

NAT-ondersteuningsparameters voor SPA8000 telefoonadapter

Doel

Network adresomzetting (NAT) is een proces dat IP-adressen wijzigt tijdens het doorsturen van een verkeersrouteringsapparaat om één IP-adres in een IP-pakketheader opnieuw in te delen. NAT wordt voor veiligheidsdoeleinden gebruikt om het interne IP-adres verborgen te houden om tegenstrijdige IP-adressen te voorkomen. Het doel van dit document is om NAT-ondersteuningsparameters te configureren op een SPA8000 analoge telefoonadapter. NAT-ondersteuningsparameters spelen een belangrijke functie in de configuratie van Session Initiation Protocol (SIP) dat de NAT-topologie ondersteunt.

Toepassbaar apparaat

- SPA8000

Softwareversie

- 6.1.12

Configuratie NAT-ondersteuningsparameters

Stap 1. Meld u aan bij het programma voor webconfiguratie als beheerder en kies **Admin Login > Geavanceerd > Voice > SIP**. De *SIP*-pagina wordt geopend:

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:	

NAT Support Parameters			
Handle VIA received:	no	Handle VIA rport:	no
Insert VIA received:	no	Insert VIA rport:	no
Substitute VIA Addr:	no	Send Resp To Src Port:	no
STUN Enable:	no	STUN Test Enable:	no
STUN Server:	192.168.15.1	TURN Server:	192.168.14.3
Auth Server:	192.168.2.3	EXT IP:	192.168.0.3
EXT RTP Port Min:	1	EXT RTP Port Min Mod2:	3
EXT RTP Port Min Mod3:	4	EXT RTP Port Min Mod4:	5
NAT Keep Alive Intvl:	15		

Stap 2. Kies **ja** uit de vervolgkeuzelijst Handle VIA om de adapter in staat te stellen om de ontvangen parameter in de VIA header te verwerken. Als dit op **nee** is ingesteld, wordt de parameter genegeerd. De standaardwaarde is nee.

Stap 3. Kies **ja** uit de vervolgkeuzelijst Handle VIA rapport om de adapter in staat te stellen om de ontvangen parameter in de VIA header te verwerken. Als dit op **nee** is ingesteld, wordt de parameter genegeerd. De standaardwaarde is nee.

Stap 4. Kies **ja** van de vervolgkeuzelijst invoegen VIA ontvangen, om de adapter in staat te stellen de ontvangen invoegparameter in de VIA-kop van SIP-reacties op te nemen, als de ontvangen waarden van IP en VIA verzonden IP verschillen. De standaardinstelling is nee.

Stap 5. Kies **ja** van de vervolgkeuzelijst invoegen van het VIA-rapport om de adapter in staat te stellen de ontvangen parameter in de VIA-kop van de SIP-reacties te plaatsen indien de ontvangen waarden van IP en VIA verzonden IP verschillen. De standaardinstelling is nee.

Stap 6. Kies **ja** uit de suboptie VIA Address om gebruik te maken van NAT-in kaart gebrachte IP poortwaarden in de VIA header. De standaardwaarde is nee.

Stap 7. Kies **ja** van Send Resp to Src Port vervolgkeuzelijst. Met deze optie kunnen reacties naar de poort van de aanvraagbron worden verzonden in plaats van VIA-poort. De standaardwaarde is nee.

Stap 8. Kies **ja** van de vervolgkeuzelijst STUN Enable om NAT-afbeeldingen te ontdekken. De standaardinstelling is **nee**.

Stap 9. Als de optie STUN Enable in Stap 9 is ingeschakeld en er een geldige STUN-server beschikbaar is, kan de adapter een NAT-type zoekactie uitvoeren wanneer deze aan staat. Het contacteert de geconfigureerde stunserver en het resultaat van de ontdekking wordt in een waarschuwingsheader in alle volgende REGISTER-verzoeken gemeld. Als de adapter een symmetrische NAT of een symmetrische firewall zou detecteren, zou NAT-mapping worden uitgeschakeld. De standaardwaarde van dit veld is nee. Om de waarde in te stellen op ja, kiest u **ja** in de vervolgkeuzelijst STUN Test Enable.

Stap 10. Voer in het veld STUN Server het IP-adres in of de Full Qualified Domain Name van de STUN-server om contact op te nemen voor NAT-kaartontdekking.

Stap 1. Voer in het veld TURN-server (Verplaatsing met Relay-out rond NAT) in. TURN-server stelt toepassingen achter de NAT in staat gegevens te ontvangen.

Stap 12. Voer de Auth Server in het veld Auth Server in. Auth server is een authenticatieserver die wordt gebruikt om de gebruikersnaam en het wachtwoord van een apparaat te authenticeren.

Stap 13. Voer in het veld EXT IP het externe IP-adres in dat het IP-adres van de adapter in

alle uitgaande SIP-berichten kan vervangen. De standaardwaarde is 0.0.0.0. Als 0.0.0 wordt ingevoerd, dan wordt geen vervanging uitgevoerd.

Stap 14. In de EXT RTP-poortadapter voert u het externe poortkaartnummer van de RTP-poortmin in. De standaardwaarde voor dit veld is nul. Als deze niet nul is, dan zou het RTP poortnummer in alle uitgaande SIP berichten voor de corresponderende havenwaarde in het externe RTP poortbereik worden vervangen.

Stap 15. Voer een waarde in in het veld NAT Houd Alive Inv in die het interval tussen NAT-mapping biedt, houdt u levende berichten in. NAT bewaar berichten die voorkomen dat NAT-mappingen op NAT-apparaat verlopen. De standaardwaarde is 15 seconden.

Stap 16. Klik op **Alle wijzigingen indienen** om de instellingen op te slaan.