SPA8000電話アダプタのNATサポートパラメータ設定

目的

ネットワークアドレス変換(NAT)は、IPパケットヘッダー内の1つのIPアドレスを再マッピングするために、トラフィックルーティングデバイスを通過する際にIPアドレスを変更するプロセスです。 NATは、IPアドレスの競合を避けるために、内部IPアドレスを隠すためにセキュリティ目的で使用されます。このドキュメントの目的は、SPA8000アナログ電話アダプタでNATサポートパラメータを設定することです。NATサポートパラメータは、NATトポロジを支援するSession Initiation Protocol(SIP)の設定において重要な機能を果たします。

該当するデバイス

- SPA8000

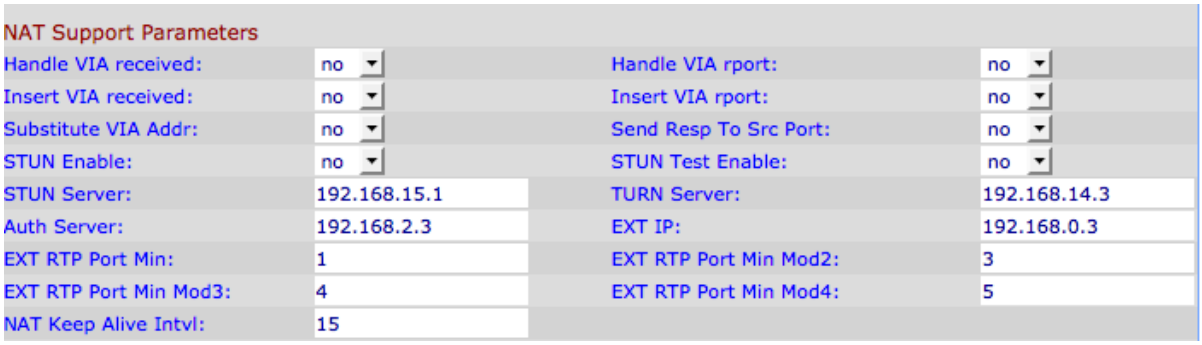
[Software Version]

- 6.1.12

NATサポートパラメータの設定

ステップ1：管理者としてWeb構成ユーティリティにログインし、**[Admin Login] > [Advanced] > [Voice] > [SIP]を選択します。**[*SIP*]ページが開きます。

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:	



ステップ2:[Handle VIA received]ドロップダウンリストから[**yes**]を選択し、アダプタがVIAヘッダーで受信したパラメータを処理できるようにします。noに設定した場合、パラメータは無視されます。デフォルト値はnoです。

ステップ3:[Handle VIA report]ドロップダウンリストから[yes] を選択し、アダプタがVIAヘッダーで受信したレポートパラメータを処理できるようにします。noに設定した場合、パラメータは無視されます。デフォルト値はnoです。

ステップ4:[Insert VIA received]ドロップダウンリストから[yes] を選択し、SIP応答のVIAヘッダーに受信した挿入パラメータを挿入できるようにします（received-from IPとVIA sent-by IPの値が異なる場合）。デフォルトは no です。

ステップ5:[Insert VIA rport]ドロップダウンリストから[yes] を選択し、[received-from IP]と[VIA sent-by IP]の値が異なる場合、アダプタが受信したレポートパラメータをSIP応答のVIAヘッダーに挿入できるようにします。デフォルトは no です。

ステップ6:[Substitute VIA Addr]から[**yes**]を選択し、VIAヘッダーのNATマッピングされたIPポート値を使用します。デフォルト値はnoです。

ステップ7:[Send Resp To Src Port]ドロップダウンリストから[**yes**]を選択します。このオプションを使用すると、VIAの送信ポートではなく、要求の送信元ポートに応答を送信できます。デフォルト値はnoです。

ステップ8:[STUN Enable]ドロップダウンリストから[**yes**]を選択し、NATマッピングを検出します。デフォルトは no です。

ステップ9：ステップ9でSTUN Enable機能が有効になっていて、有効なSTUNサーバが使用可能な場合、アダプタは電源がオンになったときにNATタイプの検出操作を実行できます。設定されたstunサーバに接続し、検出の結果は、後続のすべてのREGISTER要求で警告ヘッダーに報告されます。アダプタが対称NATまたは対称ファイアウォールを検出すると、NATマッピングは無効になります。このフィールドのデフォルト値は「no」です。値を「yes」に設定するには、「STUN Test Enable」ドロップダウン・リストから「**yes**」を選択します。

ステップ10:[STUN Server]フィールドに、NATマッピング検出のために接続するSTUNサーバのIPアドレスまたは完全修飾ドメイン名(FQDN)を入力します。

ステップ11:[TURN Server]フィールドにTURN(Traversal Using Relays around NAT)サーバを入力します。TURNサーバは、NATの背後にあるアプリケーションがデータを受信できるようにします。

ステップ12:[Auth Server]フィールドに認証サーバを入力します。認証サーバは、デバイスのユーザ名とパスワードの認証に使用される認証サーバです。

ステップ13:[EXT IP]フィールドに、すべての発信SIPメッセージでアダプタの実際のIPアド

レスを置き換える外部IPアドレスを入力します。デフォルト値は0.0.0.0です。0.0.0.0を入力すると、置換は実行されません。

ステップ14:[EXT RTP Port Min]に、RTPポートの最小の外部ポートマッピング番号を入力します。このフィールドのデフォルト値は0です。ゼロでない場合、すべての発信SIPメッセージのRTPポート番号が、外部RTPポート範囲の対応するポート値に置き換えられます。

ステップ15:[NAT Keep Alive Vl]フィールドに、NATマッピングのキープアライブメッセージ間の間隔を示す値を入力します。NATキープアライブメッセージは、NATデバイスのNATマッピングの期限切れを防止します。デフォルト値は15秒です。

ステップ16:[**Submit All Changes]をクリック**して、設定を保存します。