Comcast Business UCaaS Sessions and Comcast Business VoiceEdge® Over-the-Top Services Technical Requirements

A customer's guide to the technical requirements for the Comcast Business UCaaS Sessions and Comcast Business VoiceEdge™ ("Business VoiceEdge") Over-the-Top services

This guide sets forth certain technical requirements for Comcast Business VoiceEdge over-the-top ("OTT") and Comcast Business UCaaS Sessions (each, a "Comcast Business OTT Voice Service" and collectively, the "Comcast Business OTT Voice Services") customers. As a reminder, Business VoiceEdge can be delivered either (a) OTT, utilizing customer's internet connectivity service or (b) if customer is within Comcast's footprint, customer can have a dedicated Business VoiceEdge modem and enterprise SIP gateway installed at the customer's service location to have customer's voice traffic on a separate, dedicated connection (the "Dedicated Service"). These Technical Requirements only apply to the UCaaS Sessions service and the Business VoiceEdge OTT service, not the Business VoiceEdge Dedicated Service.

This guide is designed to help you optimize call quality for the Comcast Business OTT Voice Services and supplements the Product-Specific Attachments for your Business VoiceEdge and UCaaS Sessions services available at https://business.comcast.com/enterprise/terms-conditions (each a "PSA" and collectively, the "PSAs").

We recommend that you review this guide with your company's Information Technology (IT) specialist prior to installation of your Comcast Business OTT Voice Service to ensure that your company is prepared for the installation of your Comcast Business OTT Voice Service and continues to meet these specifications or your Comcast Business OTT Voice Service will not function.

If you have questions about any of the requirements contained in these Technical Specifications, please speak to your Comcast Business sales engineer or project manager.

TABLE OF CONTENTS

Comcast Business OTT Voice Services Requirements

Business VoiceEdge OTT Specific Requirements

UCaaS Sessions-Specific Requirements

COMCAST BUSINESS

Comcast Business OTT Voice Services Requirements

Network Requirements

Bandwidth Requirements: Minimum 100 kbps per Voice over Internet Protocol ("VoIP") call

The Comcast Business OTT Voice Services share an internet connection with all computers and devices connected to your Internet network. Any spike in internet usage could affect call quality (including, for example, call completion) if there is insufficient bandwidth.

The Comcast Business OTT Voice Services require a minimum of 100 kbps available bandwidth (both upload and download) per VoIP call, including, without limitation, on local area networks (LANs) and wide area networks (WANs).

FOR EXAMPLE:
If you have 5 devices that each receive a phone call at the same time, you must have 500 kbps of bandwidth available. If you have 10 devices that each receive a phone call at the same time, you must have 1 Mbps of bandwidth available.

Ability to Troubleshoot

Keep in mind, you are solely responsible for procuring, maintaining and troubleshooting internet connectivity to support the Comcast Business OTT Voice Services. The Comcast Business OTT Voice Services will not be available for use if your internet connectivity service is inoperable.

Advanced: Network Settings, Configurations, and Port Assignments

Voice over IP (VoIP) Network requirements

Your internet connectivity service must meet three general network requirements to enable acceptable call quality. If your Internet services fail to meet any of these requirements, your service may fail completely or you could experience dropped calls and/or poor call quality.

Performance Metric	Network Requirement for Comcast Business OTT Voice Services
Latency (Measured 1 way from the phone to the UCaaS Service)	<40ms
Jitter (Network Delay Variation)	<20ms
Packet Loss	<2%

Router and Firewall Settings

Your router, firewall, and other edge devices connected to your network must be configured appropriately to support your Comcast Business OTT Voice Service.

Quality of Service and DSCP support

Comcast Business VoiceEdge IP Phones support Differentiated Services Code Point (DSCP) marking, which allows you to prioritize voice traffic (i.e., calls) over other traffic on your LAN. With DSCP marking, if there is a spike in data usage, your phone calls will take priority on your LAN.

To enable DSCP prioritization for voice traffic, please configure your router and firewall settings as follows:

- **Media:** Expedited Forwarding 46 (DSCP-46)
- **Signaling:** Assured Forward 31 (DSCP-26)

Domain Name System (DNS)

You must utilize a DNS solution that can resolve public DNS records, including Naming Authority Pointer (NAPTR), Service Record (SRV), and A records or the Comcast Business OTT Voice Service will not operate.

SIP ALG and NAT settings

All Comcast Business OTT Voice Service customers must disable the following settings:

- SIP ALG
- SIP Passthrough
- Deep Packet Inspection (DPI)
- Stateful Packet Inspection (SPI)

Confirm your Session Initiation Protocol (SIP) Application Layer Gateway (ALG) default setting is turned to "Off." Having the SIP ALG setting enabled may modify the SIP signaling to the phone and negatively impact Business VoiceEdge or UCaaS Sessions performance. The solution does not require the enablement of the SIP ALG setting.

If your router has a setting for Network Address Translation (NAT) endpoint filtering, make sure it is set to: "Endpoint Independent Transmission Control Protocol (TCP) and User Datagram Protocol (UDP)."

DPI and SPI should be **disabled** as they may interrupt or alter the signaling and media being passed over the network.

Business VoiceEdge OTT Specific Requirements

Network Compatibility

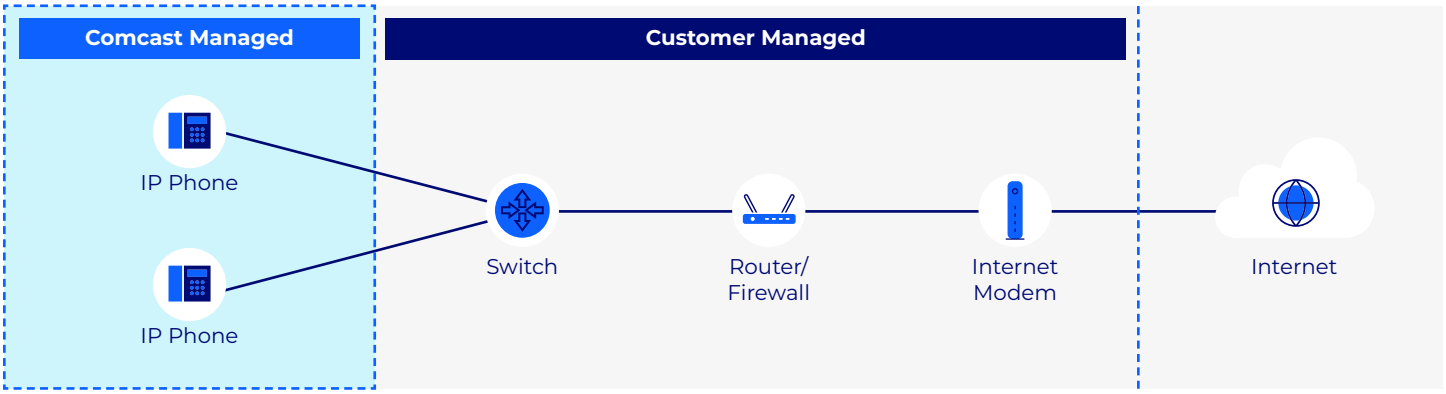
Is Business VoiceEdge OTT compatible with my internet connectivity service?

Business VoiceEdge requires certain network settings and configurations to work properly as an OTT service. You should work with your IT department or your Internet provider to troubleshoot and resolve any connectivity issues prior to your Business VoiceEdge installation. If you are using Comcast Business Internet and are experiencing issues, please contact Customer Care at (800) 741-4141 to help resolve the issue.

Business VoiceEdge OTT Basics: Wiring, Bandwidth, and Troubleshooting

Network Requirements

Business VoiceEdge IP phones must be physically connected to a network with a Cat 5 or 6 ethernet cable. IP phones cannot connect via a wireless (WiFi) network for initial setup.



Comcast Business recommends using a network switch that can provide Power Over Ethernet (PoE) to eliminate the need for a separate power adapter for each IP phone.

Dynamic Host Control Protocol (DHCP)

All Business VoiceEdge OTT equipment must be configured to obtain IPv4/Host configurations via DHCP, which allows reusable IP addresses to be dynamically assigned so that endpoints can communicate with one another on the network. You must provide a suitable DHCP server for the following Comcast Business endpoint configuration options upon bootup:

- IP Address (IPv4)
- Subnet Mask
- Default Gateway
- DNS Server(s)

Your DHCP server should be configured to NOT use Option 160 or 66.

Ports and Protocol settings

The Business VoiceEdge OTT service does not require you to expose any inbound IP addresses or ports to the public Internet, however, the following ports and protocols must be allowed to pass through to the internet.

Our current list of Business VoiceEdge OTT infrastructure protocols and associated ports for configuration are listed here:

Protocol	Transport	Port(s)	Purpose
HTTP	TCP	80	Device Provisioning
HTTPs	TCP	443	Device Provisioning
SIP	TCP	5061	SIP Signaling
Device Management	TCP	5222	Device Management
Device Management	TCP	5223	Device Management
Device Management	TCP	6800	Device Management
SIP / Device Management	UDP	5060	SIP Signaling / Device Management
Device Management	UDP	19305	Device Management
Media / Device Management	UDP	10000 – 29999	Media / Audio
Device Management	UDP	16600 – 16998	Media / Audio
DNS	UDP / TCP	53	Domain Name Service
NTP	UDP	123	Device Time Synchronization

WiFi Recommendations

An existing Business VoiceEdge OTT customer that requires a phone in a location that cannot receive wiring or has poor internet connectivity can try using a Poly WiFi USB dongle to connect your phone to the internet. Keep in mind the following:

- For use with Poly VVX 250, 350, or 450 models only
- Works with Obi WiFi 5G USB dongles
  - Customers with Poly VVX 350 or 450 models can use a USB headset in the extra USB port (side)
- LAN connection is automatically disabled when WiFi is enabled
- Network details (SSID and Password)
  - WPA2-PSK network: Enter Password
  - WPA2-Enterprise network: Enter User ID and Password
- Range plays a significant factor in voice and signaling quality. We recommend being as close as possible to your WiFi access point.

Please also note that Comcast Business cannot support or diagnose any third-party WiFi issues.

UCaaS Sessions-Specific Requirements

Network Compatibility

UCaaS Sessions requires certain network settings and configurations to work properly as an OTT service. You should work with your IT department or internet service provider to troubleshoot and resolve any network issues prior to UCaaS Sessions activation. If you are using Comcast Business Internet and are experiencing issues, please contact Customer Care at (800) 741-4141 to help resolve the issue.

The following section will help you determine if your internet network is compatible with the UCaaS Sessions service.

Network Requirements

Trunk Group Public IPv4 Address(es)

Trunks for UCaaS sessions will use public IPv4 address for each trunk group and Comcast will only signal with one (1) IP address at a time per trunk. This IP address does not need to be a public IPv4 address dedicated for the trunk and NAT is supported. Multiple trunks may also use the same public IPv4 IP address. Using multiple ISP exit paths (i.e., load balancing) could result in the blocking of VoIP traffic. IPv6 is not supported at this time.

Media anchoring at Private Branch Exchange (PBX) / Enterprise Border Session Controller (eSBC) or UCaaS Sessions

Ensure that your PBX/eSBC is the endpoint that is sending/receiving media with the Comcast session border controllers (SBCs). PBX phone < -- > PBX < -- > Comcast SBC.

Select Service Records (SRV) based on region

Select Comcast servers based on TLS protocol version and time zone / region and provision your PBX/eSBC accordingly.

Customer must provision its PBX / eSBC to resolve the Comcast SBCs based on the customer's time zone / region and TLS version for UCaaS Sessions. (e.g., TLSv1.2 / TLSv1.3). Customer will be able to select this SRV record from a published list per region. For example, a customer using TLSv1.2 in the Central Time Zone would select: tls12cent.sipott.comcast.net. The following reflects the current list of Comcast SRVs:

- **TLS Version 1.2**
  - Eastern TLS1.2 - tls12east.sipott.comcast.net
  - Central TLS1.2 - tls12cent.sipott.comcast.net
  - Mountain TLS1.2 - tls12mtn.sipott.comcast.net
  - Pacific TLS1.2 - tls12pac.sipott.comcast.net
- **TLS Version 1.3** – Not supported at this time

Application Requirements

Support SIP protocol as described in RFC 3261

Customer's PBX/eSBC must support the well-known RFC 3261 for SIP.

SIP Registration Expiry timer

Honor the SIP Registration Expiry timer (currently 180 seconds) as provided by Comcast and renew registration based on this expiry timer for UCaaS Sessions.

Failure to do so could result in missed inbound calls to customer's PBX/eSBC.

SBC Failover / Failback

Configure your PBX/eSBC to ensure failover to secondary SBC occurs upon no response or a negative response. You could also configure your PBX/eSBC to fail back to primary SBC after validating availability.

Append / Accept TGRP and Trunk-Context to Contact Header

Append Trunk Group ID (tgrp) and trunk-context to outbound messages and accept SIP messaging with tgrp/trunk-context populated.

(See REGISTER example below)

<--- Transmitting SIP request (696 bytes) to TLS:45.45.45.45:5061 --->

REGISTER sip:ott-pbx.example.comcast.net SIP/2.0

Via: SIP/2.0/TLS 75.75.75.75:5061;branch=z9hG4bKPje60ff09a-d04f-49b8-aac0-bafd74cccf24;alias

From: <sip:PUNJ-000001001@ott-pbx.example.comcast.net>;tag=b9f3e17f-9696-46e3-b405-7cf93b10eeae

To: <sip:PUNJ-000001001@ott-pbx.example.comcast.net>

Call-ID: 22fc1f2a-da05-4f9c-974e-7d03904ac11b

CSeq: 38271 REGISTER

Contact:<sip:PUNJ-000001001;tgrp=TGNJ-000001001;trunk-context=test.example.comcast.net@75.75.75.75:5061;transport=TLS>

Expires: 600

Allow: OPTIONS, INVITE, ACK, BYE, CANCEL, UPDATE, PRACK, REGISTER, SUBSCRIBE, NOTIFY, PUBLISH, MESSAGE, REFER

Max-Forwards: 70

User-Agent: FPBX-16.0.40.13(18.20.2)

Register SIP Trunk to Comcast

You must register your trunk groups using Comcast-provided SIP User and Auth User, and customer created password meeting Comcast's password requirements. SIP Trunks must be registered to Comcast in your PBX/eSBC in order to place/receive calls.

SDP Early Offer Support (SDP in initial INVITE)

Customer's PBX/eSBC should send SDP within the initial INVITE for outbound calls and accept SDP within initial INVITE for inbound calls from Comcast.

Support g.711 and/or g.722 audio codecs for media. (p-time 20ms).

Comcast only supports g.711 and g.722 for media between the customer's PBX/eSBC and Comcast SBCs. Sampling or p-time must be 20ms. Out of band (DTMF RFC2833) is supported.

Replace unknown FROM TN with known telephone number (TN) for all calls including, Operator Services and Directory Services.

Using anything other than known TNs in the From header for emergency calls (911/988) will result in forwarding to Intrado ECRC. It is highly recommended that all emergency calls have a known TN in the From header. Emergency calls will always be switched.

Security Requirements for UCaaS Sessions

Support Comcast Cipher Suites for TLS signaling

Customer must use one of the below cipher suites for TLS signaling:

- **TLS Version 1.2**
  - TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384 (Most Secure)
  - TLS_DH_RSA_WITH_AES_256_GCM_SHA384
  - TLS_DH_RSA_WITH_AES_256_CBC_SHA256 (Most compatible)
- **TLS Version 1.3**
  - (TLS Version 1.3 is not currently supported)

Support Comcast Cipher Suites for RTP media

Customer must use one of the below cipher suites for media encryption:

- AES_192_CM_HMAC_SHA1_80
- AES_128_CM_HMAC_SHA1_32
- AEAD_AES_128_GCM

PBX/eSBC must trust Digicert as a certificate signing authority or CA

Comcast SBCs will provide a Digicert signed certificate during TLS handshake with customer's PBX/eSBC.

© 2026 Comcast. CB-BVE_OTT_Customer-Reference-Guide_SLS91228-D_1.26

COMCAST BUSINESS