NAT Support Parameters Configuration on SPA8000 Phone Adapter

Objective

Network Address Translation (NAT) is a process that modifies IP addresses while in transit across a traffic routing device for the purpose of remapping one IP address in an IP packet header. NAT is used for security purposes to keep the internal IP address hidden to avoid conflict of IP addresses. The objective of this document is to configure NAT Support Parameters on a SPA8000 Analog Telephone Adapter. NAT Support Parameters play an important function in the configuration of Session Initiation Protocol (SIP) which assists the NAT topology.

Applicable Device

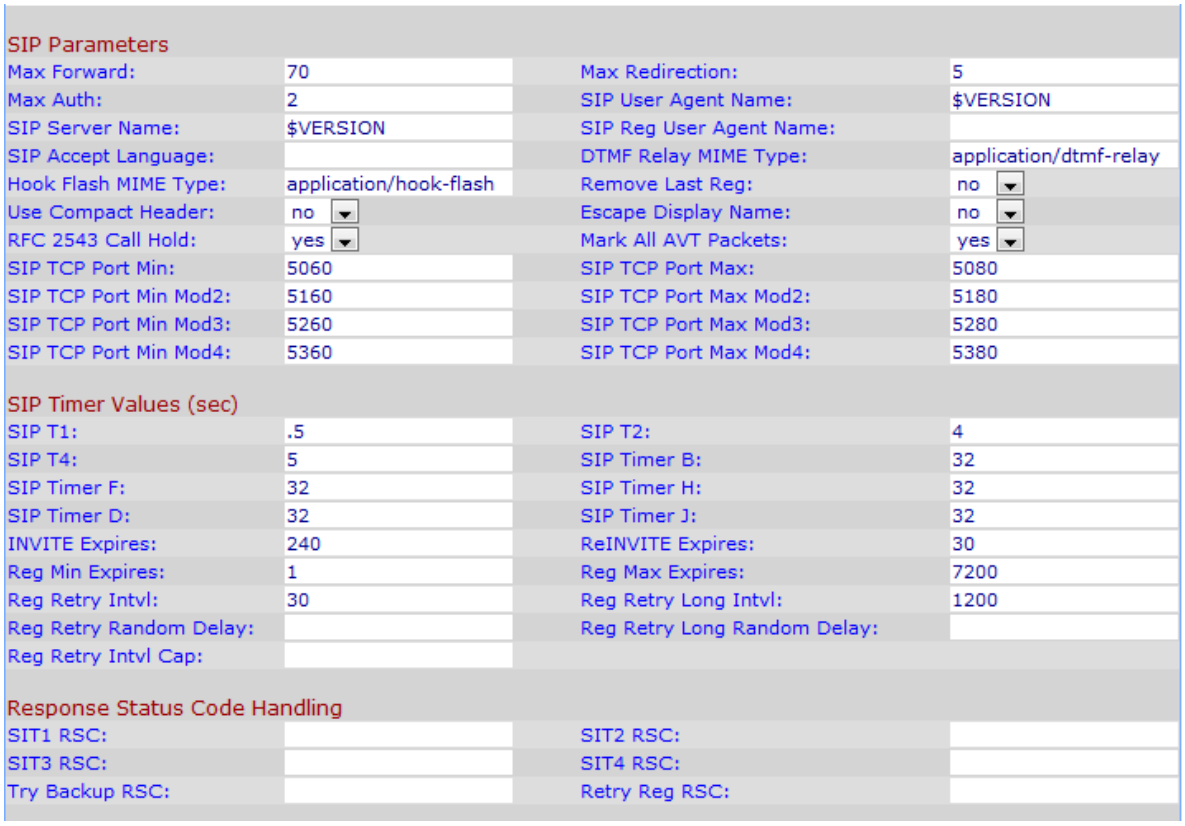
- SPA8000

Software Version

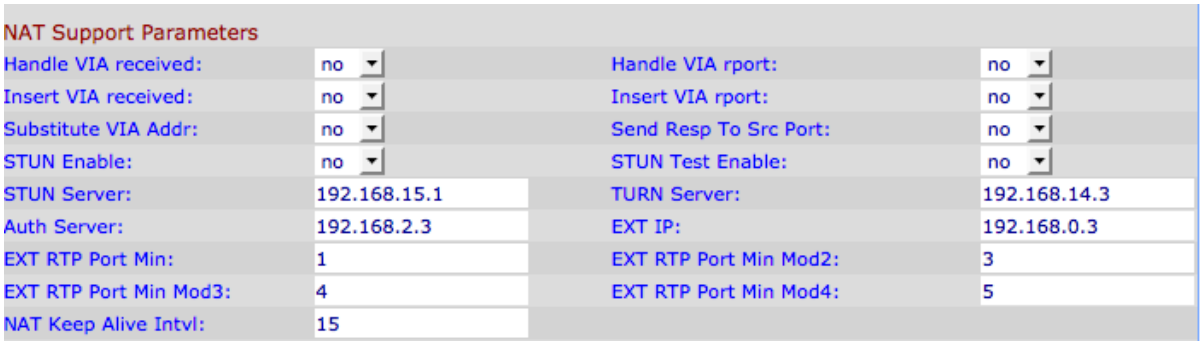
- 6.1.12

NAT Support Parameters Configuration

Step 1. Log in to the web configuration utility as an administrator and choose **Admin Login > Advanced > Voice > SIP**. The *SIP* page opens:



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:	



Step 2. Choose **yes** from the Handle VIA received drop-down list to enable the adapter to process the received parameter in the VIA header. If set to **no** then the parameter would be ignored. The default value is no.

Step 3. Choose **yes** from the Handle VIA rport drop-down list to enable the adapter to process the received rport parameter in the VIA header. If set to **no** then the parameter would be ignored. The default value is no.

Step 4. Choose **yes** from the Insert VIA received drop-down list to enable the adapter to insert the received insert parameter into the VIA header of SIP responses, if the received-from IP and VIA sent-by IP values differ. The default is no.

Step 5. Choose **yes** from the Insert VIA rport drop-down list to enable the adapter to insert the received rport parameter into the VIA header of SIP responses if the received-from IP and VIA sent-by IP values differ. The default is no.

Step 6. Choose **yes** from the Substitute VIA Addr to make use of NAT-mapped IP port values in the VIA header. The default value is no.

Step 7. Choose **yes** from Send Resp To Src Port drop-down list. This option allows responses to be sent to the request source port instead of the VIA sent-by port. The default value is no.

Step 8. Choose **yes** from the STUN Enable drop-down list to discover NAT mappings. The default is **no**.

Step 9. If the STUN Enable feature is enabled in Step 9 and a valid STUN server is available, the adapter can perform a NAT-type discovery operation when it would power on. It contacts the configured stun server and the result of the discovery would be reported in a warning header in all subsequent REGISTER requests. If the adapter would detect a symmetric NAT or a symmetric firewall, NAT mapping would be disabled. The default value of this field is no. To set the value to yes, choose **yes** from the STUN Test Enable drop-down list.

Step 10. In the STUN Server field, enter the IP Address or the Fully Qualified Domain Name of the STUN server to contact for NAT mapping discovery.

Step 11. Enter the TURN (Traversal Using Relays around NAT) Server in the TURN Server field. TURN server allows applications behind the NAT to receive data.

Step 12. Enter the Auth Server in the Auth Server field. Auth server is an authentication server used to authenticate the username and password of a device.

Step 13. In the EXT IP field, enter the External IP Address that would substitute the actual IP address of the adapter in all outgoing SIP messages. The default value is 0.0.0.0. If 0.0.0.0

is entered, then no substitution is performed.

Step 14. In EXT RTP Port Min enter the external port mapping number of the RTP Port Min. The default value for this field is zero. If it is not zero, then the RTP port number in all outgoing SIP messages would be substituted for the corresponding port value in the external RTP port range.

Step 15. Enter a value in the NAT Keep Alive Intvl field that provides the interval between NAT-mapping keep alive messages. NAT keep alive messages prevent the expiration of NAT mappings on NAT device. The default value is 15 seconds.

Step 16. Click **Submit All Changes** to save the settings.