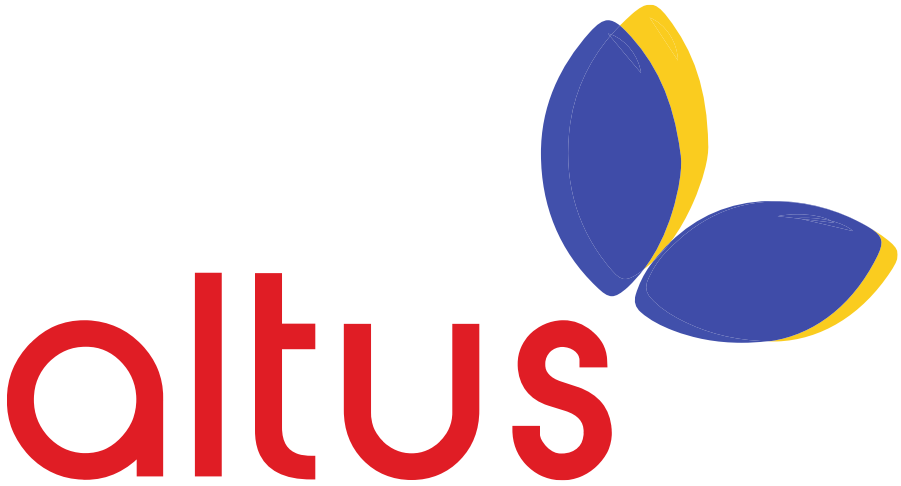

Altus UC Customer Network Minimum Requirements

Document Version 2.1

720 Cool Springs Blvd, Suite 520
Franklin, TN 37067
Tel +1 615.465.4001

WWW.ALTUSUC.COM

Requirements Summary

Customer network design and configuration has many variables, many of which can affect the performance and quality of Voice over IP (VOIP) service. For the Altus UC VOIP service to work in most customer network environments, there are a set of minimum requirements the customer network must meet to ensure service will function as expected. These requirements apply to both SIP phones and analog adapters (generally referred to from this point forward as SIP devices). Below is a summary of these requirements:

- Customer LAN must contain a DHCP server capable of providing an IP address to SIP devices when they boot.
- Customer LAN must contain a DNS server or provide DNS relay functionality to allow resolution of URL's used by SIP devices to communicate with external service platforms.
- DNS server must be capable of resolving both SRV and A records.
- Customer firewall must allow HTTP (TCP port 80) and HTTPS (TCP port 443) traffic for SIP devices to communicate with external configuration servers.
- Customer firewall must allow SIP and RTP to allow SIP devices to place and receive calls.
- Customer router must set Network Address Translation (NAT) bind timer at a value greater than or equal to 30 seconds.
- Customer router/firewall must not manipulate the SIP or RTP packets at the application layer. If any CPE devices can function as a SIP Access Layer Gateway (ALG), the ALG functionality should be disabled.
- Customer router should support Differentiated Service Code Point (DSCP) and ensure that higher priority packets take precedence over lower priority packets for all outbound packets.
- Customer router should be configured to mark all SIP and RTP packets from the Altus UC call control platforms as high priority to ensure these packets take priority over lower priority packets for all inbound packets. The Altus UC call control platforms can be uniquely identified by a set of specific IP addresses. SIP and RTP packets can be uniquely identified by the ports defined in the Firewalls section of this document.
- Customer Internet bandwidth must be sized to allow the minimum amount of required data bandwidth plus the total number of simultaneous voice calls required by the office.
- Customer Local Area Network (LAN) must be sized to allow the maximum amount of required data bandwidth plus the total number of simultaneous voice calls required by the office.

Requirements Detail

1. DHCP Server

Dynamic Host Configuration Protocol (DHCP) is a protocol used by networked devices to obtain various parameters necessary for the devices to operate in an IP network. The DHCP parameters provided by the site DHCP server that are necessary for Altus UC service to function properly are IP address, subnet mask, default gateway, and DNS server.

DHCP servers are commonly integrated into the customer's router, but they can be a stand alone server dedicated to only performing the DHCP function. For most broadband applications, the DHCP server will be integrated into the broadband router provided by the service provider. In this case, the configuration of the DHCP server (including whether or not it is on or off) can be controlled by logging into the broadband router.

All Altus UC SIP devices are configured by default to obtain IP address and DNS server information from a local DHCP server. When a SIP device is booted, it will attempt to locate the local DHCP server and obtain this information. If the customer network does not contain a DHCP server or does not provide the required information, the SIP device will not boot properly and will be unusable.

Some DHCP servers are capable of providing "options" as part of its response to a client's request. For SIP applications, Option 66 is commonly used to provide the client, in this case a SIP device, with the address of the configuration server it should contact to obtain its configuration. In the case of Altus UC service, this option is not required. All Altus UC SIP devices are hard coded to point to a specific configuration server address and if an Option 66 is received by the SIP device in response to a DHCP request, the SIP device will ignore it.

2. DNS Server

Domain Name System (DNS) is an Internet service that translates domain names into IP addresses. It provides a method of naming Internet devices with words that are easier to remember than the devices' actual numeric IP address. Also, certain types of DNS records are capable of associating a single word name with a list of IP addresses. This functionality is useful for cases in which device redundancy is used to improve performance and/or reliability.

All Altus UC SIP devices require DNS to translate domain names to IP addresses. During the boot process, the domain name of the SIP device configuration server is translated so the SIP device can locate and receive configuration information from the proper configuration server. Also, once the phone has completed the boot process, the domain name of the call control servers is translated so the SIP device can locate and communicate with these call control servers. If a DNS server is not available to provide name translation, the SIP device will not boot properly and will be unusable.

There are several types of DNS records. The Altus UC service utilizes “A” (address) and “SRV” (service) record types. “SRV” records are used to provide a mechanism of redundancy for the call control platforms. For Altus UC to function properly, both of these record types must be supported on the customer network.

3. Firewalls

A firewall is a device or set of devices in a data network configured to protect the network from potentially harmful traffic. One general function of a firewall is to permit or deny services of specific types from passing across the public network interface. One application of this functionality is to restrict the types of services users on the private network can publicly access or to restrict public access to the private network to ensure security of the network.

Firewalls can impede SIP devices from communicating with configuration servers, call control servers, network gateways, and other SIP devices. For Altus UC service to function properly, firewalls must allow the following services:

HTTP (port 80) – required for communication between the local SIP devices and the configuration servers which contain the SIP devices configuration information

HTTPS (port 443) - required for communication between the local SIP devices and the configuration servers which contain the SIP devices configuration information

SIP (port 5060) – required for communication between the local SIP devices and remote SIP devices including call control platforms, network gateways, and other SIP devices

SIP (port 8933 to 8943) - required for communication between the local SIP devices and remote SIP devices including call control platforms, network gateways, and other SIP devices. Note: This port range is not commonly associated with SIP. In this instance, it is used to avoid encounters with Application Layer Gateway (ALG) functionality that may damage the payload of SIP packets. For more information, refer to the Application Layer Gateway section of this document

RTP (ports 19560-65535) – required for communication between the local SIP devices and remote SIP devices including call control platforms, network gateways, and other

SIP devices. Note: ports 19560-65535 are not commonly associated with RTP. In this instance, they are used to avoid encounters with Application Layer Gateway (ALG) functionality that may damage the payload of RTP packets. For more information, refer to the Application Layer Gateway section of this document. With these services allowed, SIP devices should be able to properly communicate with all necessary external sources.

The ExamiNet network readiness tool is used to determine if the Altus UC service will function properly on the network being tested. For this tool and the PacketSmart device to function properly, the firewall must allow computers running the ExamiNet test and the PacketSmart device access through the customer firewall to specific IP endpoints.

A list of ports, protocols, services, destination IP addresses, and purpose of the source access is listed in section 3 of this document.

4. Network Address Translation

Network Address Translation (NAT) is a common router function which allows multiple private IP addresses on a LAN to be translated to a single public IP address on the WAN. The main reason NAT functionality exists is to conserve public IP addresses. There are not enough IP addresses within IPv4 to allow every computer connected to the Internet to have a unique public IP address. Also, NAT functionality does provide a level of security to devices with private IP addresses because those devices are not always publicly addressable.

Although necessary, NAT functionality creates issues for VOIP traffic. A typical NAT only translates IP information from private to public at the TCP/IP layer. It does not, however, translate any IP address information at the application layer. This means that any IP address information contained in the application layer payload of VOIP packets remains un-translated. Since these addresses are private, they are not routable in a public domain and are effectively unreachable. In the case of SIP, the IP address and port the SIP device wishes to advertise for establishing a connection is contained in payload of SDP attached to SIP messages. If this information is not translated, the far end will not be able to communicate with the SIP device. This usually creates a phenomenon commonly referred to as one-way RTP (voice path is only available in one direction).

Another issue with NAT functionality is that private devices are not reachable publicly unless a translation, commonly referred to as a bind, is created between the private IP address and the public IP address. This is done dynamically each time a private device attempts to communicate with a public device. The act of requesting communication causes the NAT to create a temporary bind between the private IP address requesting the communication and the public IP with which it is attempting to communicate. Bind duration is controlled by a timer which will expire and cause the bind to be removed if there is a period of inactivity on the bind equal to the length of the timer. During the

time the bind is active, public to private communication is possible, but once the bind becomes inactive, the private device is no longer publicly addressable. The most common duration for this timer is between 30 and 60 seconds. Also, binds can often be statically configured in a NAT. This functionality is often referred to as port forwarding. When this is done, the NAT is configured with a permanent bind between a private and public address.

With the Altus UC product, the challenges presented by the presence of a NAT are addressed. A technique called NAT Traversal is used to overcome the issues created by the presence of a NAT. Part of the Altus UC call control platform is responsible for maintaining constant communication with all SIP devices. This constant communication ensures that the NAT bind timer never expires, effectively making the dynamic bind permanent. Without this, a SIP device in a private network would not be able to receive calls. Also, the Altus UC call control platform uses a technique called Media Relay to overcome the issue where the NAT does not manipulate application layer information. This functionality allows the call control platform to discover the public IP address and port of the RTP stream once the SIP device sends out its first RTP packet. The call control platform performs this function on both ends of a call and bridges the two legs of the call together, effectively relaying the traffic from one device to another.

5. Application Layer Gateway

Application Layer Gateway (ALG) is a method of manipulating IP address and port information at the application layer. It is similar to NAT functionality in that it typically translates private IP and port information created by a SIP device on a private network to public IP and port information on the WAN side of the router performing the ALG function. If done properly, this functionality negates the need for Media Relay functionality because all information advertised in the application layer is publicly routable.

Although this functionality is intended to improve the processing of VOIP traffic, not all ALG devices perform the application layer translation of packets properly. In many cases, portions of the packet are modified when they should not be which causes interworking problems between the SIP device and the call control platform. When this occurs, the ALG causes the SIP device to not function properly.

With the Altus UC product, it is recommended that all ALG functionality between the SIP device and the call control platform be turned off. Doing this eliminates the potential for the ALG to improperly translate packets which could render service unusable. However, in some cases, this functionality may not be configurable. To accommodate this case, the Altus UC product uses uncommon ports for SIP and RTP traffic. Port 8933 to 8943 is used instead of 5060 which is the commonly used for SIP. Since most ALGs assume a SIP port of 5060, using

port 8933 to 8943 will typically cause the ALG to ignore the packet completely and perform no manipulation. Also, the same is done for RTP. Although not specifically defined by any specific standard, the most common port range used for RTP is 16384-16482. To avoid the potential for ALG interaction, the Altus UC product uses RTP ports 19560-65535.

6. Quality of Service Settings

Quality of Service (QOS) refers to the ability to provide different priority to different applications over a data network connection to ensure higher priority traffic takes precedence over lower priority traffic. A voice conversation is real-time and traffic associated with a voice call must process efficiently or issues such as clipping or choppy audio will occur. On the other hand, normal Internet traffic is best-effort. If packets are dropped or delayed, service is usually not noticeably disrupted. As a result, voice traffic generally is considered to be higher priority traffic than data traffic.

The Altus UC product utilized Differentiated Services Code Point (DSCP), also commonly referred to as DiffServ, as the mechanism for marking packet priority. Each SIP device automatically sets every packet it sends as high priority. However, this does not ensure that all data network equipment in the traffic path will honor the setting and ultimately allow voice traffic to take priority of data traffic.

To ensure voice packets take priority over data packets, customer routers must be properly configured to handle DSCP. This functionality is sometimes referred to as Class of Service (COS) or priority queuing. In either case, it is recommended that the router be configured with strict priority queuing allowing packets marked with higher DSCP values to have higher priority. If this is not done properly, perceived call quality could noticeably deteriorate during peak traffic times.

Also, packets set with high priority by SIP devices only addresses traffic sent from the SIP device to other devices outside of the customer's network. It does not address packets inbound to the SIP device. These packets are normally not marked with a higher priority when received by the customer's router because priority values are normally not maintained across a WAN. As a result, without additional configuration these packets will not be prioritized over normal data traffic. To accommodate this case, it is recommended that priority rules be established to allow all inbound SIP and RTP traffic to have higher priority than all other traffic. The specific ports associated with SIP and RTP are defined in the Firewall section of this document. It may also be necessary to define the IP addresses of the Altus UC call control platforms to have higher priority over all other traffic. A specific list of these IP addresses is not defined in this document because they are currently subject to change. IP address prioritization is required for a specific customer application, the unique IP addresses that must be provisioned will be provided upon request.

8. Internet Bandwidth

Internet bandwidth is the amount of capacity available for Internet traffic on a customer's network. This amount is determined by the service provided by the Internet Service Provider. The amount of bandwidth available will determine the amount of simultaneous voice calls and data traffic that the Internet connection will support. If properly sized and with the proper QOS settings in the customer router, the Altus UC service will function properly. However, if undersized or if QOS is not provisioned correctly, perceived call quality could noticeably deteriorate during peak traffic times. The following information provides information and guidelines for properly sizing voice service for a given Internet bandwidth. To determine the number of phones that can be supported over a given bandwidth, the maximum number of simultaneous calls that can be supported must first be calculated using one of the following formulas. There are two calculations that must be completed:

Worst Case Calculation (No Compression)
Max Calls = Available Voice Bandwidth (Kbps) / (SimCalls * 80Kbps)

Where,

- Available Voice Bandwidth (Kbps) – is the maximum amount of bandwidth allowed for voice traffic. This value is equal to the lower of the connection download and upload speeds minus an amount reserved for processing data traffic. Offices with routers provisioned to prioritize voice traffic over data traffic can process voice calls at up to 100% of total connection bandwidth without jeopardizing call quality. However, at sustained high call volumes, data traffic quality will be impacted. As a result, it is recommended that calculations for maximum calls and maximum phones be done assuming only a portion of the overall bandwidth can be used for voice traffic.
- SimCalls – the number of simultaneous calls coming out of a site
- 80Kbps – is the bandwidth required for a fax/modem call

Best Case Calculation (With Compression)
Max Calls = Available Voice Bandwidth (Kbps) / ((Phone * 24Kbps)+(Fax * 80Kbps))

Where,

- Available Voice Bandwidth (Kbps) – is the maximum amount of bandwidth allowed for voice traffic. This value is equal to the lower of the connection download and upload speeds minus an amount reserved for processing data traffic. Offices with routers provisioned to prioritize voice traffic over data traffic can process voice calls at up to 100% of total connection bandwidth without jeopardizing call quality. However, at sustained high call volumes, data traffic

quality will be impacted. As a result, it is recommended that calculations for maximum calls and maximum phones be done assuming only a portion of the overall bandwidth can be used for voice traffic.

- Phone – the number of simultaneous phone calls with compression coming out of a site
- 24Kbps – is the bandwidth required for a phone call with compression
- Fax – the number of simultaneous fax calls (no compression) coming out of a site
- 80Kbps – is the bandwidth required for a fax/modem call

There are certain call flows in the BroadCloudPBX service that do not support compression, such as calls to Voice Mail or to the Conferencing service. Therefore, the actual amount of bandwidth required will vary between the best and worst case calculations.

The maximum number of phones that can be supported over a given bandwidth can now be calculated using the following formula:

Max Phones = Max Calls * Users per Simultaneous Call

Where,

- Max Calls – is the amount of simultaneous calls that can be supported over the given bandwidth
- Users per Simultaneous Call – is a statistical approximation of the total number of users that can share one call path with non-blocking results. The value of 4 is recommended for average office usage. However this number could vary drastically depending on the type and size of office.

The following two tables provide estimates for two different office applications. The first provides estimates for an average usage office, and the second provides estimates for a high usage office. The actual values for a give office application will vary depending on actual usage requirements.

	Maximum Simultaneous Calls			Maximum Phones		
Bandwidth	Phones Only	Fax Only	9:1 Mix	Phones Only	Fax Only	9:1 Mix
DSL (128K)	3	0	0	12	0	0
DSL (384K)	9	2	7	36	8	28
DSL (512K)	12	3	10	48	12	40
DSL (768K)	19	5	15	76	20	60
T1	39	11	31	156	44	124

*assumes 60% of total bandwidth is available for voice and 4 users per simultaneous call

Table 1: Average Usage Office

	Maximum Simultaneous Calls			Maximum Stations		
Bandwidth	Phones Only	Fax Only	9:1 Mix	Phones Only	Fax Only	9:1 Mix
DSL (128K)	2	0	0	4	0	0
DSL (384K)	8	2	6	16	4	12
DSL (512K)	10	3	8	20	6	16
DSL (768K)	16	4	12	32	8	24
T1	32	9	26	64	18	52

*assumes 50% of total bandwidth is available for voice and 2 users per simultaneous call

Table 2: High Usage Office

Note 1: Offices with routers provisioned to prioritize voice traffic over data traffic will be able to process more voice calls without jeopardizing call quality. However, if call volumes are extremely large, data traffic quality could be impacted. As a result, we recommend that bandwidth engineering be done considering only a portion of the overall bandwidth being available for voice traffic.

Local Area Network Bandwidth

Local Area Network (LAN) Bandwidth is the amount of capacity a customer's internal network can support. This amount is determined by the throughput specification of the LAN infrastructure. In most customer applications, the LAN infrastructure is a single layer 2 switch. The amount of bandwidth available will determine the amount of simultaneous voice calls and data traffic that the LAN will support. If properly sized, the Altus UC service will function properly. However, if undersized, perceived call quality could noticeably deteriorate during peak traffic times. It is the customer's responsibility to ensure that their internal network is sized properly to support the addition of VOIP to their network.