SIP Trunking – Customer Overview

AN ALLSTREAM WHITE PAPER

Table of Contents

Welcome 1

SIP Security Recommendations 1

Prepare Your LAN for VoIP 2

Environment Setup for SIP Trunking Over Internet (Allstream or Third-Party) 2

- PBX Connectivity Set-Up 3
- Firewall Set-Up 4

Environment Setup for SIP Trunking Over MPLS VPN 4

- PBX Connectivity Set-Up 4
- DHCP Considerations 4

Programming the IP PBX 5

- SIP Specifications 5
- RTP Media Specifications 6

About Allstream 7

Welcome

We are confident that our service will help increase your organization's performance and productivity while keeping a lid on your costs.

Summarized below is some important technical information that you or your integrator must know regarding how SIP Trunking works, and parameters that your equipment needs to adhere to in order to effectively work with the service. Please ensure that your equipment is configured to support these parameters. If you have any further questions or require assistance, please contact your Account Representative and again, Welcome to Allstream!

SIP Security Recommendations

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

It's essential that the PBX manufacturer's hardening recommendations be followed when connecting your PBX to public or Internet resources such as SIP trunks or phones. Included are some initial recommendations. Suffice it to say that connecting your PBX directly to the Internet without a firewall or SBC (Session Border Controller) is not manufacturer recommended except for the very few PBX's that come equipped with such capabilities. Doing so will most likely result in possible fraudulent long distance charges as well as costly professional services to properly re-configure or re-install and harden the PBX.

Administration

- Remove any direct external (public/internet) access to administration features
- Use complex non-dictionary passwords
- Change passwords every quarter
- Ensure external/public admin access is only available via secure (IPSec, SSL-VPN, 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
- Change passwords every quarter
- Add filters to only allow connectivity to and from SIP provider

System

- Disable unused services where applicable
- If Wireless is available used WPA2 with complex password
- Monitor system regularly for fraud

Operations

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

Remote Users

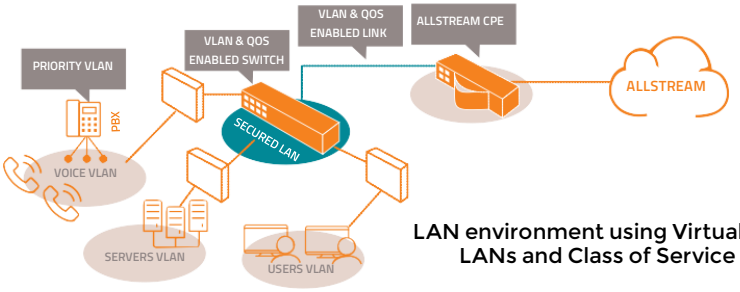
- Cell phones/tablets to have automatic lockouts to prevent fraudulent use if lost or stolen
- Laptops are to have screen lockout and drive encryption where possible
- Limit remote user capabilities such as forwarding features
- Where possible encrypt voice connections to reduce unauthorized monitoring

Prepare Your LAN for VoIP

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:

- **Establishment of Virtual LANs (VLANs) for voice traffic, and**
- **Establishment of Class of Service (CoS) handling for voice traffic**

It is highly recommended that voice and data packets be separated 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.



LAN environment using Virtual LANs and Class of Service

Use of Class of Service (CoS) marking for traffic in the LAN is also recommended 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 voice performance.

Environment Setup for SIP Trunking Over Internet (Allstream or Third-Party)

For Canada Customers connecting over Internet	
SBC Signaling & Media IP	
Markham	Calgary
74.216.209.10	172.110.72.60

For US Customers connecting over Internet	
Portland SBC	Salt Lake SBC
FQDN	FQDN

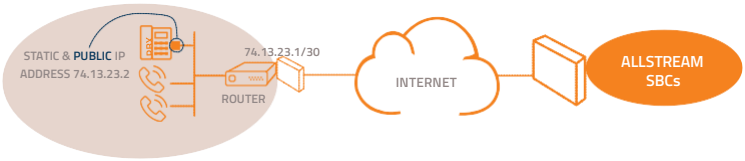
PBX Connectivity Set-Up

The following three configurations are supported for Customer LAN deployment with Allstream SIP Trunking:

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.

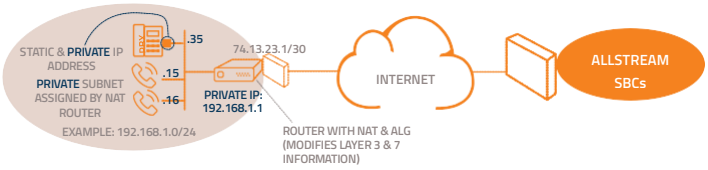
The public IP address used by the customer must be static, and the subnet is assigned by the ISP. The IP address and subnet information of the Allstream-facing VoIP equipment must be provided as part of the SIP Trunking Internet order.



PBX Connectivity using Public IP – no NAT

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

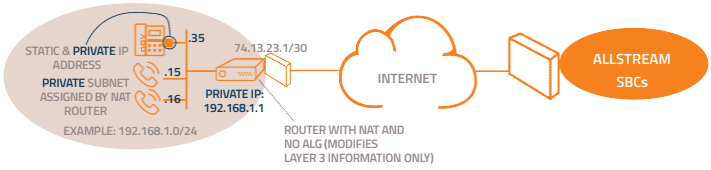
Some customers may deploy an Application Layer Gateway (ALG). The primary purpose of an ALG is to manipulate or translate IP address information in the application layer. More specifically, the function of the ALG would replace the private IP address in the SIP Invite and SDP message with the NAT'd public 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) must be provided to Allstream with the SIP Trunking Internet order.



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) must also be provided to Allstream in order for 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 must be provided as part of the SIP Trunking Internet order.



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 SIP Trunking signaling and media to pass through:

- **Adjust firewall to allow signaling and media to be received from the Allstream Session Border Controller at the IP address ranges provided in section above**
- **Allow for SIP signaling utilizing TCP/UDP on port 5060**
- **Allow for RTP media utilizing UDP on ports 16384 to 64000**

Environment Setup for SIP Trunking Over MPLS VPN

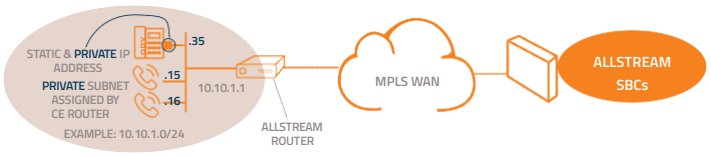
Allstream's SIP Trunking platform comprises of two fully redundant pairs of SBCs located at geographically diverse locations (Markham and Calgary) and dedicated for SIP Trunks established over MPLS VPN. This architecture provides unparalleled robustness, reliability and security. Each SBC appears like another site in the customer VPN. Public IP addresses assigned for the SBC SIP interface are not advertised and are not accessible over public Internet. Each customer's SIP traffic over MPLS stays totally private through dedicated VRFs / VLANs.

For Customers connecting over MPLS	
SBC Signaling & Media IP	
Markham	Calgary
172.110.64.132	172.110.73.228

PBX Connectivity Set-Up

PBX Connectivity via Private IP VPN Network

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



PBX Connectivity via Private IP VPN Network

DHCP Considerations

VoIP requires that all endpoints including phones are assigned unique IP addresses. When using NAT, customer must ensure that all endpoints are assigned 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 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 that is pre-certified with Allstream SIP Trunking. Speak to your Sales Engineer for more details.

Ensure that you program your IP PBX to use the same voice codec that you used when calculating required bandwidth for your order. Failure to do this may result in call degradation due to bandwidth congestion.

Please note the following changes for all new SIP Trunking installations after August 2013:

- **Outgoing calls from the IP PBX no longer require any digit prefixing based on rate centre**
- **The PBX may be programmed to outpulse either 10 digits (NPA-NXX-XXXX) or 11 digits (1+NPA+NXX-XXXX) for North American calls as desired**
- **Local calls to 211, 311, 511 and 811 municipal services will not be supported. For any calls to these services, the IP PBX must be programmed to outpulse the appropriate local telephone number**

SIP Specifications

SIP Signaling	
Protocol	SIP – RFC 3261
Transport	UDP – port 5060
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: P-Asserted-ID per RFC3325 Privacy • Re-Invite to 0.0.0.0 or a=send only are supported for on-hold
SIP Authentication	Session border controller authenticates the customer PBX by using the PBX's static IP address
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) • 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 CS5 (real-time class)
SIP Authentication (*US Customers Only*)	Requires both Registration with Digest Authentication and IP Match

RTP Media Specifications

RTP Media	
Protocol	RTP – RFC1889
Transport	UDP – port range • 16000 - 64000
DTMF Support	RTP In-band and via RFC2833
Codecs	• G.711A/μ: Frame (packet) time: 20ms (50 packets per second) • G.729: 8 Kbps, 20ms frame size
Voice Activity Detection	No
Early Media Support	Yes
Fax	G.711 pass-through, T.38
QoS	DiffServ: DSCP for media is EF (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
Traffic Load-Sharing – SIP pooling
Call Routing
Local Directory Services (411) Repair
Service 611
Telecommunications IP Relay Service
Call Barring

About Allstream

Allstream is a leader in business communications throughout North America. Founded over 170 years ago in parallel with Canada's first transcontinental railroad, Allstream continually re-invented itself to remain a leading provider of business communication services. Allstream's offerings include a range of innovative, highly scalable, managed services voice, internet and connectivity solutions for enterprise customers. We combine scalable solutions with exceptional customer service to deliver the latest technology, and we're positioned to help our customers accelerate into the future.

Allstream is the creator of powerful, software-defined wide-area networks (SD-WANs) for the most challenging locations requiring high availability and business-critical application traffic. For more information, visit: **www.allstream.com**.