Voice and Collaboration

SIP Trunking

SIP Trunking Quick Start Guide

Overview

We are confident that our SIP based service will increase your organization's performance and productivity while keeping your costs under control. Summarized below is some important technical information that you or your integrator must know regarding how SIP Trunking works, and the parameters that your equipment needs to adhere to in order to effectively work with the service. If you have any further questions or require assistance, please contact your Account Representative.

Customer Deliverables

In order for us to provide the best service possible, it will be important for you, the customer, to provide the following information:

Static IP or IP Addresses: As an additional customer verification method, Allstream ensures that SIP Signaling matches the customer IP address. If you are purchasing Internet from Allstream, our technician will provide this information to you.

Codec and DTMF Combination: To ensure proper network inter-working please choose from one of the following Codec and DTMF Combinations:

Codec and DTMF Combination	Codecs	DTMF
G.711; In-Band DTMF only	G711µ	RTP Stream
G.711; RFC2833 DTMF only	G711µ	RFC2833
G.711 & G.729; RFC2833 DTMF only	G711µ, G729	RFC2833

- Allstream cannot guarantee use of G.729 for all calls, in-order for this codec to be used, all parties (including other carriers) in the call path must allow the G.729 codec
- Recommended bandwidth allowance is 100 kbps per simultaneous call to accommodate for G.711 requirements
- The use of the G.729 codec requires that all DTMF signaling be passed via RFC2833 (out-of-band)

SIP Trunk Standards

End Points

Here are a few examples of SIP endpoints, suitable for using the Allstream Network:

- IP PBX Appliances
- VoIP/Fax Gateways
- Voice Enabled Servers
- Virtual Machine IP PBXs
- Call and Contact Centers
- Enterprise Session Border Controllers
- Collaboration and Unified Communications

The Allstream voice network is designed, optimized, and built only for 'conversational traffic'. Any potential customer's traffic not meeting this requirement is unacceptable on Allstream's voice network (e.g., robocallers, auto dialers, excessive call attempts, excessive short duration calls, excessive unanswered calls).

Requirements

Allstream allows a degree of flexibility within the SIP product suite. The following bullet points provide specific details about our standards for the SIP trunk product:

- Customers will use a static IP on their SIP Endpoint or Endpoints
- Registration with Digest Authentication (DA) is mandatory in the US
- DA credentials are mandatory in the US; each outgoing INVITE from a SIP Endpoint is met with a '401 Unauthorized' challenge
- Allstream does not respond to or accept '401 Unauthorized' challenges when sending INVITES toward/to the SIP Endpoint
- An FQDN for the Allstream Session Boarder Controllers (SBCs) must be used; an IP address instead of FQDN for the SBC is not recommended and cannot guarantee connectivity
- T.38, V.17 (G3 at 14.4kbps max) fax is supported and is the Allstream standard, *please note, T.38 requires end to end compatibility and is not guaranteed*
- 10-digit, 11-digit, and 011 outbound dialing patterns are supported
- SIP INFO DTMF is currently not supported
- RFC-2833 DTMF is supported and the Allstream standard, note that this can also be changed to inband DTMF if needed for the SIP Endpoint
- Recommended voice codec order is G.711µ primary with optional G.729a secondary upon request, *please note that the use of G.729a requires RFC-2833 for ALL calls, additionally G.729a requires end to end compatibility and is not guaranteed*
- Allstream sends OPTIONS messages on SIP trunks every 30 seconds as a keep-alive method: any response is accepted; no response will result in call failures and an OOS trunk

SIP Security Recommendations

A VoIP switch is a crucial component of your business that requires attention to ensure its operation and availability are not impacted by hackers, hacktivists, competitors and others attempting to gain access to free services or disrupt the services you have.

Customers are responsible for any charges incurred due to toll fraud, which can occur when a party gains unauthorized access to a Customer's PBX system. Review Allstream's current Toll Fraud Policy at: **support.allstream.com/knowledge-base/toll-fraud-policy.**

Some tips to prevent toll fraud or other unauthorized access to your system are listed below, but it is critical that you work with your PBX system provider to determine your points of vulnerability and build a strategy that can help protect you.

Administration

- Remove any direct external (public/internet) access to administration features
- Use complex non-dictionary passwords
- Change passwords regularly
- Ensure external/public admin access is only available via secure (IPsec, VPN, SSL, etc.) authenticated connection to the firewall or other security device

Internet Access

- Enable firewall features on PBX if available
- Add or connect to the Internet via a stateful firewall or SBC
- Add filters to only allow connectivity to and from SIP provider

System

- Disable unused services where applicable
- If Wireless is available, use WPA2 with complex passwords
- Monitor system regularly for fraud

Operations

- Upon deployment, scan your Internet presence (i.e. IP range) for vulnerabilities
- Repeat vulnerability scans regularly
- Patch and secure the PBX as recommended by the manufacturer

Remote Users

- Cell phones/tablets to have automatic lockouts to prevent fraudulent use if lost or stolen
- Laptops are to have screen lockout and drive encryption where possible
- Limit remote user capabilities such as forwarding features
- Where possible, encrypt voice connections to reduce unauthorized monitoring

LAN Configuration

When moving to a converged environment running both voice and data over IP, your LAN environment must be prepared to carry real-time voice traffic. This preparation typically focuses on two key areas:

1. Establishment of Virtual LANs (VLANs) for voice traffic
2. Establishment of Class of Service (CoS) handling for voice traffic

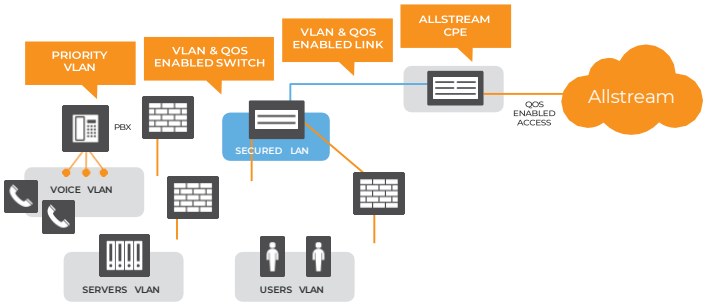

Figure 1: LAN environment using virtual LANs and Class of Service

It is highly recommended to separate voice and data packets into distinct VLANs within the LAN environment. This improves utilization of system resources by reducing broadcast traffic and prevents possible congestion conditions of one traffic type from affecting other traffic. Not utilizing VLANs may result in poor voice quality, high packet loss, client to server communication issues, and lost call control.

Additionally, we recommend the use of Class of Service (CoS) marking for traffic in the LAN when preparing for a VoIP implementation. Layer 2 Ethernet switches must support the IEEE 802.1p standard to provide CoS. This standard is part of the IEEE 802.1Q (IEEE, 2005) which defines the architecture of virtual bridged LANs (VLANs). CoS allows switches to distinguish packets and packet flows from each other, assigning labels to indicate the priority of packets. CoS enables packets to comply with configured resource limits and provides preferential treatment in situations where resource contention occurs. Without CoS enabled in the LAN switch, bandwidth contention may contribute to packet loss and latency resulting in poor VoIP performance.

Environment set-up for SIP Trunking over Internet

SIP trunking over 3rd Party Internet Access allows the customer to use their existing Internet connectivity for Allstream Voice Services. The illustration in figure 1 above is a basic representation of the connectivity between Allstream and the customer's PBX. Allstream recommends that the customers always protect their SIP Network by using an SBC or other device to prevent unwanted access to the customer's network.

PBX Connectivity Set-Up

The Allstream SIP Trunking product supports the following three configurations for Customer LAN deployments:

Configuration 1: PBX Connectivity using Public IP – no NAT

In this scenario, the PBX or VoIP equipment is accessible via the public Internet. The customer is not using NAT for VoIP traffic, so no NAT compensation occurs between the Allstream SBC cluster and the customer PBX. The following diagram is an illustration of this scenario.

The public IP address used by the customer must be static, and the ISP assigns the subnet. The IP address and subnet information of the Allstream-facing VoIP equipment is required as part of the SIP Trunking Internet order.

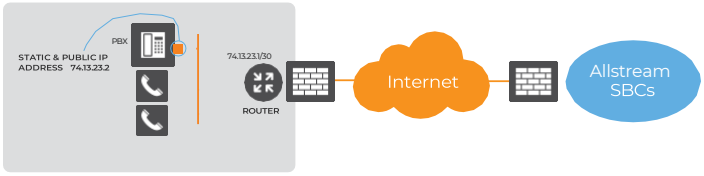

Figure 2: PBX Connectivity using Public IP - no NAT

Configuration 2: PBX Connectivity using NAT with Application Layer Gateway (ALG)

Some customers may deploy an Application Layer Gateway (ALG). The primary purpose of an ALG is to manipulate or translate IP address information in the application layer. More specifically, the function of the ALG would replace the private IP address in the SIP Invite and SDP message with the NAT'd public IP address for any outgoing traffic. Similarly, for any incoming traffic from the PSTN to the customer network, the ALG would replace the public IP address information in the SIP Invite and SDP with the private IP address information. In this configuration, the static public IP address of the Allstream-facing router (in this example 74.13.23.1) is required as part of the Allstream with the SIP Trunking Internet order.

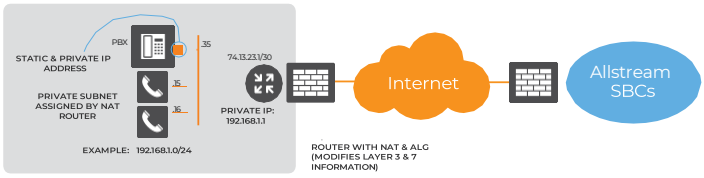

Figure 3: PBX Connectivity using NAT with ALG

Configuration 3: PBX Connectivity using NAT without ALG

In this configuration, the customer does not have their own ALG, and uses a router that performs NAT at layer three. All outgoing (private) traffic is NAT'd to a public IP address assigned by the customer's ISP (typically the IP of the WAN Interface on the router, or an unused IP address in the provided block). For this configuration, the private IP of the customer PBX (in this example 192.168.1.35) is required as part of the Allstream order, this allows the Allstream SBC to communicate with the PBX. Therefore, both the static public IP address of the Allstream-facing router (in this example 74.13.23.1) AND the static private IP address of the VoIP equipment is required as part of the SIP Trunking Internet order.

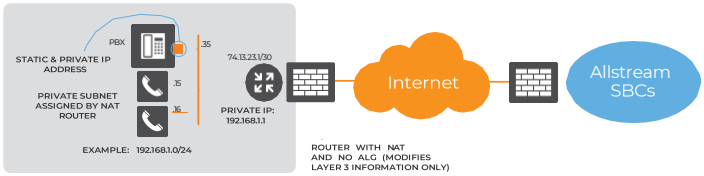

Figure 4: PBX Connectivity using NAT without ALG

Firewall Set-Up

If your environment is protected from the Internet by a firewall, settings must be configured on your firewall to allow for the SIP Trunking signaling and media to pass through.

- Adjust firewall settings to allowing signaling and media from the Allstream SBC at the IP address ranges provided by your account rep or Allstream technician
- Allow for SIP signaling utilizing UDP on port 5060
- Allow for TLS signaling utilizing TCP on port 5061
- Allow for RTP/SRTP media utilizing UDP on ports 10000 to 65535

Environment set-up for Private SIP Trunking

Allstream SIP Trunking platform allows for dedicated SIP Trunks established over private connections. The customer's SIP traffic uses a separate VLAN for traffic to and from the SBC. Each customer's SIP traffic stays private through dedicated VRFs /VLANs.

PBX Connectivity Set-Up

The Allstream SIP Trunking product supports the following three configurations for Customer LAN deployments:

Configuration 4: PBX Connectivity via Private IP VPN Network

In this configuration, the PBX communicates with the Allstream SBC over a private connection. This arrangement is similar to Configuration 1 for SIP Trunking over Internet above, since no NAT is required, and all addressing is contained in a private customer VPN. Customer LAN addressing is statically assigned or assigned via DHCP.

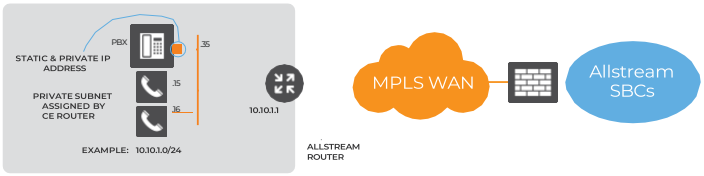

Figure 5: PBX Connectivity via Private IP VPN Network

DHCP Considerations

VoIP requires that all endpoints including phones have unique IP addresses. When using NAT, the customer must ensure that all endpoints have either static IP addresses or addresses via Dynamic Host Configuration Protocol (DHCP) within the LAN environment. Allstream does not provide DHCP services from the CE router. If the customer is not using NAT (using public addresses for the VoIP network), ensure that all SIP endpoints, which will communicate directly with Allstream SBCs, are assigned static IP addresses within the subnet provided by the ISP.

Programming the IP PBX

Refer to the manufacturer's documentation for specific instructions on how to program and configure your IP PBX. Allstream can provide configuration guides for equipment pre-certified with Allstream SIP Trunking. Speak to your Sales Engineer for more details.

Ensure that you program your IP PBX to use one of the codec combinations in the Codec and DTMF Combinations table on page 1. Remember, Allstream recommends allowing 100 kbps bandwidth per simultaneous call to accommodate for G.711 codec requirements. Failure to do this may result in call degradation due to bandwidth congestion.

Please note the following dialing parameter requirements:

- For Single-State and Non-Extended Voice services the PUC Mandated dialing plan is followed
- For Multi-State and Extended Voice services, the PBX programming is required to outpulse either 10 digits (NPA-NXX-XXXX) or 11 digits (1+NPA+NXX-XXXX) for North American calls as desired

SIP and Media Specifications

SIP Signaling Specifications

Protocol	SIP – RFC 3261
Transport	UDP – port 5060, TCP – port 5061
Caller ID	• P-Asserted-ID header (as per RFC3325) • A valid 10-digit Caller Identification must be sent
Caller ID Blocking	Privacy ID header (per RFC3325)
Supported SIP Methods	• ACK, BYE, CANCEL, INVITE, OPTIONS, INFO, NOTIFY, PRACK, UPDATE • SIP Headers: a) P-Asserted-ID per RFC3325 b) Privacy • Re-Invite to 0.0.0.0 or a=send only are supported for on-hold
SIP Authentication	Requires Registration with Digest Authentication (US) and IP Match (US and Canada)
Other Service Characteristics	• Early SDP • INVITE without SDP • Unknown header: "Unknown" • Anonymous header: "Anonymous" • Supported Extensions: 100rel, timer
Error Condition Treatment	• Unassigned Number - SIP 404 (no audio message) • SIP sessions Max out – SIP 503 • Voice codec P-time miss-match - SIP 488 • Session-Expires header is too small - SIP 422
Signaling Parameters	• maxSipMsgSize: 2048 • Session timer: MIN-SE 600 • Session timer: Session Expire (default): 3600 • retransmissionT1: 500 • retransmissionT2: 4000 • retransmissionT4: 5000
QoS	DiffServ: DSCP for signaling is CS3/24 (real-time class)
SIP REFER	Yes

Media Specifications

Protocol	RTP – RFC1889, RFC3264
Transport	UDP – port range • 10000 to 65535
DTMF Support	RTP In-band and via RFC2833
Codecs	• G.711a/μ: 20ms frame size • G.722 (AVT payload 9): 20ms frame size • G.729: 8 Kbps, 20ms frame size
Network Transcoding	No
Voice Activity Detection	No
Early Media Support	Yes
Fax	G.711 pass-through, T.38 with G.711 fallback
QoS	DiffServ: DSCP for media is EF/46 (real-time class)

Service Features

99.999% VOIP core network reliability
Extended DID number
TN (Telephone Number) porting
Trunk Overflow to TN – Call Redirection and Failover
Trunk Failover to TN – Call Redirection and Failover
Multi-endpoint failover – Business Continuity
Multi-endpoint overflow – Business Continuity
Traffic Load-Sharing (Maximum 2 endpoints) – SIP Pooling
Call Routing
E911 service
Repair Service 611
Telecommunications Relay Service (TRS) 711
Regional 211, 311, 511, and 811 calls
Account codes by call type (Operator, Premium, International, etc.)
Call Barring