TELNET

Cloud PBX LAN
Guide

Table of Contents

Local Area Network Requirements 2
Routers and Switches 2
Additional Configuration Recommendations 3
Disable SPI 3
Disable SIP ALG 3
Disable any VoIP-specific functions 3
Firewalls 4
Firewall Configuration Settings for Optimal Functionality 4
System Access 4
Persistent NAT Connections 4
SIP 4
RTP... 4
OBi302 & OBi508vs ATAs 4
Grandstream HT81X ATAs 5
Unity Applications 5
Yealink 5
Bandwidth 6
Facilities 6
Quality of Service 6
Physical Network Separation 6
Logical Network Separation 6
Reliability 6
Latency 6
Jitter 6
Packet Loss 6
Computer Traffic 6
Network Topology 7

Local Area Network Requirements

TelNet Cloud PBX service has a few basic network and installation requirements which ensure optimal quality and system uptime. In many cases, existing client hardware can satisfy these requirements.

Please share this document with your designated LAN administrator. Any required LAN changes or upgrades should be completed prior to service deployment.

We understand the appeal of using Wi-Fi for office phones, we recommend utilizing a dedicated and secure wired connection for our IP-based phone system. This will ensure reliable connectivity, consistent call quality, and compliance with emergency response requirements.

Utilizing Wi-Fi on IP Phones

Please review the below risks with using Wi-Fi on desk and/or conference phones.

1. 911 Related Issues:
One of the primary concerns with using Wi-Fi for office phones is the potential impact on emergency calls. If the Wi-Fi signal is weak or unavailable, it may prevent your IP-based phone from making a successful 911 call. This could pose a serious risk to employee safety and regulatory compliance.

2. Inconsistent Wi-Fi Signal
Wi-Fi networks can experience gaps in coverage, particularly in larger office spaces or areas with multiple floors. These gaps challenges can result in unreliable signal strength and intermittent connectivity, leading to dropped calls, poor call quality, and frustrating user experiences. When troubleshooting, we may ask you to plug a phone into an ethernet port.

3. Network Congestion:
Wi-Fi networks shared by multiple users can experience congestion, especially during peak usage times. Activities such as streaming video and audio can consume significant bandwidth, leading to decreased call quality, delays, and potential call drops. This can adversely affect the overall productivity and efficiency of your office communication.

4. Open Network and Lack of Password Protection:
Connecting IP-based phones to Wi-Fi networks introduces the potential security risk of an open network. If the Wi-Fi network is not properly secured with a password, unauthorized individuals may gain access to sensitive communications, potentially compromising confidential information or leading to misuse of resources.

5. Random Wi-Fi Password Resets:
Managed Service Providers (MSPs) or IT staff occasionally reset Wi-Fi passwords for security reasons or network maintenance. This can lead to interruptions in phone service if the IP-based phones are not promptly reconfigured with the updated credentials. Such resets can cause unnecessary disruptions and delays in communication, impacting your business operations.

Routers and Switches

Power over Ethernet (PoE) switches are highly recommended, as they eliminate the need for individual power adapters for each phone and also allow for centralized power redundancy. Additional benefits include extending phones into hard to reach areas (without surge protector and extension cord) and virtually separating voice and data traffic.

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 changes 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

SIP/RTP/TCP/UDP entire blocks & ports 5060 to 5090, port 69	
64.27.210.0/27	64.255.76.64/29
66.79.197.240/28	64.255.74.160/27
66.79.209.0/26	209.142.200.0/26
UDP, port 53	
69.54.192.2	69.54.200.10
NTP - UDP port 123	
0.0.0.0\0	

TCP, ports 80, 443		
50.19.91.154	64.54.192.26	64.255.76.67
174.129.241.97	54.209.17.125	64.255.64.21
54.210.244.98	64.255.64.30	34.238.237.220
54.174.154.29	52.5.133.228	52.71.103.102
52.201.1.15	34.238.237.220	34.235.12.107
35.153.119.139		

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

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.

OBi302 & OBi508vs ATAs

www1.obitalk.com service provider portal
https: port 443
Allow Outgoing TCP ports: 6800, 5222, 5223
Allow Outgoing UDP ports: 5060, 5061, 10000 to 11000, 16600 to 16998, 19305
Allow Incoming UDP port: 10000

Grandstream HT81X ATAs

Domain	Port	Description	Protocol
www.gdms.cloud	80, 443	For web access, firmware download and configuration download.	HTTP/HTTPS
us.download.gdms.cloud	80, 443	Firmware download and network speed detection.	HTTP/HTTPS
acs.gdms.cloud	80, 443	Communication between device and server.	HTTP/HTTPS
stun1.gdms.cloud	3478	STUN, Keep-alive, receiving UDP packets from devices.	UDP
syslog.gdms.cloud	6514	Syslog server.	TLS/TCP

Unity Applications

IP Addresses
34.253.150.243
52.210.190.221
52.212.31.86

Yealink

Domain Name
*.ymcs.yealink.com
*.yealink.com

Domain	IP	Port (TCP)	Description
rps.yealink.com rpscloud.yealink.com	20.242.144.0 20.242.144.1 52.71.103.102 51.11.241.228 20.19.96.56	433 HTTPS, 5061 phone_rps	Yealink auto provisioning

Bandwidth

All Cloud 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 voice 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.

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

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

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).

Facilities

Ethernet cabling and electrical power (or PoE) are required at each endpoint location. Cat-5 or better cabling is required. Consider using Cat-6 or Cat-6e cabling to support gigabit Ethernet networks. Battery backup is recommended for all network equipment.

If power adapters are used, be sure to use a surge protector.

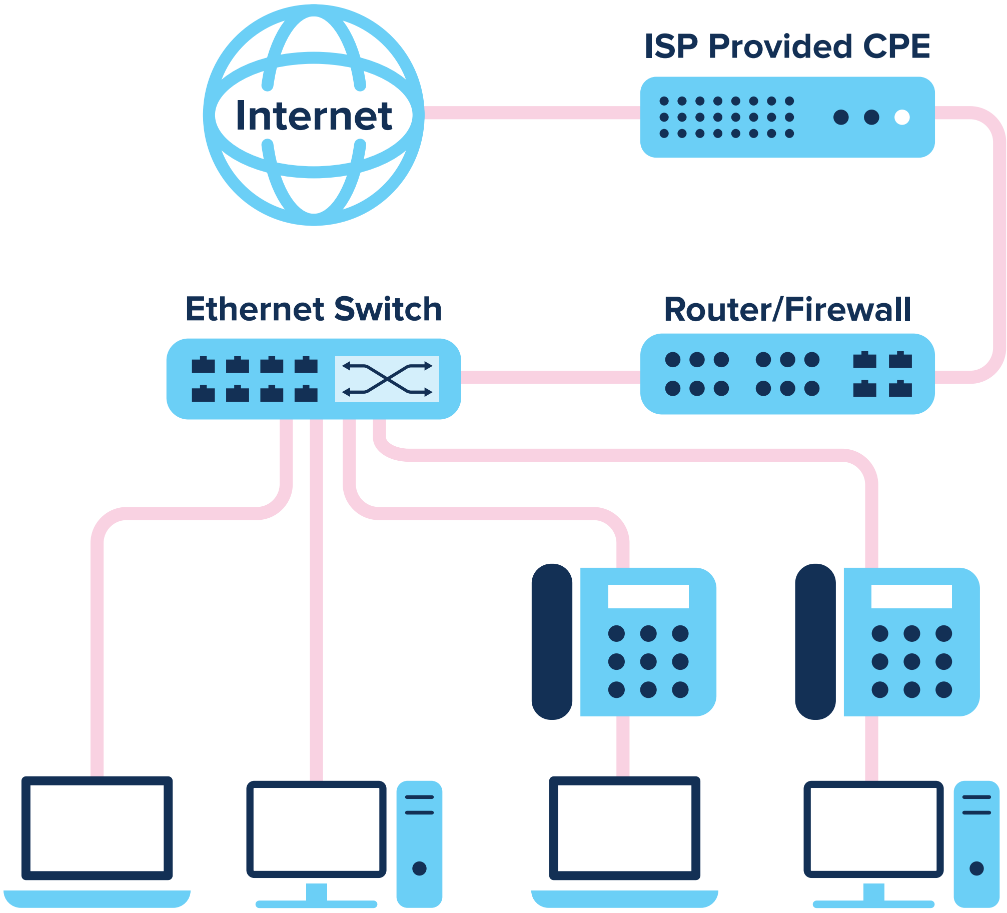
Quality of Service

Quality of Service (QoS) protocols provide the means to guarantee certain resource levels to specific types of network traffic. QoS is particularly important in voice implementations.

Cloud PBX services can utilize several QoS methods to ensure quality. The following strategies are the most effective in producing a stable, scalable network environment.

Physical Network Separation

Many institutions separate voice and/or video on a dedicated Internet connection to ensure quality. This strategy typically involves both separate physical WAN and LAN connections.


Internet
ISP Provided CPE
Ethernet Switch
Router/Firewall