Configuration des paramètres de prise en charge NAT sur l'adaptateur téléphonique SPA8000

Objectif

La traduction d'adresses de réseau (NAT) est un processus qui modifie les adresses IP lors du transit sur un périphérique de routage de trafic afin de remapper une adresse IP dans un en-tête de paquet IP. La fonction NAT est utilisée à des fins de sécurité pour garder l'adresse IP interne cachée afin d'éviter les conflits d'adresses IP. L'objectif de ce document est de configurer les paramètres de prise en charge NAT sur un adaptateur téléphonique analogique SPA8000. Les paramètres de prise en charge NAT jouent un rôle important dans la configuration du protocole SIP (Session Initiation Protocol) qui aide la topologie NAT.

Périphérique applicable

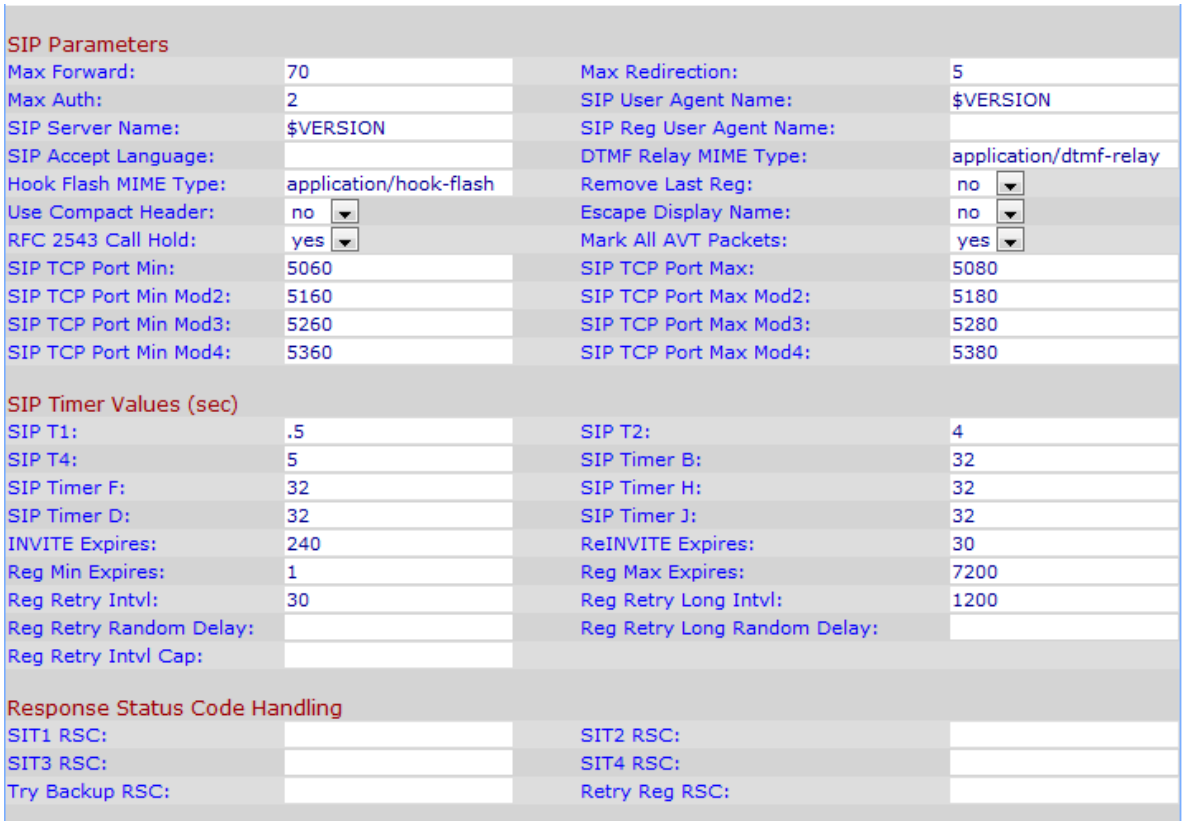
- SPA8000

Version du logiciel

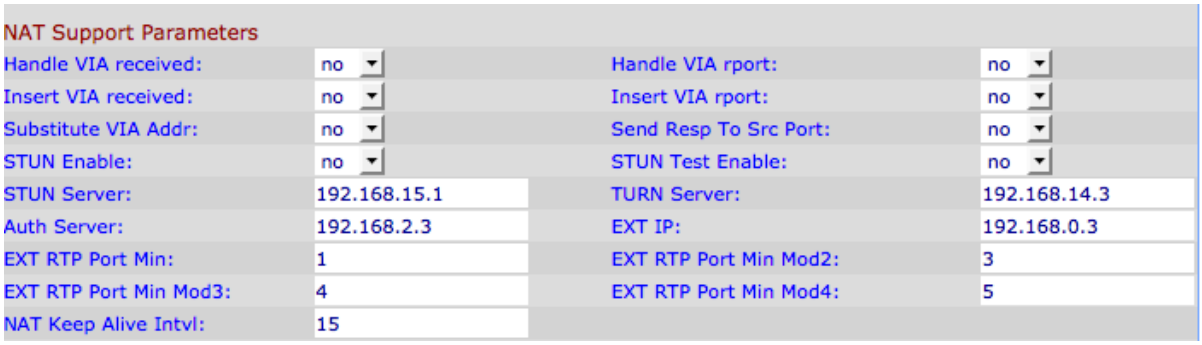
- 6.1.12

Configuration des paramètres de prise en charge NAT

Étape 1. Connectez-vous à l'utilitaire de configuration Web en tant qu'administrateur et sélectionnez **Admin Login > Advanced > Voice > SIP**. La page *SIP* s'ouvre :



SIP Parameters			
Max Forward:	70	Max Redirection:	5
Max Auth:	2	SIP User Agent Name:	$VERSION
SIP Server Name:	$VERSION	SIP Reg User Agent Name:	
SIP Accept Language:		DTMF Relay MIME Type:	application/dtmf-relay
Hook Flash MIME Type:	application/hook-flash	Remove Last Reg:	no
Use Compact Header:	no	Escape Display Name:	no
RFC 2543 Call Hold:	yes	Mark All AVT Packets:	yes
SIP TCP Port Min:	5060	SIP TCP Port Max:	5080
SIP TCP Port Min Mod2:	5160	SIP TCP Port Max Mod2:	5180
SIP TCP Port Min Mod3:	5260	SIP TCP Port Max Mod3:	5280
SIP TCP Port Min Mod4:	5360	SIP TCP Port Max Mod4:	5380
SIP Timer Values (sec)			
SIP T1:	.5	SIP T2:	4
SIP T4:	5	SIP Timer B:	32
SIP Timer F:	32	SIP Timer H:	32
SIP Timer D:	32	SIP Timer J:	32
INVITE Expires:	240	ReINVITE Expires:	30
Reg Min Expires:	1	Reg Max Expires:	7200
Reg Retry Intvl:	30	Reg Retry Long Intvl:	1200
Reg Retry Random Delay:		Reg Retry Long Random Delay:	
Reg Retry Intvl Cap:			
Response Status Code Handling			
SIT1 RSC:		SIT2 RSC:	
SIT3 RSC:		SIT4 RSC:	
Try Backup RSC:		Retry Reg RSC:	



Étape 2. Choisissez **yes** dans la liste déroulante Handle VIA Received pour permettre à la carte de traiter le paramètre reçu dans l'en-tête VIA. Si la valeur **no** est alors le paramètre sera ignoré. La valeur par défaut est no.

Étape 3. Choisissez **yes** dans la liste déroulante Handle VIA Report pour permettre à la carte de traiter le paramètre de rapport reçu dans l'en-tête VIA. Si la valeur **no** est alors le paramètre sera ignoré. La valeur par défaut est no.

Étape 4. Choisissez **yes** dans la liste déroulante Insérer VIA reçu pour permettre à l'adaptateur d'insérer le paramètre d'insertion reçu dans l'en-tête VIA des réponses SIP, si les valeurs reçues d'IP et VIA envoyées par IP diffèrent. Non est établi par défaut.

Étape 5. Choisissez **yes** dans la liste déroulante Insérer un rapport VIA pour permettre à la carte d'insérer le paramètre de rapport reçu dans l'en-tête VIA des réponses SIP si les valeurs reçues d'IP et VIA envoyées par IP diffèrent. Non est établi par défaut.

Étape 6. Choisissez **yes** dans l'adresse VIA de substitution pour utiliser les valeurs de port IP mappées NAT dans l'en-tête VIA. La valeur par défaut est no.

Étape 7. Choisissez **yes** dans la liste déroulante Send Resp To Src Port. Cette option permet d'envoyer des réponses au port source de la demande au lieu du port VIA envoyé par. La valeur par défaut est no.

Étape 8. Choisissez **yes** dans la liste déroulante STUN Enable pour découvrir les mappages NAT. Non est établi par défaut.

Étape 9. Si la fonctionnalité STUN Enable est activée à l'étape 9 et qu'un serveur STUN valide est disponible, la carte peut effectuer une opération de détection de type NAT lorsqu'elle est mise sous tension. Il contacte le serveur stun configuré et le résultat de la détection sera signalé dans un en-tête d'avertissement dans toutes les requêtes REGISTER suivantes. Si la carte détecte une NAT symétrique ou un pare-feu symétrique, le mappage NAT est désactivé. La valeur par défaut de ce champ est no. Pour définir la valeur sur yes, sélectionnez **yes** dans la liste déroulante STUN Test Enable.

Étape 10. Dans le champ STUN Server, saisissez l'adresse IP ou le nom de domaine complet du serveur STUN à contacter pour la découverte du mappage NAT.

Étape 11. Saisissez le serveur TURN (Traversal Using Relays around NAT) dans le champ TURN Server. Le serveur TURN permet aux applications derrière la NAT de recevoir des données.

Étape 12. Saisissez Auth Server dans le champ Auth Server. Le serveur d'authentification est un serveur d'authentification utilisé pour authentifier le nom d'utilisateur et le mot de passe d'un périphérique.

Étape 13. Dans le champ EXT IP, saisissez l'adresse IP externe qui remplacerait l'adresse IP réelle de la carte dans tous les messages SIP sortants. La valeur par défaut est 0.0.0.0. Si 0.0.0.0 est entré, aucune substitution n'est effectuée.

Étape 14. Dans EXT RTP Port Min, saisissez le numéro de mappage de port externe du RTP Port Min. La valeur par défaut de ce champ est zéro. S'il n'est pas égal à zéro, le numéro de port RTP de tous les messages SIP sortants sera remplacé par la valeur de port correspondante dans la plage de ports RTP externes.

Étape 15. Entrez une valeur dans le champ NAT Keep Alive Intvl qui fournit l'intervalle entre les messages de maintien de connexion de la mise en correspondance NAT. Les messages de maintien de connexion NAT empêchent l'expiration des mappages NAT sur le périphérique NAT. La valeur par défaut est de 15 secondes.

Étape 16. Cliquez sur **Submit All Changes** pour enregistrer les paramètres.