TELNET
WORLDWIDE

SIP Trunking LAN
Requirements

Routers and Switches

All on-premise hardware are network devices that require at least a commercial router to function properly. The router selected should have the following capabilities:

- **DHCP** - Devices should receive an internal IP address assignment via Dynamic Host Configuration Protocol (DHCP). Each endpoint will consume an IP address.
- **NAT** - All Network Address Translation (NAT)connections must be left open for at least 60 seconds.
- **QoS** - In a converged network, Quality of Service (QoS) must be applied to prioritize voice traffic over all other traffic types.

Additional Configuration Recommendations

Avoid Double-NATing

Ideally, you will need to have only one device performing routing functions. Double-NATing (double- outing) is known to cause many problems for VoIP phones. It is best to eliminate or bridge any extra or additional routers or modem/router combinations on your network. If you need to put your modem/router combination in bridge mode, please contact your Internet service provider (ISP) for assistance.

NOTE:

- If your service provider switches your modem to bridge mode, you are then required to provide security through your router. Please contact your equipment vendor for support

Disable SPI

SPI allows the router to approve or deny any information packets that flow through it for security reasons. However, it often incorrectly identifies VoIP traffic as a security risk. If you are experiencing connectivity issues, consider disabling SPI.

Disable SIP ALG

These are other security features that sometimes prevent traffic from flowing properly. If you are experiencing connectivity issues, consider disabling SIP ALG.

Disable any VoIP-specific functions

Networking equipment will often come customized for VoIP, but many of these custom configurations actually interfere with the traffic flow. TelNet's service does not require custom VoIP supporting functions. Ensuring all VoIP-specific functions are shut off should resolve most of your issues. After you have made the changes, you will need to restart your network.

Firewalls

Firewalls need to allow end point devices access to these protocols; HTTP, HTTPS, SIP and RTP on the network over TCP and UDP. End points must be allowed to both send and receive TCP and UDP packets on arbitrary ports and to arbitrary IP addresses. Some network ports may need to be opened manually.

Firewall Configuration Settings for Optimal Functionality

System Access

Please ensure open inbound/outbound access to the following IP addresses:

SIP/RTP/TCP/UDP entire blocks & ports 5060 to 5090, port 69	
64.27.210.0/27	66.79.209.0/26
66.79.197.240/28	209.142.200.0/26
209.142.210.4	

Persistent NAT Connections

NAT keep-alive requests must be allowed every 30 seconds.

SIP

Multiple TCP/UDP connections must be allowed.

RTP

Internally-initiated UDP requests must be allowed on ports 49152 through 65535 for audio. For additional ports that may need to be opened, please refer to your device’s user guide under the SIP Trunking section.

Bandwidth

All Hosted PBX/Voice over IP services require one or more broadband Internet connections to function properly. Dial-up, standard wireless, and satellite Internet connections are not supported and will negatively impact the delivery of Hosted Services. TelNet or partner-provided bandwidth is recommended for the best overall user experience as it is fully managed from end to end. Voice services can also be used “over the top” with alternate bandwidth providers via cable or fiber (aka, Bring Your Own Bandwidth – BYOB option).

Each voice call requires approximately 90 Kbps of bandwidth. The following table indicates required bandwidth for various levels of concurrent voice calls.

Concurrent Calls	Required Bandwidth
5	450 Kbps
10	900 Kbps
50	4.5 Mbps
100	9 Mbps

Make sure sufficient upload and download bandwidth is available to support the peak number of concurrent calls for your organization.

NOTE:

- Internal calls between IP phones within the same site only consume 8 Kbps signaling bandwidth over Internet connection (e.g., ~82 Kbps call payload remains on the LAN).

Reliability

SIP Trunking routed over a low-quality network may result in one or more of the following issues:

Latency

The time between a network request and response. Latency should be less than 100 ms. Latency greater than 150 ms will result in decreased quality.

Jitter

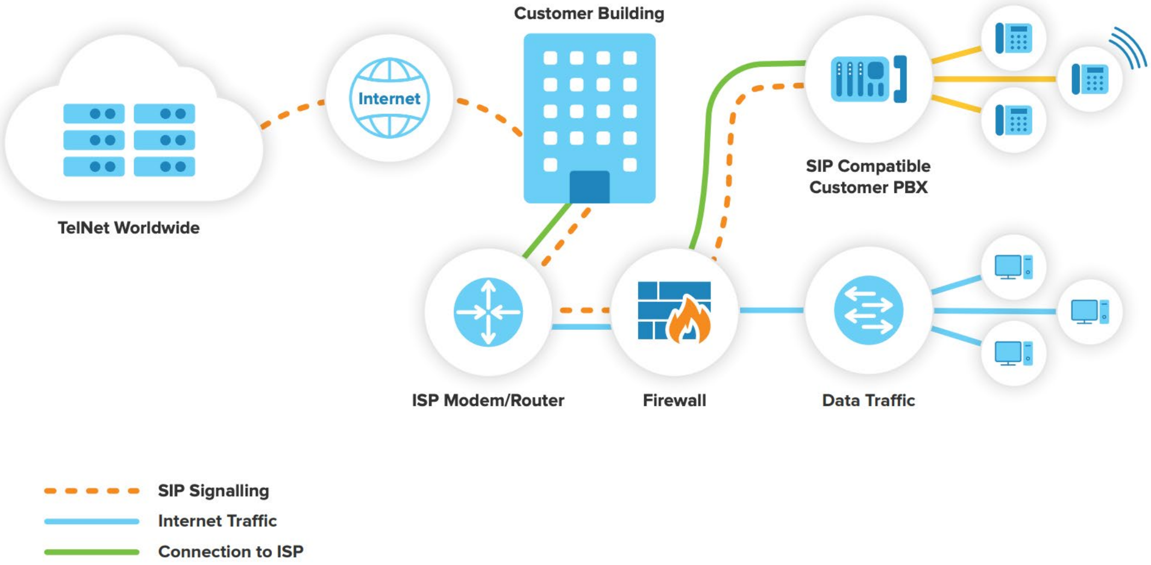
The amplitude and frequency of a network’s latency. Jitter should not exceed 20 ms. Jitter greater than 20 ms will result in decreased quality.

Packet Loss

Data from the client network that is lost in transit. Packet Loss should not exceed 1%. Packet Loss greater than 1% will result in low-quality or dropped calls.

Network Topology

Following is the typical network topology for SIP Trunking services setup:


Customer Building
TelNet Worldwide
Internet
SIP Compatible Customer PBX
ISP Modem/Router
Firewall
Data Traffic
SIP Signalling
Internet Traffic
Connection to ISP