.128 - 54.169.127.191	54.169.127.128/26
US East Coast (Virginia)	54.172.60.0 - 54.172.61.255	54.172.60.0/23
US West Coast (Oregon)	54.244.51.0 – 54.244.51.255	54.244.51.0/23

We recommend you set up all of them, regardless of your location. Our service uses Global Low Latency routing to select the data center with the lowest-latency.

Additionally, Quicklink enables DSCP by default in compatible browsers (currently Google Chrome). Capable browsers will tag WebRTC media packets, enabling differentiated handling on a LAN, so that real-time media can be prioritized above other network traffic.

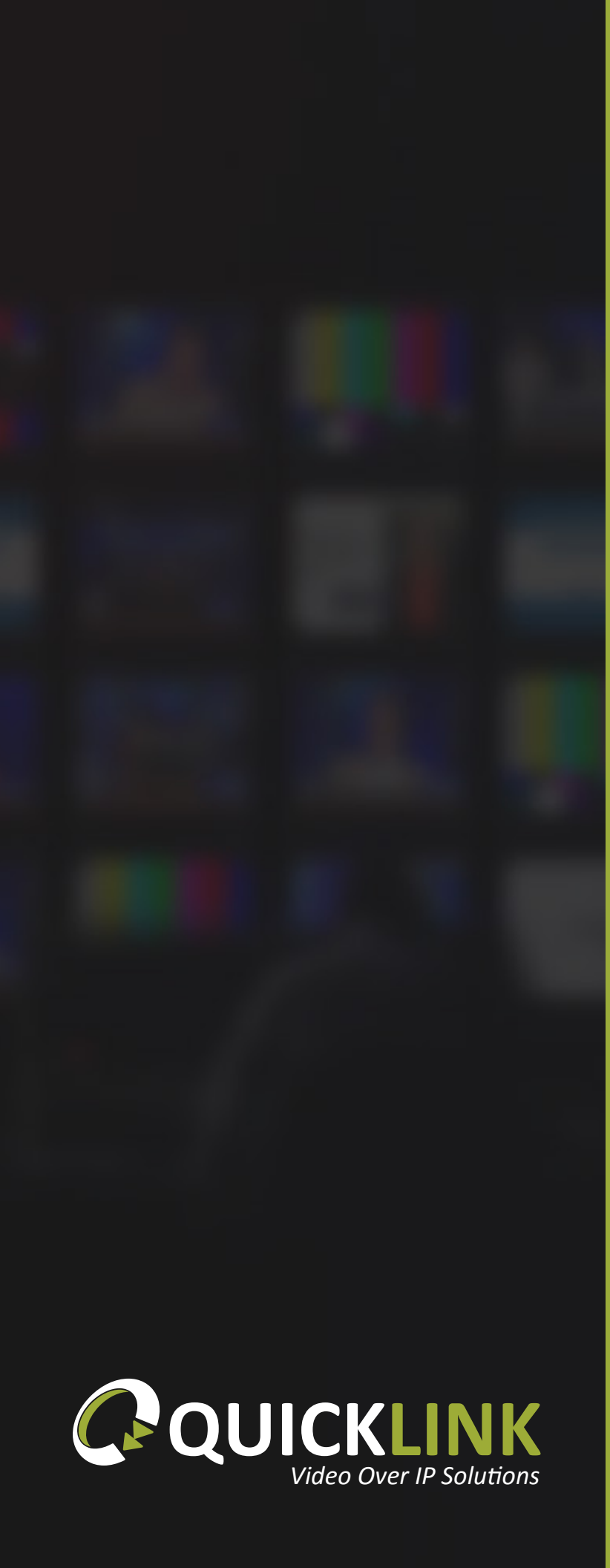
Further info

Client opens a socket on a random port (e.g. 50001)

Contacts STUN server using that socket to discover the external IP: port mapping for this socket. (e.g. 192.168.1.2:50001 maps to 1.2.3.4:50001). Ports don't necessarily have to match between internal and external addresses, but they usually do, so I'll keep with that for this example.

Through an external mechanism (SIP, XMPP, Jingle, cups with strings), the candidate address list of both nodes are exchanged. This includes all known internal and external addresses collected (e.g. 192.168.1.2:50001 and 1.2.3.4:50001).

Using the same socket opened in step 1, both sides send (STUN) messages (UDP packets) directly between each other. The first pair of messages may be blocked by the router/firewall. But because one side initiated an outbound packet to the remote address, subsequent packets from that address are allowed back in. This is called the "hole punching step". Hence, the port is dynamically open without the router needing any specific configuration.



Contact

+44 1792 720880

support@quicklink.tv

quicklink.tv

QUICKLINK
Video Over IP Solutions