Guide de démarrage rapide – Lignes groupées SIP NGN

Nous sommes convaincus que notre service aidera votre entreprise à accroître son rendement et sa productivité tout en maîtrisant les coûts. Vous trouverez ci-après un résumé de certains faits techniques importants que vous ou votre intégrateur devez savoir sur le fonctionnement des lignes groupées SIP NGN, ainsi que les paramètres à respecter afin que votre équipement soit efficace dans le cadre du service. Veuillez vous assurer que votre équipement est configuré de manière à être compatible avec ces paramètres. Si vous avez des questions ou souhaitez obtenir de l'aide, veuillez communiquer avec votre représentant commercial.

Recommandations liées à la sécurité des services SIP NGN

Un commutateur VoIP (voix sur IP) est un élément primordial de votre entreprise qui, tout comme un serveur conservant des données essentielles, doit recevoir une attention particulière pour s'assurer que son exploitation et sa disponibilité ne sont pas mises en péril par des pirates, des cybermilitants, des concurrents ou d'autres acteurs indésirables qui tentent d'accéder à des ressources gratuitement ou de nuire à vos services.

Il est essentiel de suivre les recommandations de renforcement du fabricant de PBX lorsque vous raccordez votre PBX à des ressources publiques ou sur Internet, comme des circuits ou des téléphones SIP NGN. Le présent document présente certaines recommandations fondamentales. Inutile de dire que raccorder un PBX directement à Internet sans pare-feu ni contrôleur SBC (contrôleur de session en périphérie) n'est pas recommandé par les fabricants, sauf dans le cas d'une minorité de PBX dotés de fonctions de sécurité. Une telle erreur conduira vraisemblablement à une utilisation frauduleuse de vos services interurbains et nécessitera de recourir à de coûteux services professionnels pour reconfigurer ou réinstaller adéquatement le PBX et pour le renforcer.

Administration

- Retirez tout accès extérieur direct (public/Internet) aux fonctions d'administration.
- Utilisez des mots de passe complexes introuvables dans des dictionnaires.
- Modifiez les mots de passe aux trois mois.
- Veillez à ce que l'accès extérieur/public aux fonctions d'administration ne soit possible que par le biais de connexions sécurisées (IPSec, RPV SSL, etc.) avec authentification établies avec le pare-feu ou tout autre dispositif de sécurité.

Accès Internet

- Activez les fonctions de pare-feu du PBX, s'il en est doté.
- Établissez les liaisons à Internet par l'intermédiaire d'un pare-feu ou d'un contrôleur SBC dynamique.
- Ajoutez des filtres n'autorisant le raccordement qu'avec les systèmes du fournisseur de services SIP NGN.

Systèmes

- Désactivez les services inutilisés si vous en avez.
- Si vous offrez un accès sans fil, mettez en place un accès Wi-Fi protégé par WPA2 avec mot de passe.
- Surveillez régulièrement les systèmes pour déceler tout signe de fraude.

Exploitation

- Après la mise en œuvre, vérifiez par balayage la présence de toute faille dans vos liaisons Internet (plages d'adresses IP).
- Répétez les balayages de détection des failles aux trois mois.
- Appliquez les correctifs au PBX et sécurisez-le conformément aux recommandations du fabricant.

Utilisateurs distants

- Les téléphones cellulaires et les tablettes électroniques doivent se verrouiller automatiquement pour empêcher toute utilisation frauduleuse en cas de perte ou de vol.

- L'écran des portables doit être verrouillé et les lecteurs doivent être dotés d'un logiciel de chiffrement dans la mesure du possible.
- Limitez les fonctions d'utilisation à distance comme le renvoi automatique.
- Lorsque c'est possible, chiffrez les liaisons de voix afin de réduire le risque d'écoute non autorisée.

1 Préparation du RL pour les services VoIP

Lorsque vous passez à un environnement convergent regroupant voix et données sur une même liaison IP, votre réseau local (RL) doit être bien préparé pour être en mesure d'acheminer un trafic de voix en temps réel. Les mesures de préparation portent généralement sur deux aspects clés :

1. Établissement de RL virtuels (RLV, ou VLAN en anglais) pour le trafic de voix; et
2. Établissement de classes de service (CoS) pour acheminer le trafic de voix.

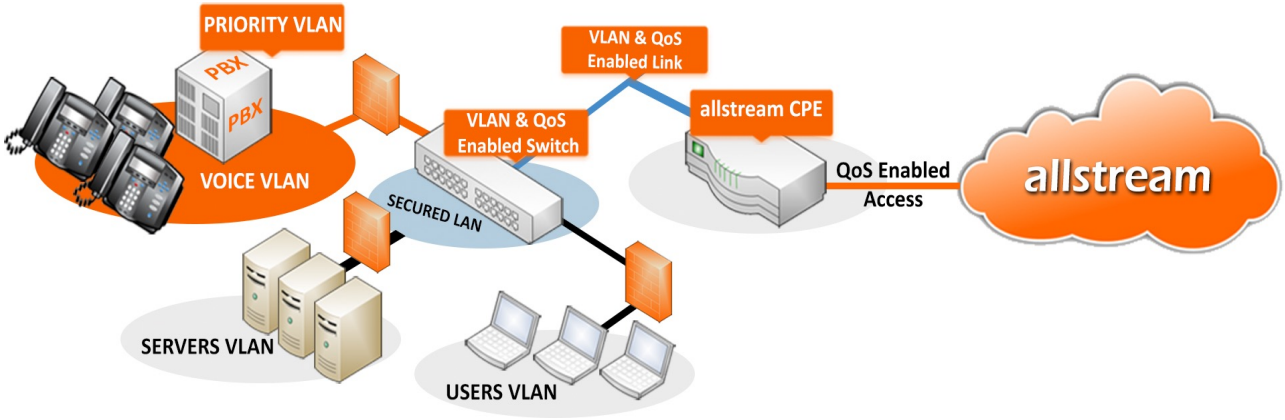

Figure 1 : Environnement de RL utilisant des RLV et des classes de service

Il est fortement recommandé de séparer les paquets de voix et de données en deux RL virtuels au sein de l'environnement du RL. De cette façon, vous améliorez l'utilisation des ressources du système en réduisant le trafic de diffusion et vous réduisez le risque que des états de congestion touchant un type de trafic ne se répercutent sur l'autre. Au contraire, ne pas recourir à des RLV peut entraîner une qualité d'appel médiocre, une perte de paquets élevée ainsi que des difficultés de communication client–serveur et de gestion des appels.

L'emploi de classes de service (CoS) pour l'étiquetage du trafic dans le réseau local est également recommandé lorsque la mise en œuvre de la technologie VoIP est envisagée. Les commutateurs Ethernet de couche 2 doivent être compatibles avec le protocole IEEE 802.1p afin de fournir les classes de service. Ce protocole fait partie de la norme IEEE 802.1Q (IEEE, 2005), qui définit l'architecture des RL à ponts virtuels (RLV, ou VLAN en anglais). Les classes de service (CoS) permettent aux commutateurs de distinguer les paquets et les flux de paquets les uns des autres en leur attribuant des étiquettes désignant leur niveau de priorité. Les classes de service permettent d'acheminer les paquets en respectant les limites de ressources qui sont configurées et accordent un traitement par ordre de priorité lorsqu'il y a concurrence pour l'utilisation des ressources. Si la fonction de classes de service du commutateur n'est pas activée, la concurrence pour la largeur de bande peut augmenter la perte de paquets et la latence, ce qui se traduit par un rendement médiocre des services VoIP.

2 Paramétrage de l'environnement des lignes groupées SIP NGN par Internet

L'architecture des services de lignes groupées SIP NGN offre la fiabilité accrue de liaisons géographiquement redondantes. Les clients en bénéficient en configurant le PBX IP pour qu'il se raccorde à un serveur mandataire SIP NGN principal (contrôleur de session en périphérie SBC d'Allstream) et à un serveur mandataire SIP NGN secondaire (un contrôleur SBC situé dans un lieu physique différent). Les clients situés en Ontario et plus à l'est utilisent le contrôleur SBC de Markham comme interface principale et le contrôleur SBC de Calgary comme interface secondaire. Ceux qui se trouvent au Manitoba et plus à l'ouest utilisent le contrôleur SBC de Calgary comme interface principale et le contrôleur SBC de Markham comme interface secondaire.

2.1 Paramétrage du raccordement du PBX

Voici trois configurations compatibles avec une mise en œuvre du réseau local du client employant les lignes groupées SIP NGN d'Allstream:

2.1.1 Configuration 1 : Raccordement du PBX avec adresse IP publique – sans NAT

Le PBX ou l'équipement VoIP est accessible par le réseau Internet public. Comme le client n'utilise pas la traduction d'adresse réseau (Network Address Translation – NAT) pour le trafic VoIP, il n'y a aucune conversion NAT entre la grappe SBC d'Allstream et le PBX du client. Le diagramme qui suit illustre cette configuration.

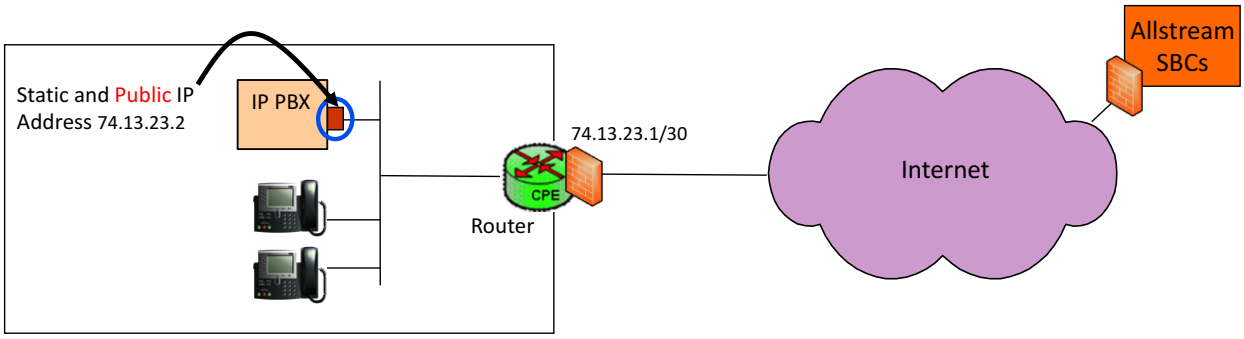

Figure 1 : Raccordement du PBX avec liaison IP publique – sans NAT

L'adresse IP publique qu'utilise le client doit être statique et le sous-réseau est attribué par le fournisseur de services Internet (FSI). L'adresse IP et l'information sur le sous-réseau de l'équipement de voix sur IP relié au réseau d'Allstream doivent être communiquées avec la demande de service de lignes groupées SIP NGN par Internet.

2.1.2 Configuration 2 : Raccordement du PBX avec NAT et passerelle ALG

Certains clients peuvent se doter d'une passerelle de couche application (Application Layer Gateway – ALG), dont la principale fonction est de manipuler ou traduire l'information sur les adresses IP dans la couche application. Plus précisément, la passerelle ALG remplace, pour tout trafic sortant, l'adresse IP privée dans la commande SIP NGN « Invite » et le message de description de session (SDP) par l'adresse IP publique issue de la traduction d'adresse réseau (NAT). De même, pour tout trafic entrant dans le réseau du client en provenance du RTPC, la passerelle ALG remplace l'information sur l'adresse IP publique dans la commande SIP NGN « Invite » et le message SDP par l'adresse IP privée. L'adresse IP statique publique du routeur relié au réseau d'Allstream (74.13.23.1 dans l'exemple montré) doit être communiquée à Allstream avec la demande de service de lignes groupées SIP NGN par Internet.

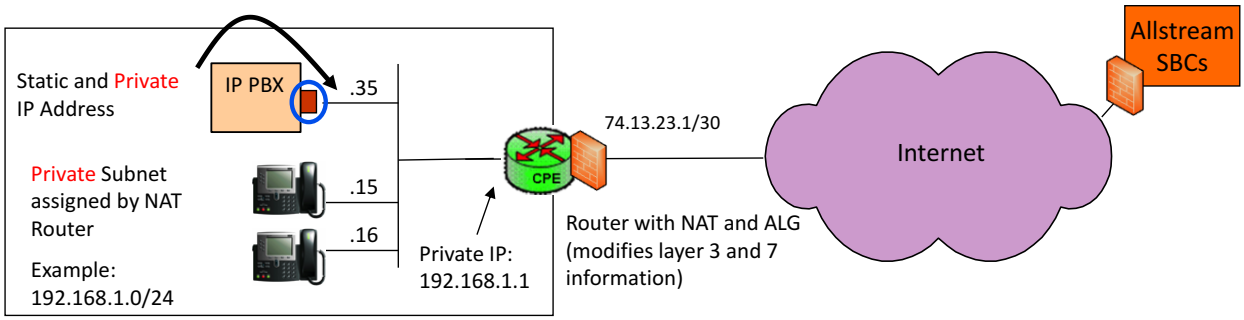

Figure 2 : Raccordement du PBX avec NAT et passerelle ALG

2.1.3 Configuration 3 : Raccordement du PBX avec NAT, sans passerelle ALG

Dans cette configuration, le client ne dispose pas de sa propre passerelle ALG; il utilise plutôt un routeur qui effectue la traduction NAT dans la couche 3. Tout le trafic sortant (privé) est traduit en une adresse IP publique attribuée par le FSI du client (généralement l'adresse IP de l'interface de réseau étendu (WAN) du routeur, ou une adresse IP inutilisée dans le bloc d'adresses fourni). L'adresse IP privée du PBX du client (192.168.1.35 dans l'exemple montré) doit également être fournie à Allstream afin que le contrôleur SBC d'Allstream puisse communiquer avec le PBX. Par conséquent, l'adresse IP statique publique du routeur relié au réseau d'Allstream (74.13.23.1 dans l'exemple montré) et l'adresse IP statique privée de l'équipement VoIP doivent TOUTES LES DEUX être communiquées avec la demande de service de lignes groupées SIP NGN par Internet.

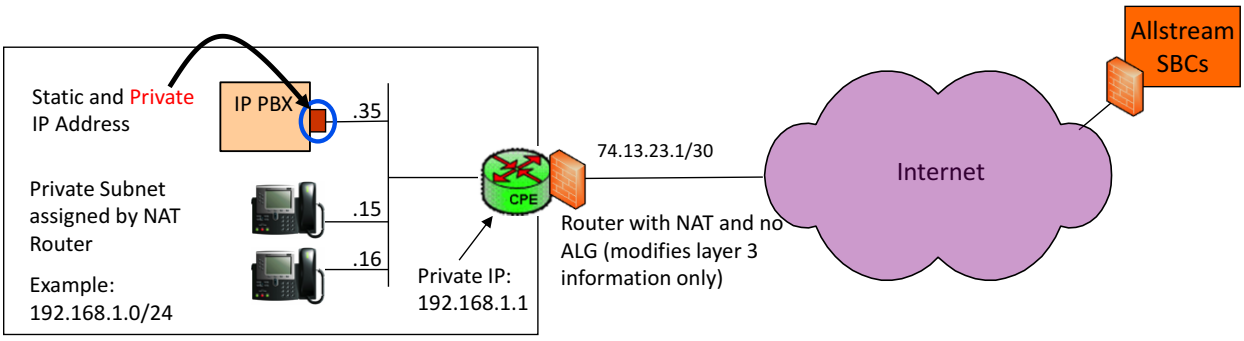

Figure 3 : Raccordement du PBX avec NAT, sans passerelle ALG

2.2 Paramétrage du pare-feu

Si votre environnement est protégé du réseau Internet par un pare-feu, les paramètres du pare-feu doivent être établis de manière à autoriser l'acheminement des transmissions de signalisation et de communication des lignes groupées SIP NGN.

Paramétrez le pare-feu de façon à autoriser la réception de la signalisation et des communications provenant du contrôleur SBC pour qu'elles parviennent aux plages d'adresses IP précitées.

Permettez la signalisation SIP NGN utilisant le protocole UDP sur le port 5060.

Permettez les transmissions RTP utilisant le protocole UDP sur les ports 16000 à 64000.

3 Paramétrage de l'environnement pour les lignes groupées SIP NGN par RPV MPLS

La plate-forme de lignes groupées SIP NGN comprend deux paires de contrôleurs SBC entièrement redondantes, situées dans deux lieux très éloignés (Markham et Calgary), et réservées aux circuits SIP NGN établis sur un RPV MPLS. Cette architecture offre une robustesse, une fiabilité et une sécurité sans égal. Chaque contrôleur SBC figure comme un emplacement distinct dans le RPV du client. Les adresses IP publiques attribuées à l'interface SIP NGN du contrôleur ne sont pas diffusées et ni accessibles par le réseau Internet public. Le trafic SIP NGN de chaque client qui emprunte le réseau MPLS demeure totalement cloisonné grâce aux mécanismes de routage et acheminement virtuel (VRF) et de réseau local virtuel (VLAN).

3.1 Paramétrage du raccordement du PBX

3.1.1 Configuration 1 : Raccordement du PBX par réseau RPV IP privé

Selon cette configuration, le PBX communique avec le contrôleur SBC d'Allstream par un réseau privé virtuel (RPV) MPLS. Cette façon de faire s'apparente à la configuration 1 expliquée plus haut, puisque la traduction d'adresse réseau (NAT) n'est pas nécessaire et que l'ensemble de l'adressage est confiné au sein du RPV privé du client. L'adressage dans le réseau local du client peut se faire de manière statique ou par l'intermédiaire du protocole DHCP.

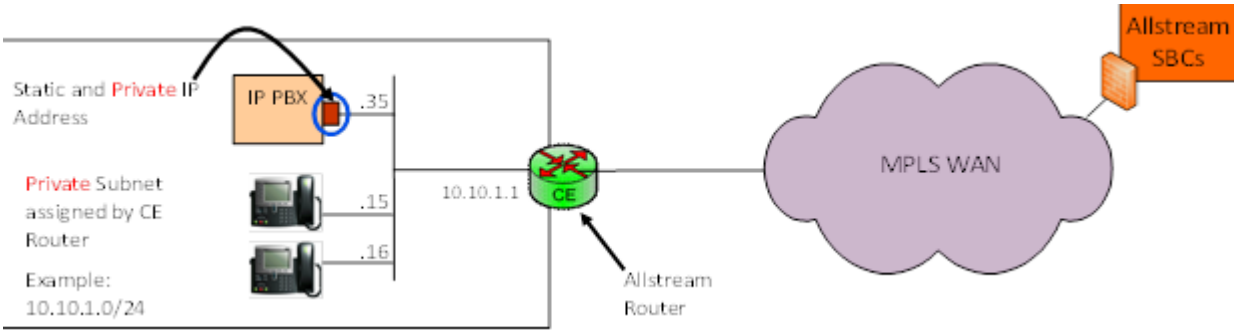

Figure 4 : Raccordement du PBX par réseau RPV IP privé

4 Aspects particuliers liés au protocole DHCP

La technologie VoIP exige que tous les points d'extrémité, y compris les téléphones, reçoivent une adresse IP unique. Lorsqu'il emploie la traduction d'adresse réseau (NAT), le client doit attribuer à chaque point d'extrémité une adresse IP statique, ou s'assurer que le protocole DHCP (Dynamic Host Configuration Protocol) lui en attribue

une au sein de l'environnement du réseau local. Allstream ne fournit pas de services DHCP à partir du routeur d'extrémité client (Customer End – CE). Si le client n'emploie pas la traduction NAT (et donc s'il utilise des adresses publiques pour le réseau VoIP), il doit veiller à ce que tous les points d'extrémité SIP NGN qui communiquent directement avec les contrôleurs SBC d'Allstream aient reçu des adresses IP statiques faisant partie du sous-réseau établi par le fournisseur de services Internet.

5 Programmation du PBX IP

Veuillez consulter la documentation du fabricant pour obtenir les instructions de programmation et de configuration précises de votre PBX IP. Allstream peut fournir des guides de configuration pour de l'équipement préalablement attesté avec les lignes groupées SIP NGN d'Allstream. Vous pouvez vous renseigner à ce sujet auprès de votre ingénieur, Ventes.

Assurez-vous de programmer dans votre PBX IP les mêmes codecs vocaux que ceux ayant servi à établir la largeur de bande requise dans votre demande de service. Autrement, une congestion pourrait survenir et réduire la qualité des appels.

Veuillez noter ce qui suit concernant les nouvelles installations de services de lignes groupées SIP NGN:

- Le PBX peut être programmé pour la composition de 10 chiffres (NPA-NXX-XXXX) ou à 11 chiffres (1+NPA+NXX-XXXX) pour les appels en Amérique du Nord, selon les besoins.
- Les appels locaux au 211 et au 311(services municipaux) ne sont pas possibles. Pour tout appel à ce type de service, il faut programmer dans le PBX IP le numéro de téléphone local approprié.

6 Spécifications liées à la signalisation et à la communication SIP NGN

Spécifications liées à la signalisation SIP NGN	
Protocole	SIP – RFC 3261
Transport	UDP – port 5060
Affichage des coordonnées (ID) de l'appelant	• En-tête P-Asserted-ID (selon RFC3325) • Une identification valide à 10 chiffres doit être transmise.
Blocage des coordonnées (ID) de l'appelant	En-tête Privacy ID (selon RFC3325)

Méthodes SIP offertes	• ACK, BYE, CANCEL, INVITE, OPTIONS, INFO, NOTIFY, PRACK, UPDATE
	• En-têtes SIP :
	  • P-Asserted-ID (selon RFC3325)
	  • Privacy
	• Réinvitation à 0.0.0.0 ou attribut a=sendonly permis pour la mise en garde

Authentification SIP	Le contrôleur SBC authentifie le PBX du client d'après son adresse IP statique.
Autres caractéristiques du service	• SDP précoce • INVITE sans SDP • En-tête inconnu : « Unknown » • En-tête anonyme : « Anonymous » • Extensions compatibles : 100rel, timer

Traitement des états d'erreur	• Numéro non attribué – SIP 404 (pas de message audio) • Nombre maximal de sessions IP – SIP 503 • Codec vocal – P-time miss-match – SIP 488 • Expiration de session – en-tête trop petit – SIP 422
Paramètres de signalisation	• maxSipMsgSize : 2048 • Minuteur de session : MIN-SE 600 • Minuteur de session : expiration de session (par défaut) : 3600 • retransmissionT1 : 500 • retransmissionT2 : 4000 • retransmissionT4 : 5000
QoS	DiffServ – Champ DSCP pour signalisation : CS5 (classe Temps réel)
SIP REFER	Oui

Spécifications liées à la communication	
Protocole	RTP – RFC1889, RFC3264
Transport	UDP – plage de ports • 16000 - 64000
DTMF	RTP intrabande et par RFC2833
Codecs	• G.711a/μ : temps de transmission de trame (paquet) : 20 ms (50 paquets par seconde) • G.729 : 8 kbit/s; taille de trame : 20 ms • G.722 : 20 ms (codec de voix haute définition)
Transcodage à même le réseau	Oui
Détection d'activité vocale	Non
Prise en charge Early Media	Oui
Télécopie	Intercommunication G.711, T.38
QoS	DiffServ : Champ DSCP pour communication : EF (classe Temps réel)

7 Caractéristiques du service

Redondance du réseau VoIP central : 99,999 %
Réservation de numéros SDA
Transfert des NT (numéros de téléphone)
Débordement du circuit vers le NT
Relève du circuit vers le NT
Relève multipoint
Débordement multipoint
Partage de la charge (2 points d'extrémité au maximum)
Acheminement des appels.
Service 911
Assistance-annuaire locale (411)
Service de réparation (611)
Service de transmission de messages (711)
Codes comptables
Modem 14,4
Inscriptions de base dans l'annuaire
Appels à frais virés
E.164