



Configuring H.323 over Port Network Address Translation (PNAT) for Avaya IP Endpoints using the Avaya™ SG200 Security Gateway - Issue 1.0

Abstract

These Application Notes describe how to configure the Avaya SG200 Security Gateway to handle Avaya IP Telephone/Softphone H.323 Voice over IP (VoIP) signaling and media traffic through PNAT. The sample VoIP configuration depicted in this document consists of an Avaya™ S8700 Media Server with an Avaya™ G600 Media Gateway (S8700/G600) located in the headquarters, and Avaya™ IP Telephones/Softphones located in a remote site.

1. Introduction

These Application Notes describe how to configure the Avaya SG200 Security Gateway to handle Avaya IP Telephones/Softphones H.323 VoIP signaling and media traffic through PNAT. The sample VoIP reference configuration depicted in this document consists of Avaya telephony equipment running Avaya Communication Manager software.

The Avaya SG200 Security Gateway is a Virtual Private Network (VPN) gateway/stateful firewall targeted for branch locations and small/medium enterprises. The SG200 Security Gateway firewall functionality features an integrated H.323 application proxy that addresses VoIP deployment issues in a NAT environment. The SG200 Security Gateway acts as an intermediary between H.323 terminals and gatekeepers performing H.323 manipulations on signaling and media streams. It is typically located in a branch location between the LAN VoIP endpoints and WAN access router.

Figure 1 illustrates the components of the VoIP network configuration used to verify these Application Notes. The Avaya SG200 Security Gateway located at the remote site is connected between the Cisco 2621 WAN access router and the Avaya P333R switch. Placing the Avaya SG200 Security Gateway in this location ensures all VoIP traffic originating from the remote site passes through the SG200 Security Gateway. The default route in the Avaya P333R switch located at the remote site, routes all voice and data traffic to the Avaya SG200 Security Gateway private interface.

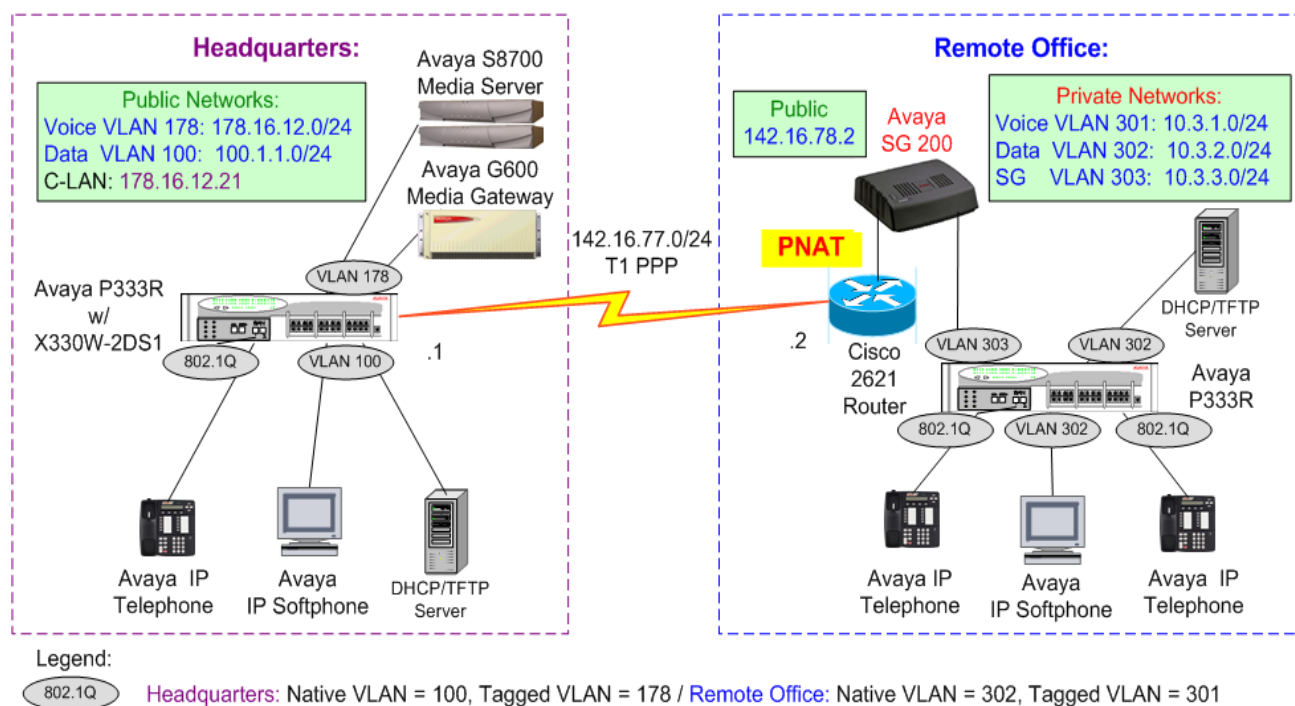


Figure 1: Avaya IP Telephone VoIP over PNAT Configuration

Note: These Application Notes assume the Layer 2 and Layer 3 network configuration depicted in **Figure 1** is already in place. Only the configuration related to the PNAT and H.323 proxy implementation is addressed. Please consult the appropriate User Guides for more information on how to setup the remaining components.

2. Hardware and Software Validated

Hardware and Software	Version
Avaya™ S8700 Media Servers	1.3
Avaya™ G600 Media Gateway	1.3
Avaya™ 4600 Series IP Telephones	1.73
Avaya™ IP Softphones	4.2.2.2
Avaya™ P333R Modular Stackable Switches	4.0.9
Avaya™ SG200 Security Gateway	4.31.20 (Beta)
Cisco 2621 Router	12.2(8)T4
DHCP/TFTP Servers: Microsoft Windows 2000 Server	5.00.2195 (SP2)

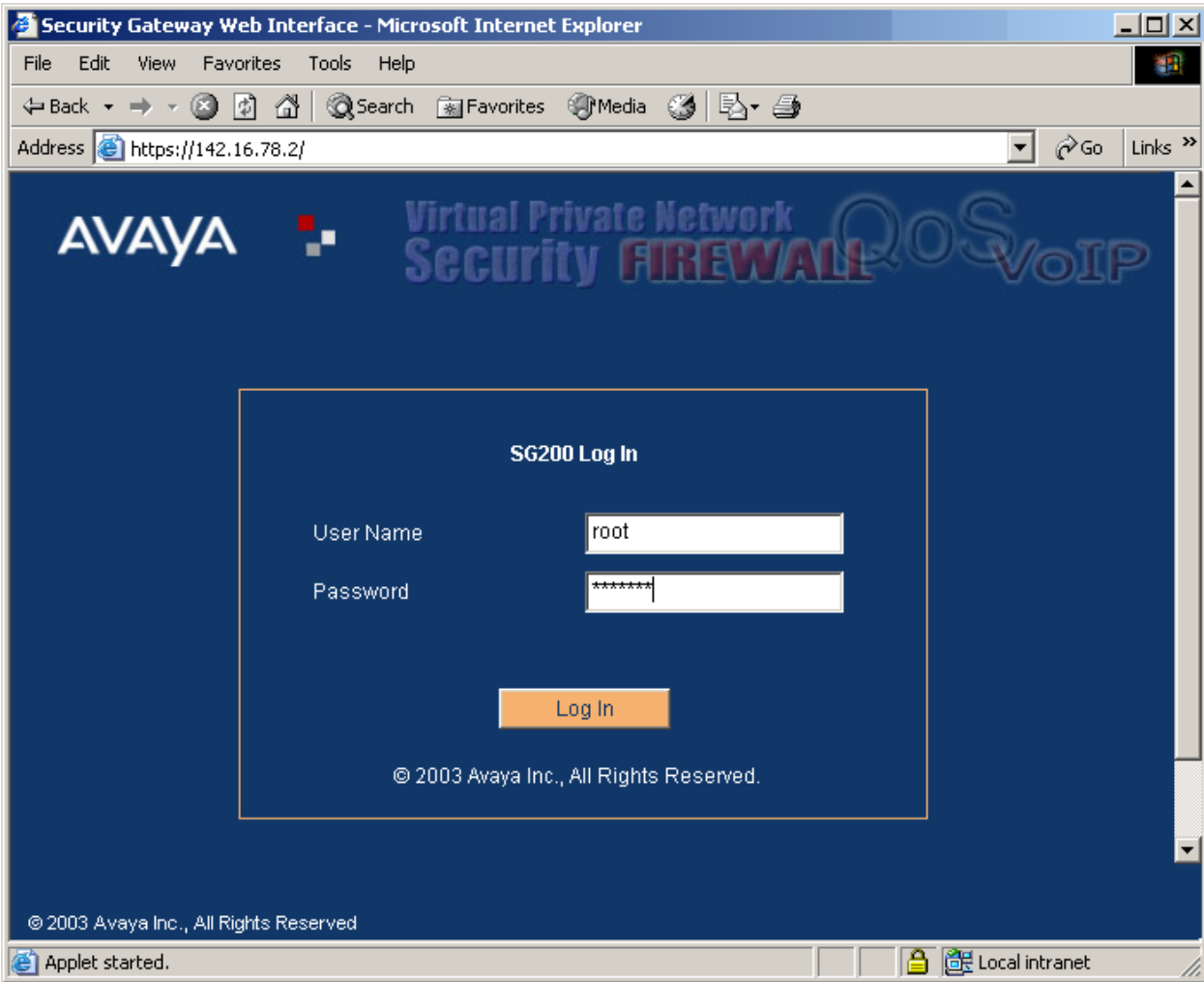
Table 1: Hardware and Software Versions

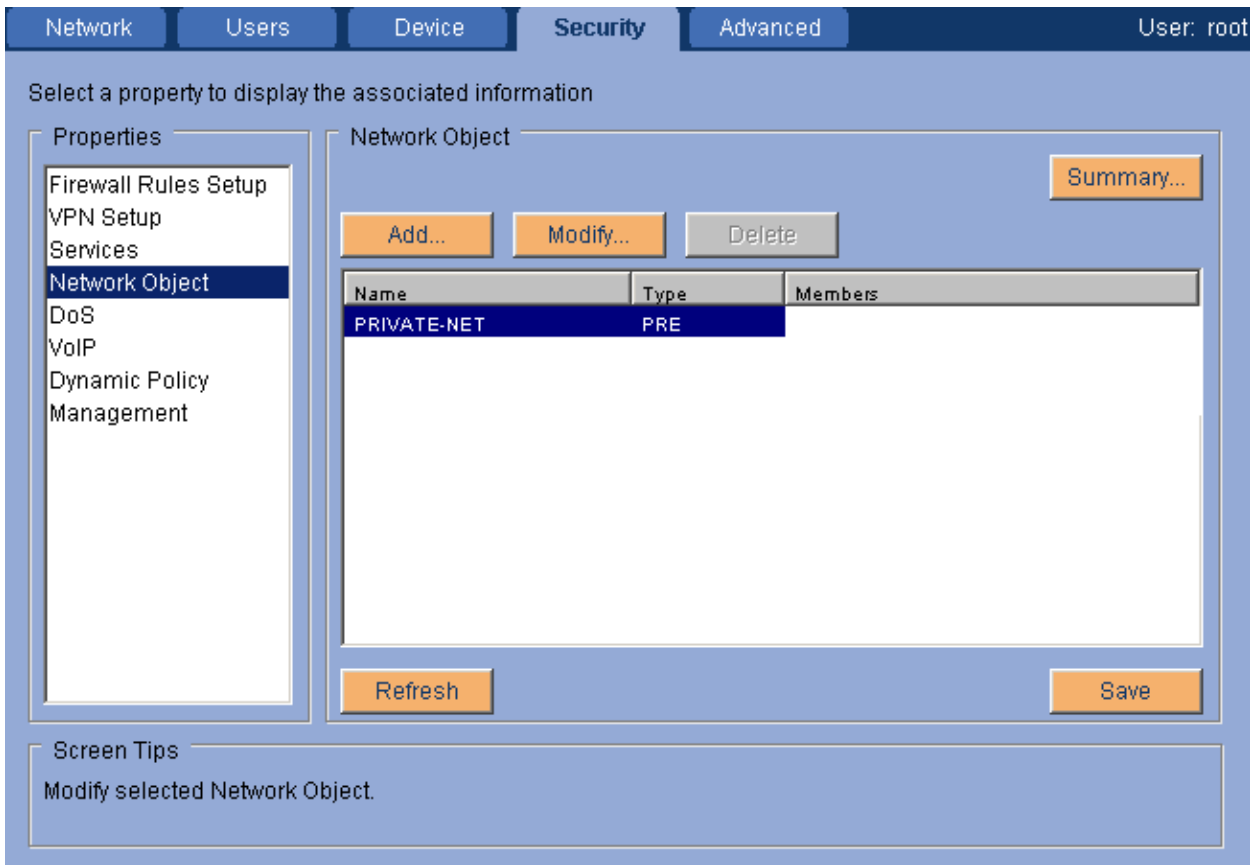
3. Avaya SG200 VoIP (H.323 proxy) Configuration

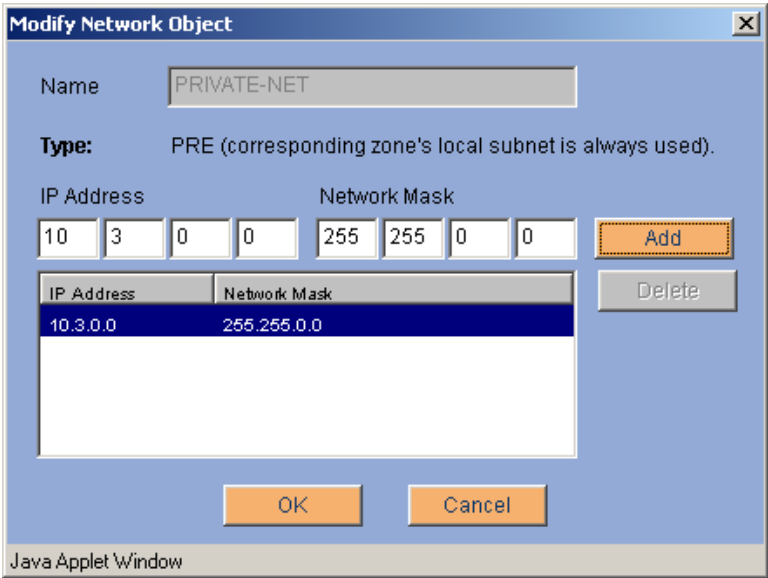
The following configuration was done through the Avaya SG200 Security Gateway Web Graphical User Interface (GUI).

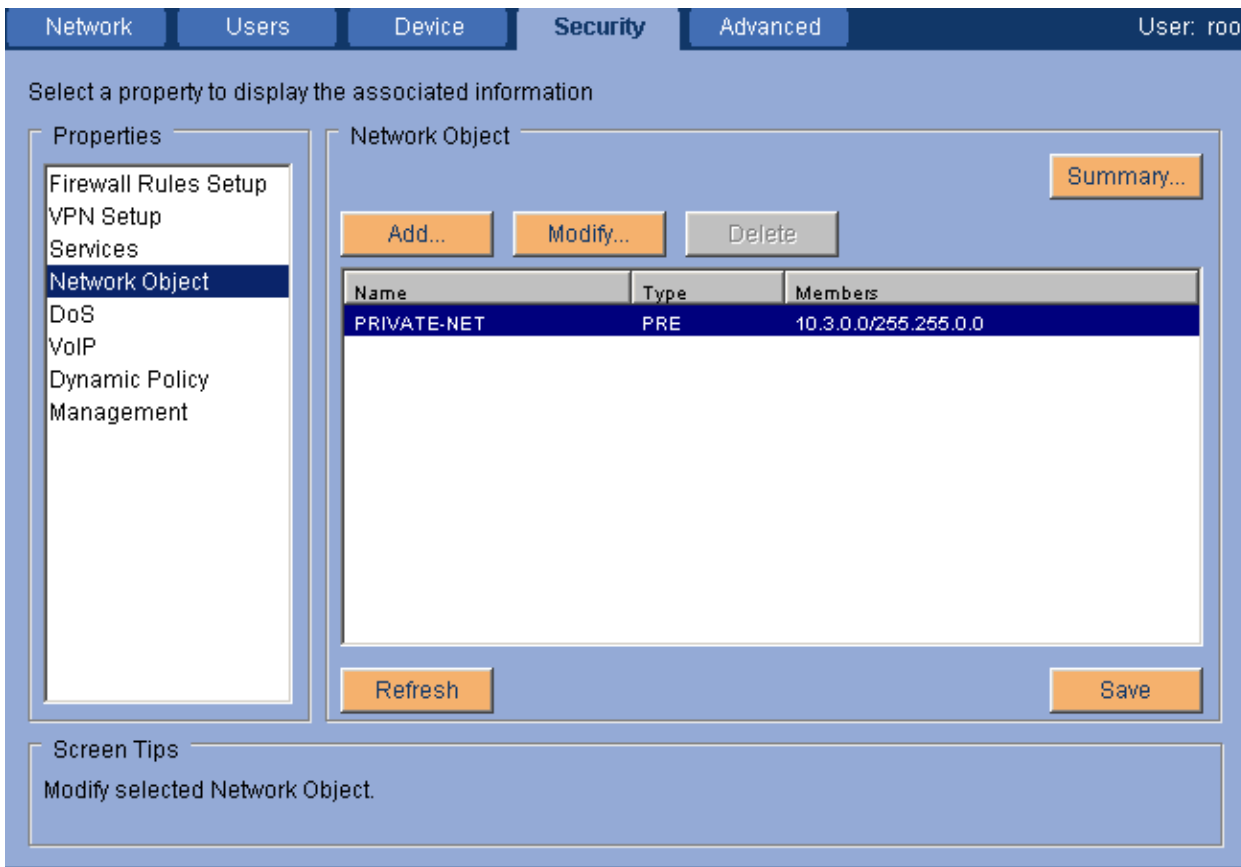
Note: This procedure can be used for all other Avaya SG20x Security Gateway products.

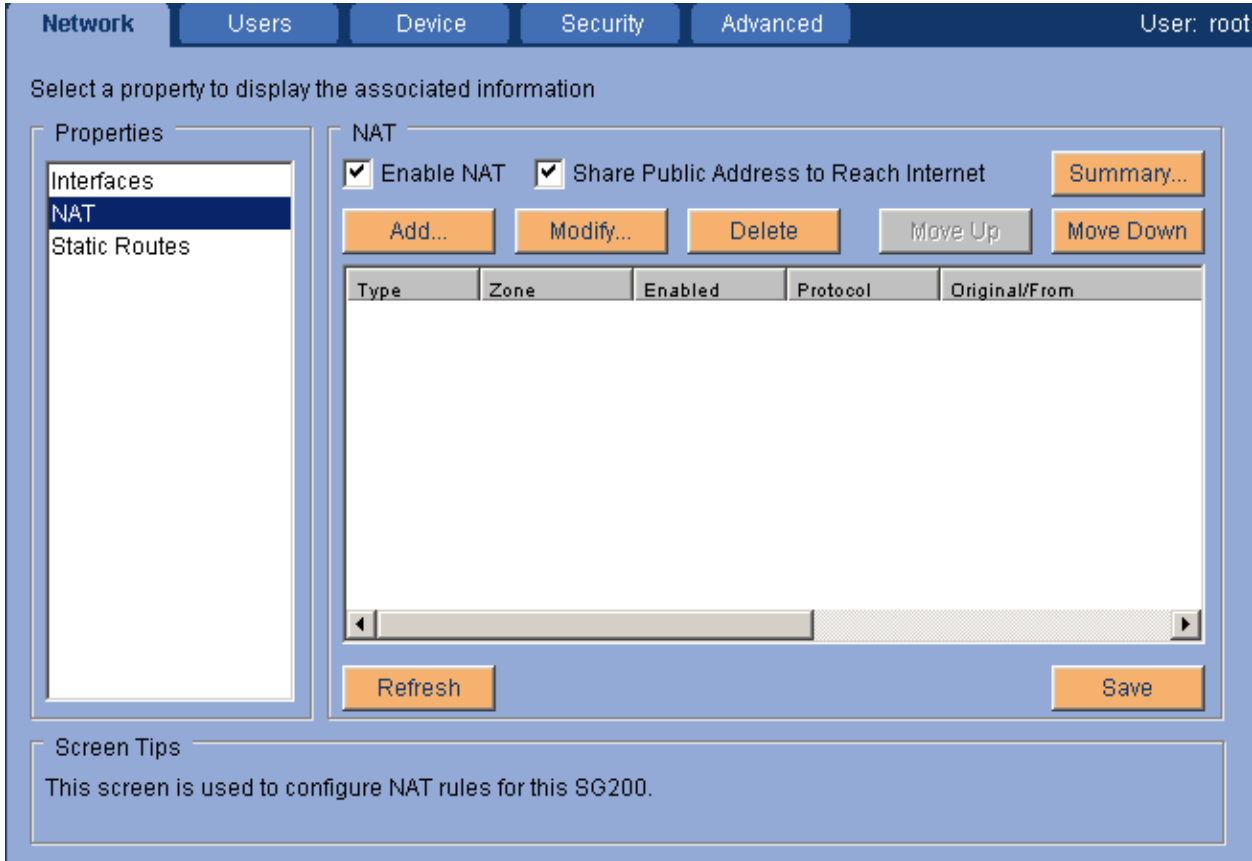
Step	Description
1.	Bring up a web browser using “https” with the public or private IP address of the Avaya SG 200 Security Gateway. Click “Yes” to accept the security alert message.  The image shows a 'Security Alert' dialog box with a blue title bar and a close button. It contains a yellow warning icon and the text: 'Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.' Below this, there are three items: a yellow warning icon with the text 'The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.', a green checkmark icon with the text 'The security certificate date is valid.', and a yellow warning icon with the text 'The name on the security certificate is invalid or does not match the name of the site'. At the bottom, it asks 'Do you want to proceed?' and has three buttons: 'Yes', 'No', and 'View Certificate'.

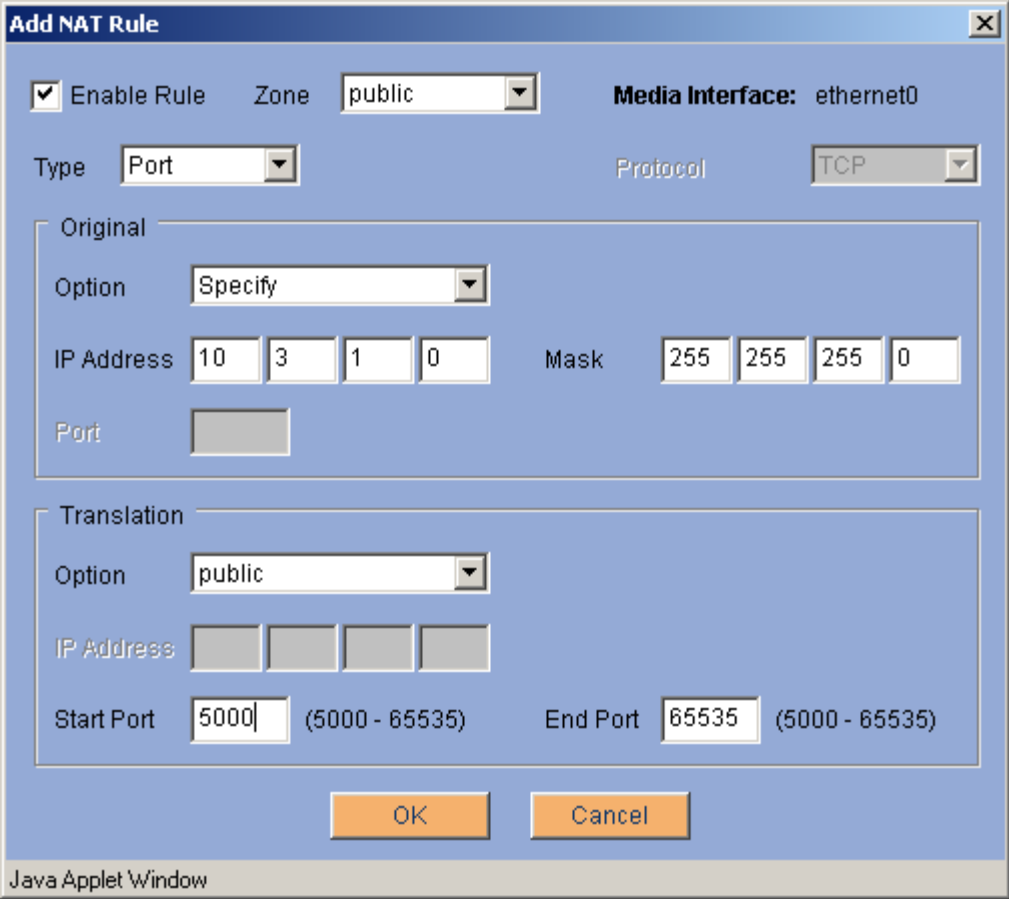
Step	Description
2.	The Avaya SG200 Security Gateway “Login” window is displayed. Enter a username and password with administrator privileges and click the “Log in” button to enter the system: 

Step	Description
3.	The main management window appears upon logging into the Avaya SG200 Security Gateway. Add the voice and data private subnets to the “PRIVATE-NET” network object. The “PRIVATE-NET” network object will be used later for H.323 proxy VoIP configuration. Navigate to “Configure” → “Security Tab” → “Network Object”. Highlight the “PRIVATE-NET” object and click the “Modify” button to specify the subnets for the private networks.  The screenshot displays the Avaya SG200 Security Gateway management interface. At the top, there are tabs for 'Network', 'Users', 'Device', 'Security' (selected), and 'Advanced'. The user is logged in as 'root'. Below the tabs, a message says 'Select a property to display the associated information'. On the left, a 'Properties' sidebar lists: 'Firewall Rules Setup', 'VPN Setup', 'Services', 'Network Object' (highlighted), 'DoS', 'VoIP', 'Dynamic Policy', and 'Management'. The main content area is titled 'Network Object' and contains a table with columns 'Name', 'Type', and 'Members'. The table has one row: 'PRIVATE-NET' with type 'PRE'. Above the table are buttons 'Add...', 'Modify...' (highlighted), and 'Delete'. To the right of the table is a 'Summary...' button. Below the table are 'Refresh' and 'Save' buttons. At the bottom, a 'Screen Tips' section says 'Modify selected Network Object.'

Step	Description
4.	The following “Modify Network Object” window is displayed. Enter the IP address(s)/ Mask(s) for the private data and voice networks. Click the “Add” button to add the IP address(s)/Mask(s) to the network object. Repeat this procedure if needed.  Click the “OK” button to modify the SG200 “PRIVATE-NET” network object.

Step	Description
5.	The SG200 "Security Tab" window is displayed. Click the "Save" button to save the SG200 "Network Object" changes. 

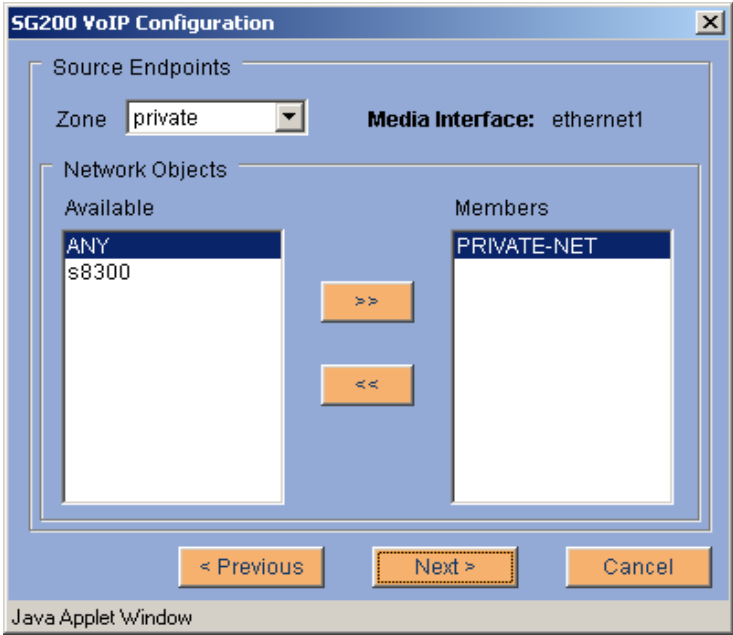
Step	Description
6.	Navigate to “Configure” → “Network Tab” → “NAT”. Check the “Enable NAT” parameter and the “Share Public Address To Reach Internet” parameter to globally enable NAT and PNAT, respectively, on the SG200 Security Gateway.  Click the “Add” button to add a NAT rule for the private voice network.
7.	The following fields are displayed in the “Add NAT Rule” window shown below: • Enable Rule – Check this box to enable the NAT rule. • Zone – Select “public” to apply the NAT rule to the public routable interface to the Wide Area Network (WAN). • Type – Select “Port” for PNAT. Original – Specify the source IP addresses/port numbers to be translated. • Option – Select “specify” to manually enter an IP address, Network Mask. • IP address – Enter the voice network IP address. • Mask – Enter subnet mask for the voice network. Translation – Specify the IP address and port range to which the source addresses/port numbers will be translated.

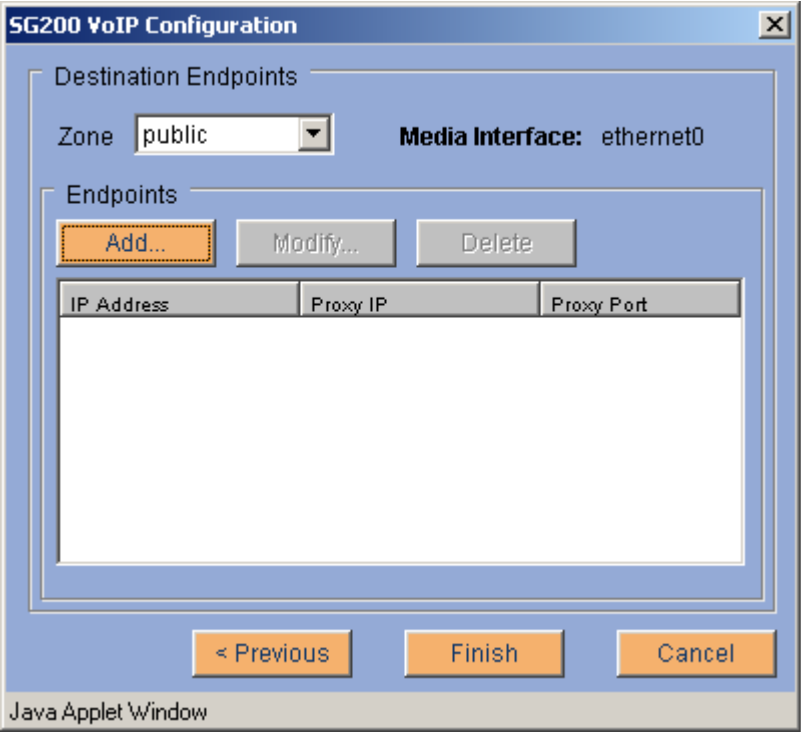
Step	Description
	• Option – Select “public” to translate the private IP addresses to the public routable IP address. • Start Port - Enter the start port number (default = 5000) for PNAT. • End Port – Enter the end port number (default = 65535) for PNAT.  Click the “OK” button to add the NAT rule.
8.	The “Configure” → “Network Tab” → “NAT” window is displayed. Click the “Add” button to add a second NAT rule for the private data network. The following fields are displayed in the “Add NAT Rule” window shown below: • Enable Rule – Check this box to enable the NAT rule. • Zone – Select “public” to apply the NAT rule to the public routable interface to the Wide Area Network (WAN). • Type – Select “Port” for PNAT. Original – Specify the source IP addresses/port numbers to be translated.

Step	Description
	• Option – Select “specify” to manually enter an IP address and network mask. • IP address – Enter the data network IP address. • Mask – Enter subnet mask for the data network. Translation – Specify the IP address and port range to translate the source addresses/port numbers to. • Option – Select “public” to translate the private IP addresses to the public routable IP address. • Start Port - Enter the start port number (default = 5000) for PNAT. • End Port – Enter the end port number (default = 65535) for PNAT. Click the “OK” button to add the NAT rule.

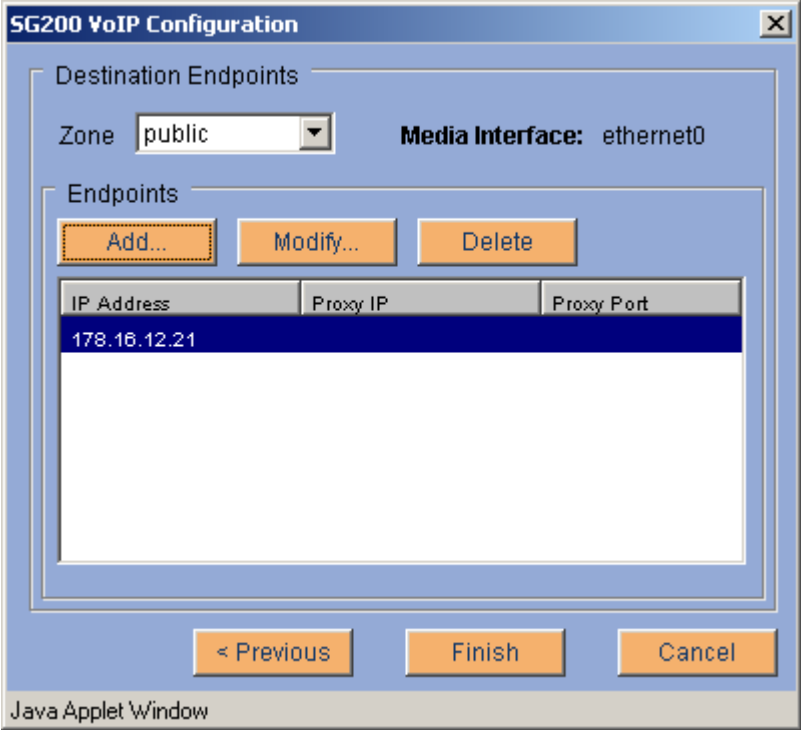
Step	Description
9.	The “Configure” → “Network Tab” → “NAT” window is displayed. Click the “Save” button to save the NAT rules.

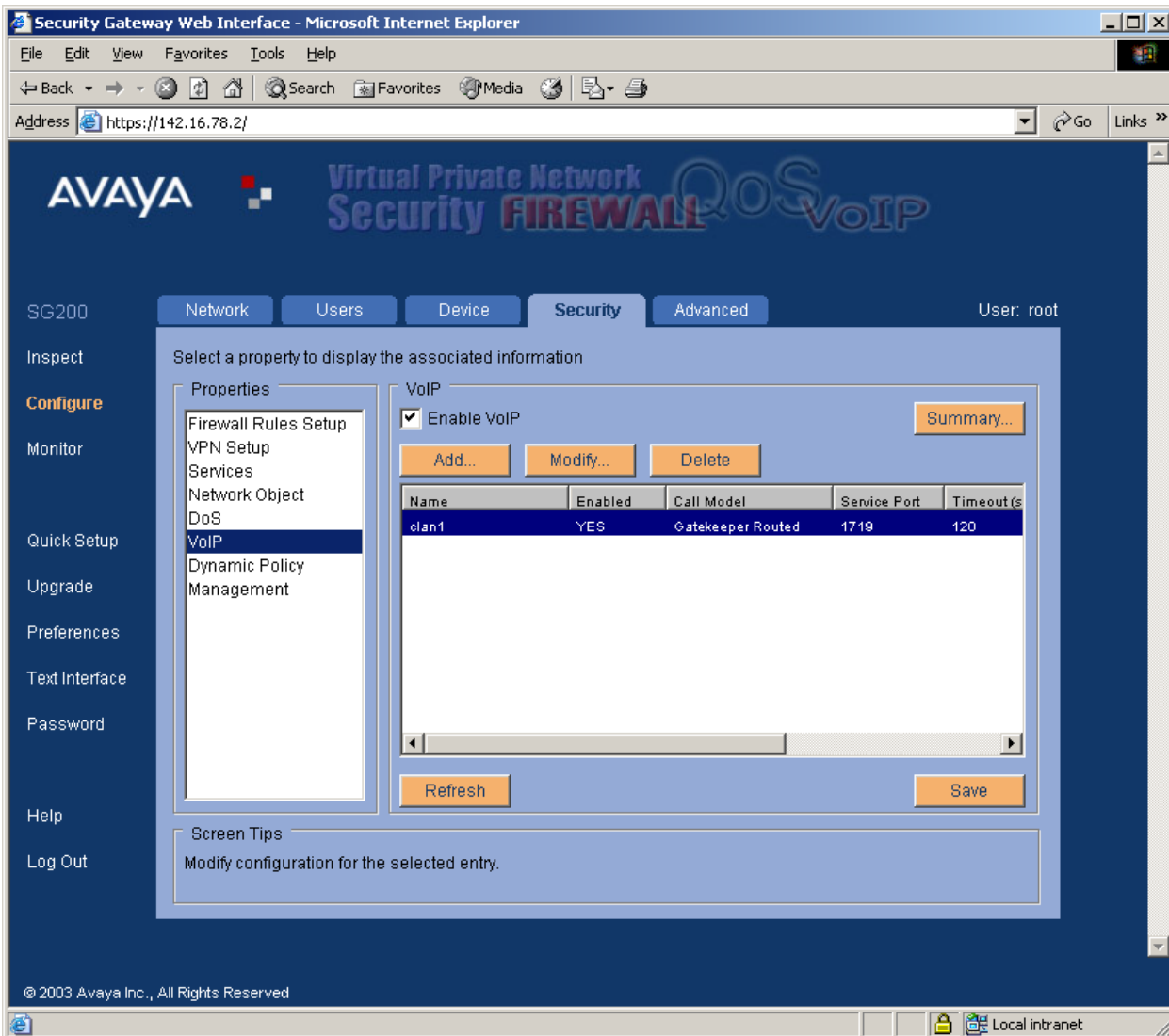
Step	Description
10.	Add an H.323 proxy VoIP rule. This rule instructs the SG200 how to manipulate H.323 signaling and media traffic through PNAT. Navigate to “Configure” → “Security Tab” → “VoIP”. Check the “Enable VoIP” check box to enable the VoIP feature globally on the SG200. Click the “Add” button. The following fields are displayed in the “SG200 VoIP Configuration” window: • Enable Rule – Check to enable the VoIP rule. • Name – Enter a unique name for the VoIP rule. • Call Model – Select “Gatekeeper Routed” to enable the rule for H.323 IP Endpoints. • Service Port – Enter destination port number for H.323 IP endpoint registration (Default port: 1719). • Timeout – Enter session timeout in seconds Click the “Next” button to continue.

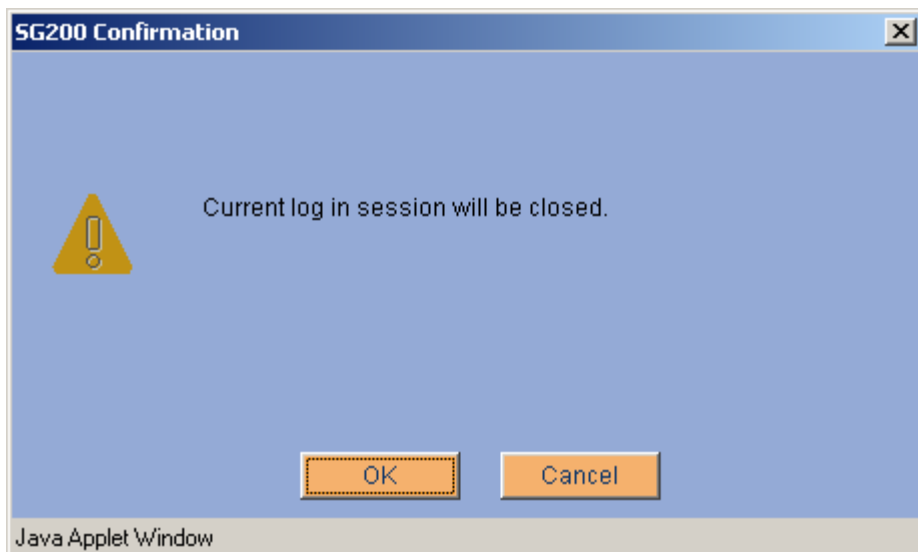
Step	Description
11.	Configure the source endpoints to which the H.323 proxy VoIP rule will be applied: Select the “private“ source endpoint “Zone“ to indicate the Avaya H.323 IP Endpoints are located on the private non-routable side of the SG200 Security Gateway. Move the “PRIVATE-NET“ network object from the “Available“ box to the “Members“ box, to specify to which IP Endpoints on the private side the rule will be applied.  Click the “Next” button to continue.

Step	Description
12.	Select the zone where the C-LAN card is located: Select the “public“ destination endpoint “Zone“ to indicate the C-LAN card is located on the public side. Click the “Add“ button to add the IP address of the C-LAN card located in the Headquarters office.  The image shows a Java Applet window titled "SG200 VoIP Configuration". It has a blue header bar with a close button (X) in the top right corner. The main content area is divided into two sections: "Destination Endpoints" and "Endpoints". In the "Destination Endpoints" section, there is a "Zone" dropdown menu currently set to "public" and a "Media Interface" label with the value "ethernet0". In the "Endpoints" section, there are three buttons: "Add..." (highlighted with an orange border), "Modify...", and "Delete". Below these buttons is a table with three columns: "IP Address", "Proxy IP", and "Proxy Port". The table is currently empty. At the bottom of the window, there are three buttons: "< Previous", "Finish", and "Cancel". The bottom-most bar of the window is labeled "Java Applet Window".

Step	Description
13.	The “Add Destination Endpoint” window is displayed. Enter the IP address of the C-LAN card in the “Endpoint IP” field. Leave the “Proxy IP” and “Proxy Port” fields blank. The Avaya H.323 IP endpoints use the “Endpoint IP” address to register to the Avaya S8700 Media Server. Click the “OK” button to add the C-LAN IP Address.

Step	Description
14.	The following “SG200 VoIP Configuration” window is displayed.  Click the “Finish” button to finish adding the VoIP rule.

Step	Description
15.	The “Configure” → “Security Tab” → “VoIP” window is displayed. Click the “Save” button to save the H.323 proxy VoIP rule.  Click the “Logout” button to log out of the SG200 Security Gateway.

Step	Description
16.	The “SG200 Confirmation” window is displayed:  The image shows a Java Applet Window titled "SG200 Confirmation". It has a blue background and a yellow warning icon on the left. The text in the center says "Current log in session will be closed." At the bottom, there are two buttons: "OK" and "Cancel". Click the “OK” button to log out of the Avaya SG200 Security Gateway.

4. Remote Office DHCP Server Configuration

The configuration depicted in **Figure 1** does not require any special DHCP scope configuration to support H.323 traffic over PNAT. For completeness, the table below summarizes the DHCP server configuration:

DHCP Scope	Option 3 Router	Option 176 String	Notes
10.3.2.0 (10.3.2.150-254)	10.3.2.1	L2Q=1,L2QVLAN=301	From untagged VLAN ID 302
10.3.1.0 (10.3.1.150-254)	10.3.1.1	MCIPADD=178.16.12.21, MCPORT=1719, TFTPSRVR=10.3.2.61	178.16.12.21 is the headquarters G600 C-LAN IP address.

Table 2: DHCP Server Configuration

The following occurs when an IP telephone is installed (or reset). The IP telephone initially sends an untagged DHCP request. The Avaya P333R switch port connected to the IP Telephone is configured with both an untagged and tagged VLAN. The untagged DHCP request is associated with the untagged VLAN on the port. The P333R switch layer-3 interface on the native (untagged) VLAN has IP address 10.3.2.1. When the P333R switch layer-3 interface relays the DHCP request to the configured DHCP server, it will use 10.3.2.1 as the source address. The DHCP server associates this request with the 10.3.2.0 scope and returns a reply

with option 176 string set, instructing the requestor to enable 802.1Q tagging with VLAN ID 301. The IP telephone receiving this reply will release the supplied IP address and issue a new DHCP request with VLAN ID 301. This request will be associated with the tagged VLAN on the port. The router interface of this VLAN has IP address 10.3.1.1 and will relay the DHCP request to the DHCP server with this address as the source. The DHCP server associates this address with scope 10.3.1.0 and replies with an IP address from that scope as well as several parameters in the Option 176 string, as indicated in the second row of **Table 2**.

When a computer issues a DHCP request, it too will send an untagged DHCP request. This request will be serviced like the initial request from the phone. However, the computer will ignore the Option 176 values specifying a new VLAN. Therefore, no new DHCP request is issued.

5. IP Telephone Station “IP Shuffling” Configuration

Since IP shuffling¹ is not supported by the current version of the Avaya SG200 Security Gateway shown in Section 2, the feature should be disabled on all IP stations behind PNAT. To disable IP shuffling, type “change station <station ID>” at the System Access Terminal (SAT), go to Page 2, and match the highlighted parameter in **Figure 2**. Then apply the changes.

```

Telnet 135.8.23.11
change station 38108                                     Page 2 of 3
STATION
FEATURE OPTIONS
  LWC Reception: spe                                     Auto Select Any Idle Appearance? n
  LWC Activation? y                                     Coverage Msg Retrieval? y
  LWC Log External Calls? n                             Auto Answer: none
  CDR Privacy? n                                       Data Restriction? n
  Redirect Notification? y                             Idle Appearance Preference? n
  Per Button Ring Control? n                           Restrict Last Appearance? y
  Bridged Call Alerting? n
  Active Station Ringing: single
  H.320 Conversion? n                                  Per Station CPN - Send Calling Number?
  Service Link Mode: as-needed
  Multimedia Mode: enhanced
  MMI Served User Type:
  AUDIX Name:
  Emergency Location Ext: 38102
  Display Client Redirection? y
  Select Last Used Appearance? n
  Coverage After Forwarding? s
  Multimedia Early Answer? n
  Direct IP-IP Audio Connections? n
  IP Audio Hairpinning? y
ESC-x=Cancel Esc-e=Submit Esc-p=Prev Pg Esc-n=Next Pg Esc-h=Help Esc-r=Refresh

```

Figure 2: Change Station Form – IP Shuffling

¹ Please note that shuffling is known as “Direct IP-IP Audio Connections” by the Avaya S8700 Media Server.

6. Verification Steps

In the field, the following tests can be performed to verify the Avaya SG200 VoIP H.323 proxy feature over PNAT:

1. Verify that at least two Avaya IP Endpoints on the private side are able to register to the Avaya S8700 Media Server located at the headquarters office on the public side.
2. Verify two simultaneous calls can be placed between two Avaya IP endpoints located at the remote site and two Avaya IP Endpoints located at the headquarters office. Verify two way talk path exists on both calls.

The “status station <station ID>” command (Page 3) can be issued from the Avaya S8700 Media Server SAT to find out the NAT’ed IP addresses and port numbers used by each IP station for signaling and media traffic.

7. Conclusion

The Avaya SG200 Security Gateway can be successfully configured to handle H.323 VoIP traffic over PNAT originating from Avaya’s IP Endpoints with Avaya Communication Manager Release 1.3. The Avaya SG200 Security Gateway transparently manipulates H.323 traffic signaling and media streams, thus providing seamless end-to-end VoIP transmission.

©2003 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya Solution & Interoperability Test Lab at interoplabnotes@list.avaya.com