



Avaya Solution & Interoperability Test Lab

Application Notes for NetScout nGenius with Avaya Communication Manager running on the Avaya S8300 Media Server and Avaya G700 Media Gateway - Issue 1.0

Abstract

These Application Notes describe the configuration steps required for NetScout nGenius to successfully interoperate with the Avaya Communication Manager running on the Avaya S8300 Media Server and Avaya G700 Media Gateway. Features and functionality were validated and performance testing was conducted in order to verify operation under load. Information in these Application Notes has been obtained through compliance testing and additional technical discussions. Testing was conducted via the Developer*Connection* Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describe the compliance-tested configuration utilizing Avaya Communication Manager on an Avaya S8300 Media Server with NetScout nGenius monitoring the traffic via port mirroring.

NetScout nGenius provides customers a unified performance management solution. Key performance management disciplines, application and network monitoring, capacity planning, troubleshooting, fault prevention, and service-level management are fully integrated into a single management application, providing a total network view through a browser interface. For customers wanting to monitor their converged infrastructure, nGenius allows the monitoring of the RTP streams associated with IP telephony devices such as telephones and media gateways. In this configuration, the monitoring of RTP streams is done via port mirroring. This sample configuration utilizes an Avaya P333T-PWR switch, which requires a one-to-one mapping between the mirror source and destination ports (i.e., a number of ports cannot be mirrored to a single port). This is why the uplink port, rather than the phone ports or voice VLAN, is mirrored. Refer to the document “Application Notes for NetScout nGenius with Avaya Communication Manager and Extreme Networks Summit 48” for more information on port mirroring options that are better suited for Avaya Communication Manager running on Media Server and Media Gateways combinations other than the S8300/G700.

As seen in **Figure 1**, Avaya Communication Manager runs on the Avaya S8300 Media Server. In this sample configuration, Avaya IP Telephones have been configured with and without direct IP-IP connections. Either setting can be used, depending on the end customer requirements with regard to the monitoring of IP telephones. The P333T-PWR is functioning as a Layer 2 switch, where port 1/24 is the uplink to the network. The P333T-PWR provides power over Ethernet to the IP telephones, and a port provisioned to mirror the network uplink provides the information to the NetScout probe. A DHCP server and a TFTP server reside on the 192.45.50.0 network to support the IP telephones, but their configurations are not specific to the integration with NetScout. As such, they are not discussed.

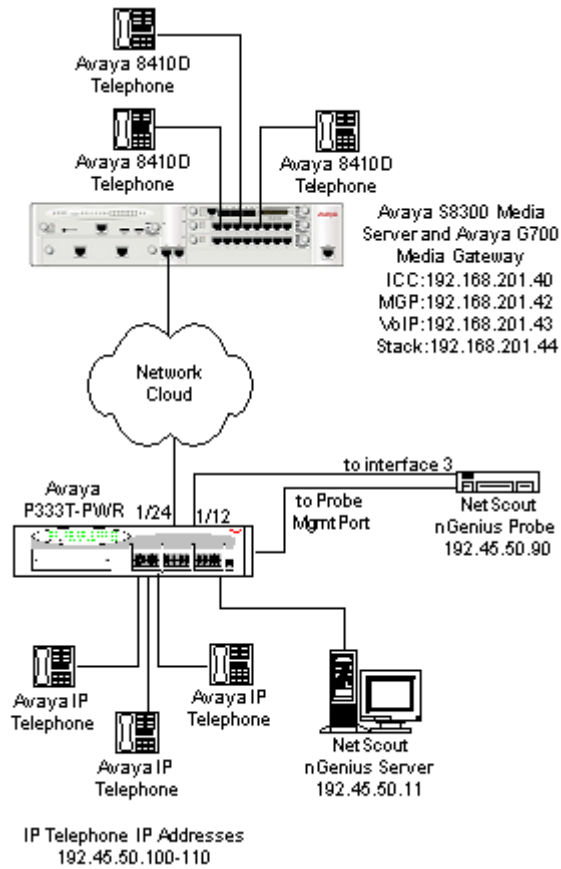


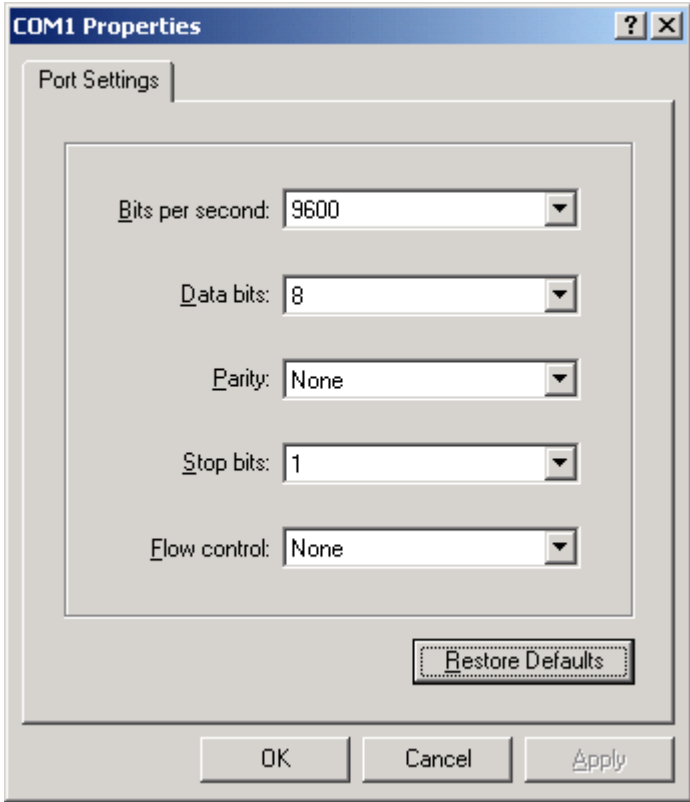
Figure 1: Avaya DeveloperConnection Compliance Test Configuration

2. Equipment and Software Validated

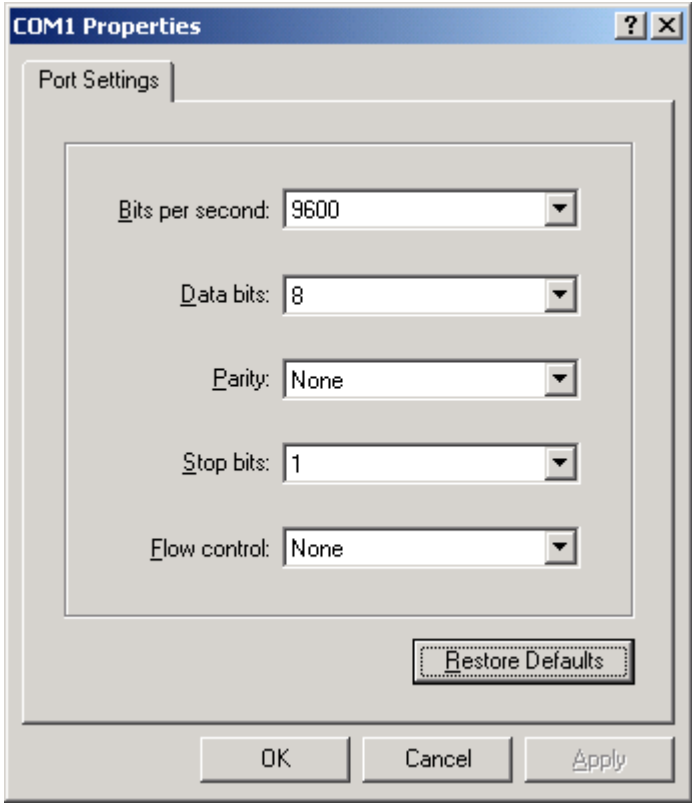
The following equipment and software were used for the sample configuration provided:

Equipment	Software
Avaya S8300 Media Server and Avaya G700 Media Gateway	Avaya Communication Manager 2.0
Avaya P333T-PWR Stackable Switch	3.12.1
Avaya IP Telephones <ul style="list-style-type: none"> • Avaya 4606 IP Telephone • Avaya 4620 IP Telephone • Avaya 4624 IP Telephone 	R 1.81
NetScout nGenius Server	Version 2.0.1 Build 1420
NetScout nGenius 8241ET Probe	V6.0.1 (Build 109)

3. Configure the Avaya P333T-PWR

Step	Description
1.	<p>Connect a console cable to the P333T-PWR. Use Hyperterm with the settings shown below:</p> 
2.	Log in using the appropriate credentials and enter configuration mode. Enter the command “set port mirror source-port 1/24 mirror-port 1/12 sampling always direction both” .
3.	Connect port 1/24 to the network.
4.	Connect port 1/12 to Interface 3 on the NetScout probe.

4. Configure the NetScout Probe

Step	Description
1.	<p>Connect a console cable to the NetScout probe console port. Use Hyperterm with the settings shown below:</p>  <p>The screenshot shows a Windows dialog box titled "COM1 Properties" with a "Port Settings" tab selected. The settings are as follows:</p> <ul style="list-style-type: none">Bits per second: 9600Data bits: 8Parity: NoneStop bits: 1Flow control: None <p>Buttons at the bottom include "Restore Defaults", "OK", "Cancel", and "Apply".</p>

Step	Description
2.	<p>Once connected, enter 1 to change the IP address of the probe. When prompted, enter the IP address 192.45.50.90 and press Enter.</p> <div style="border: 1px solid black; padding: 10px; margin: 10px 0;"> <pre> ***** NetScout Model 8241ET V6.0.1 (Build 109 - Extended H323) ***** Interface number : 3 [1] Change IP Address 192.45.50.90 [2] Change Net Mask 255.255.255.0 [3] Change Default Gateway Address Not configured [4] Change Config Server Address Not configured [5] Change Read Community public [6] Change Write Community public [7] Select Interface FAST-ETHERNET [8] Software Options [9] Agent Options [10] Download Firmware [11] Enter Command-line mode [12] Reset Agent [13] Security Options [14] Console Logout Enter your response or hit Esc to Abort Selection#:</pre> </div>
4.	<p>Enter 3 to change the gateway address of the probe. When prompted, enter the IP address 192.45.50.1 and press Enter.</p> <div style="border: 1px solid black; padding: 10px; margin: 10px 0;"> <pre> ***** NetScout Model 8241ET V6.0.1 (Build 109 - Extended H323) ***** Interface number : 3 [1] Change IP Address 192.45.50.90 [2] Change Net Mask 255.255.255.0 [3] Change Default Gateway Address 192.45.50.1 [4] Change Config Server Address Not configured [5] Change Read Community public [6] Change Write Community public [7] Select Interface FAST-ETHERNET [8] Software Options [9] Agent Options [10] Download Firmware [11] Enter Command-line mode [12] Reset Agent [13] Security Options [14] Console Logout Enter your response or hit Esc to Abort Selection#:</pre> </div>

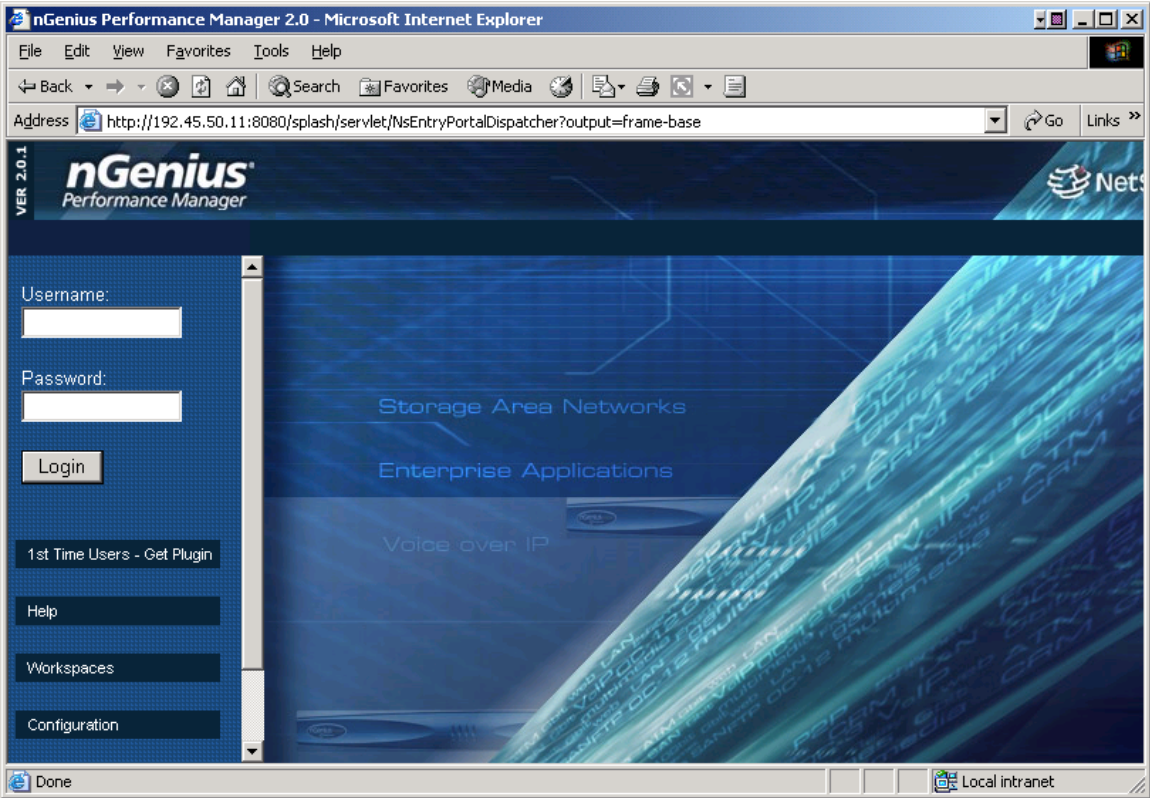
Step	Description
5.	<p>Enter 8 to change Software Options.</p> <div style="border: 1px solid black; padding: 10px; margin: 10px 0;"> <p style="text-align: center;">***** NetScout Model 8241ET V6.0.1 (Build 109 - Extended H323) *****</p> <p>Interface number : 3</p> <p>[1] Change IP Address 192.45.50.90 [2] Change Net Mask 255.255.255.0 [3] Change Default Gateway Address 192.45.50.1 [4] Change Config Server Address Not configured [5] Change Read Community public [6] Change Write Community public [7] Select Interface FAST-ETHERNET [8] Software Options [9] Agent Options [10] Download Firmware [11] Enter Command-line mode [12] Reset Agent [13] Security Options [14] Console Logout</p> <p style="text-align: center;">Enter your response or hit Esc to Abort</p> <p>Selection#: 8</p> </div>
6.	<p>At the Software Options Menu, enter 1 to set Multi-Media Monitor to on. Enter 99 to return to the main menu..</p> <div style="border: 1px solid black; padding: 10px; margin: 10px 0;"> <p style="text-align: center;">***** NetScout Model 8241ET V6.0.1 (Build 109 - Extended H323) *****</p> <p>Software Options Menu:</p> <p>[1] Multi-Media Monitor on [2] Response Time Monitor off [3] NL and AL Host off [4] NL and AL Conversation off [6] All Host off [7] All Conversation off [8] Tunnel Parsing off</p> <p>[99] Go Back to Main Menu</p> </div>

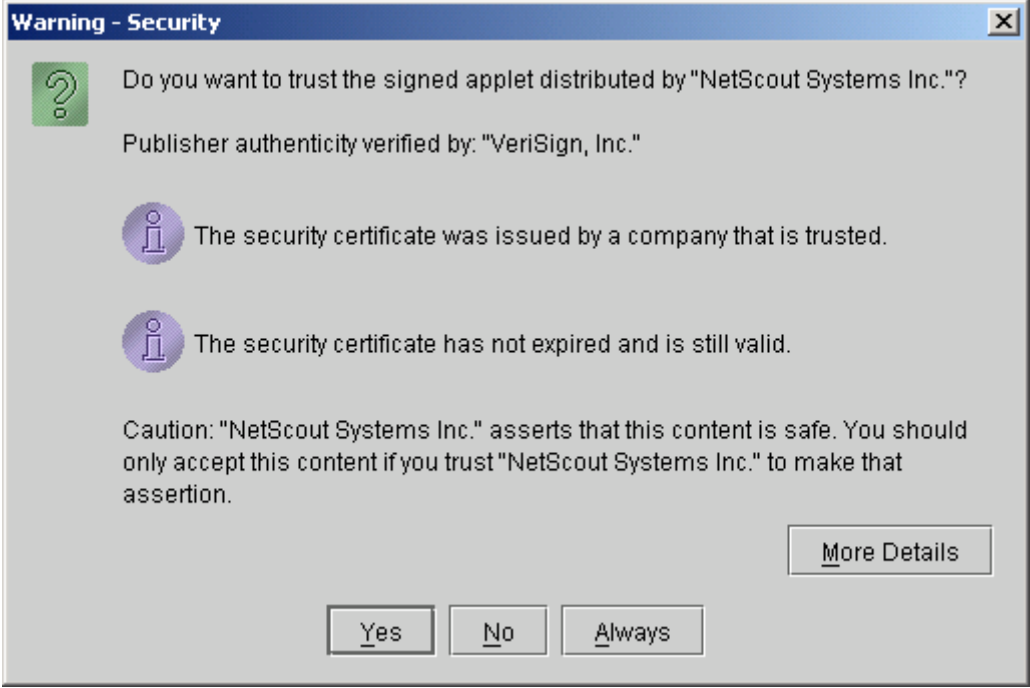
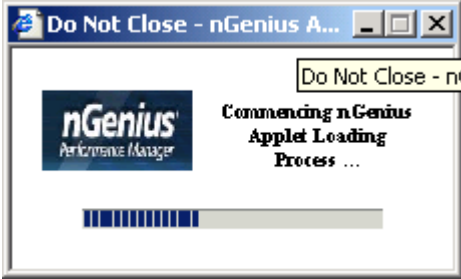
Step	Description
7.	<p>At the main menu, enter 11 to Enter Command-line mode.</p> <div style="border: 1px solid black; padding: 10px; margin: 10px 0;"> <pre> ***** NetScout Model 8241ET V6.0.1 (Build 109 - Extended H323) ***** Interface number : 3 [1] Change IP Address 192.45.50.90 [2] Change Net Mask 255.255.255.0 [3] Change Default Gateway Address 192.45.50.1 [4] Change Config Server Address Not configured [5] Change Read Community public [6] Change Write Community public [7] Select Interface FAST-ETHERNET [8] Software Options [9] Agent Options [10] Download Firmware [11] Enter Command-line mode [12] Reset Agent [13] Security Options [14] Console Logout Enter your response or hit Esc to Abort Selection#: 11 </pre> </div>
8.	<p>Type the command get mmon to view the Extended H323 settings.</p> <div style="border: 1px solid black; padding: 10px; margin: 10px 0;"> <pre> Enter "quit" to exit command-line mode % get mmon sccp_port 2000 mgcp_port 2427 sip_port 5060 Extended_H323 off </pre> </div>

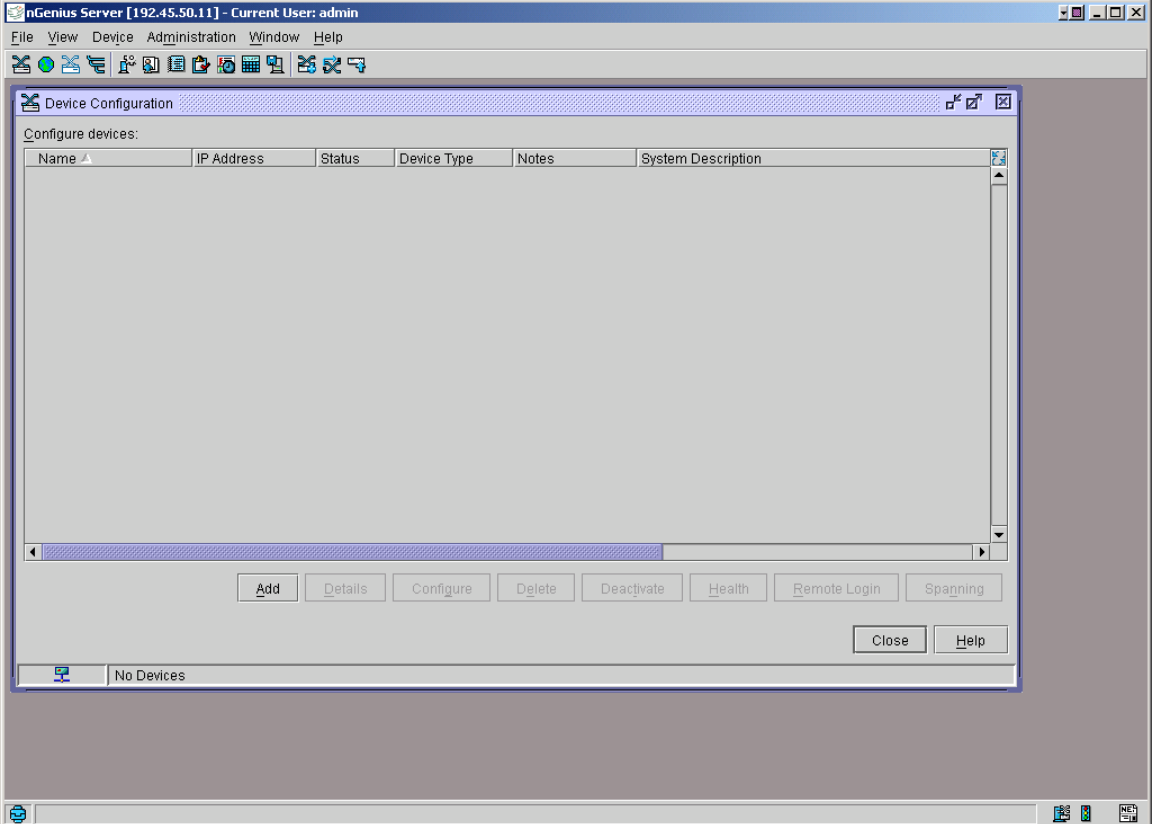
Step	Description
<p>9.</p>	<p>Type the command set mmon Extended_H323 on to set the Extended H323 field. Enter get mmon to verify the modified Extended H323 settings.</p> <div data-bbox="323 384 1422 861" style="border: 1px solid black; padding: 10px;"> <pre> Enter "quit" to exit command-line mode % get mmon sccp_port 2000 mgcp_port 2427 sip_port 5060 Extended_H323 off % set mmon Extended_H323 on % get mmon sccp_port 2000 mgcp_port 2427 sip_port 5060 Extended_H323 on </pre> </div>
<p>10.</p>	<p>Reboot the probe by typing do reset. Enter y and press Enter to confirm.</p> <div data-bbox="323 953 1422 1121" style="border: 1px solid black; padding: 10px;"> <pre> % do reset WARNING : agent will be reset, confirm [n] y </pre> </div>

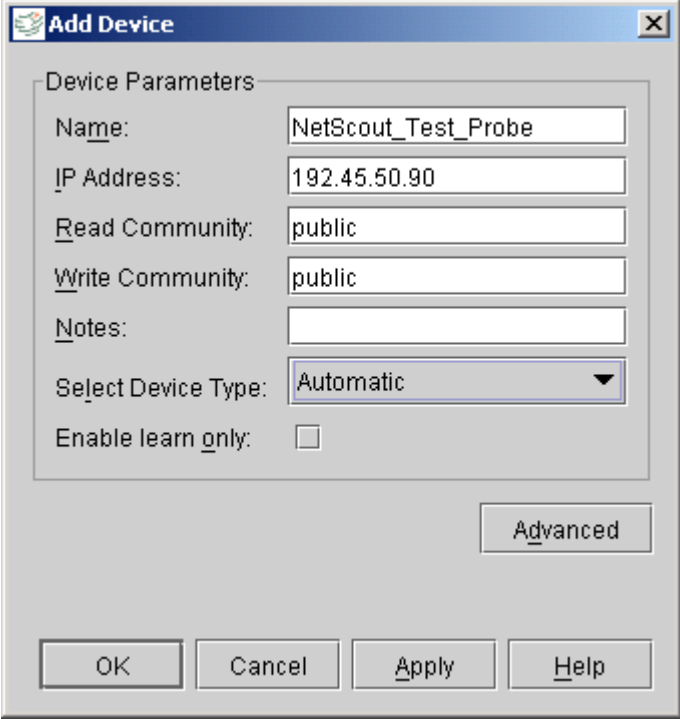
5. Configure the NetScout nGenius Server

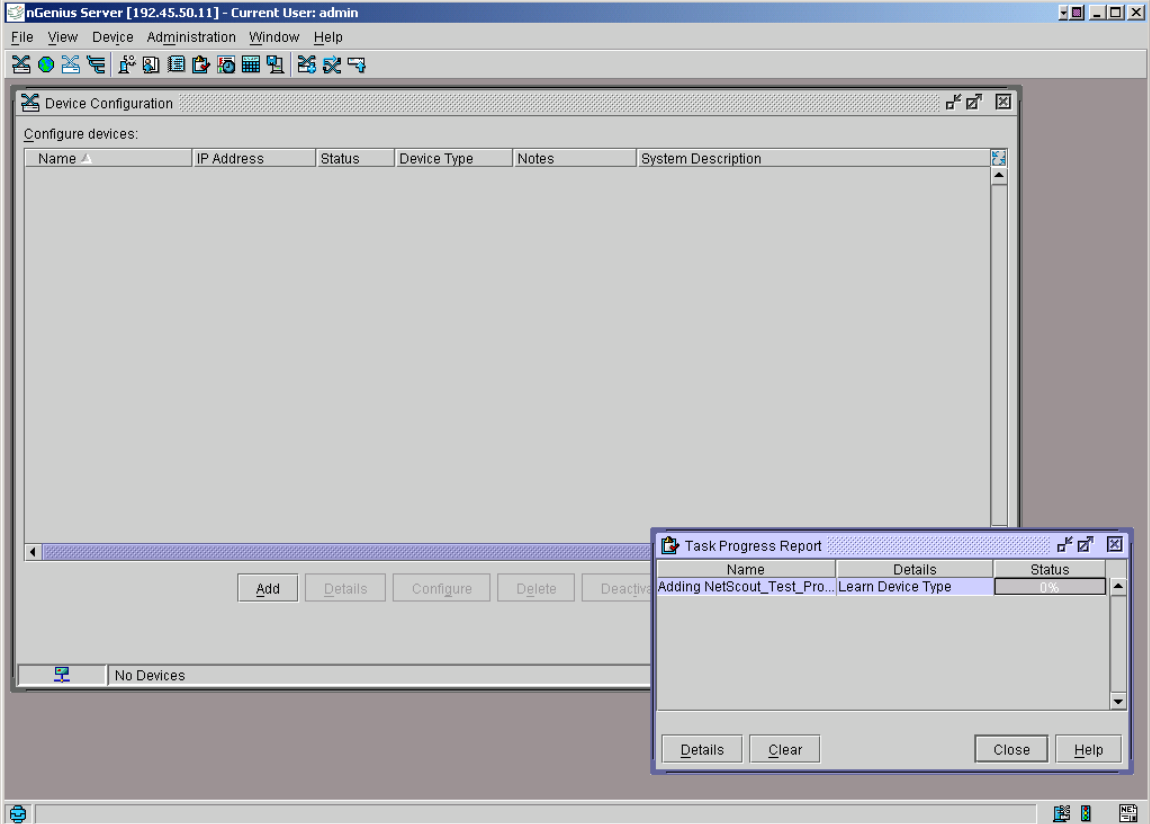
Installation of the NetScout server software is a straightforward task that requires no additional instruction. In some cases, NetScout may ship a pre-installed server to the end customer. As such, the installation process of the server is not documented in these Application Notes. However, the probes must be provisioned on the nGenius server. This is done via the web as shown in the following steps.

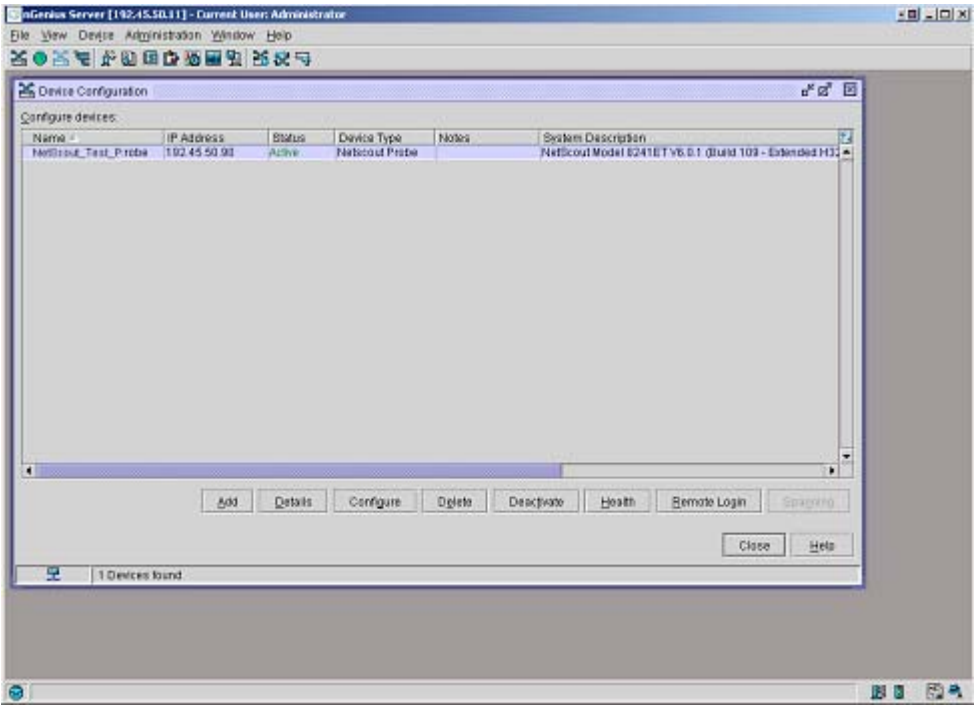
Step	Description
1.	<p>Open a browser and enter the IP address of the NetScout nGenius Server, followed by :8080, as shown below.</p> 

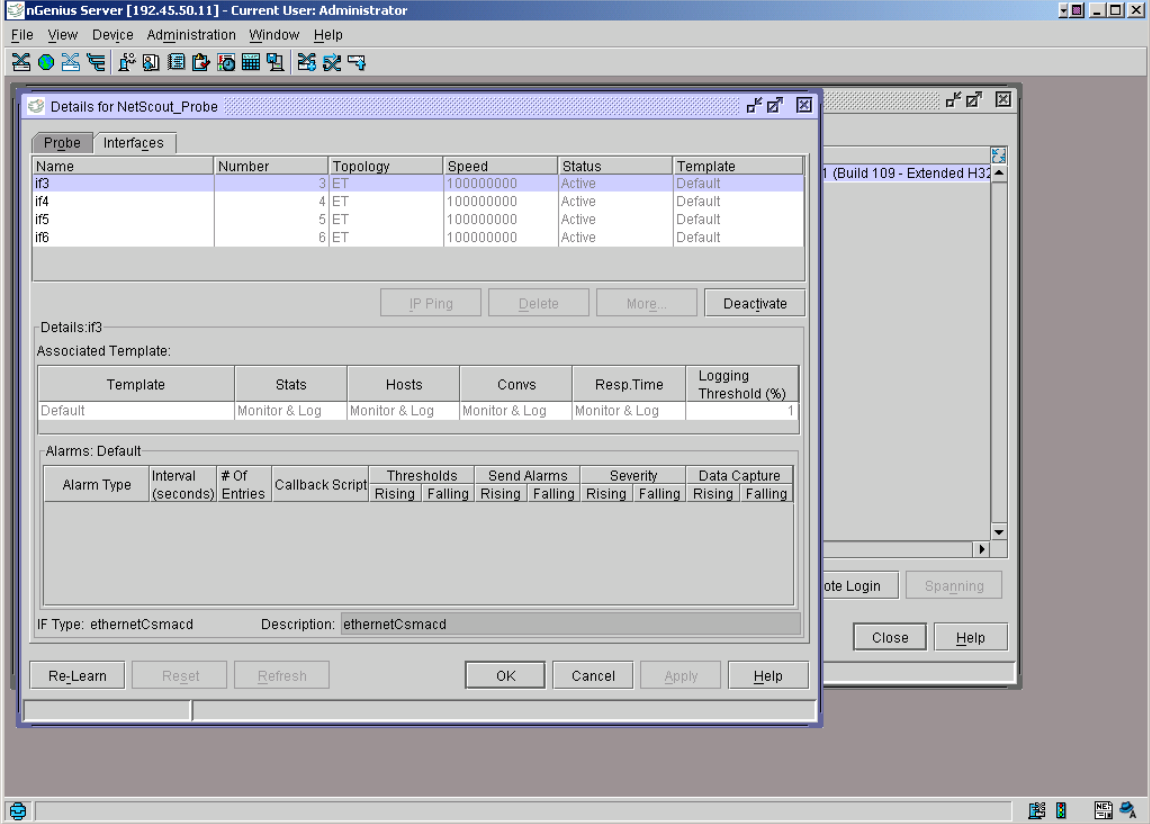
Step	Description
2.	<p>Enter the proper credentials and log into the server. The following dialog box will be displayed. Click Always.</p>  <p>The image shows a Windows-style dialog box titled "Warning - Security". It contains a question mark icon and the text: "Do you want to trust the signed applet distributed by 'NetScout Systems Inc.'? Publisher authenticity verified by: 'VeriSign, Inc.'". Below this are two information icons with text: "The security certificate was issued by a company that is trusted." and "The security certificate has not expired and is still valid." At the bottom, there is a "Caution" message: "Caution: 'NetScout Systems Inc.' asserts that this content is safe. You should only accept this content if you trust 'NetScout Systems Inc.' to make that assertion." and buttons for "Yes", "No", "Always", and "More Details".</p>
3.	<p>The following box will be displayed. At some point, this box will minimize to the task bar and will no longer be seen.</p>  <p>The image shows a dialog box titled "Do Not Close - nGenius A...". It features the nGenius Performance Manager logo and the text: "Commencing nGenius Applet Loading Process ...". Below the text is a progress bar with several blue segments.</p>

Step	Description
4.	<p>Return to the browser shown in Step 1 and click Server Administration. The following window is displayed. Click Add.</p> 

Step	Description
5.	<p>Enter the name and IP address for the nGenius Probe as shown below (other settings are default). Click Apply and OK.</p> 

Step	Description
6.	<p>The window will display an update as the probe is being added to the system, as shown below. When the status is shown as complete, click Close.</p>  <p>The screenshot shows the nGenius Server application window. The main window has a menu bar (File, View, Device, Administration, Window, Help) and a toolbar. Below the toolbar is a 'Device Configuration' window with a table titled 'Configure devices:'. The table has columns: Name, IP Address, Status, Device Type, Notes, and System Description. Below the table are buttons for 'Add', 'Details', 'Configure', 'Delete', and 'Deactivate'. At the bottom of the main window, it says 'No Devices'. A 'Task Progress Report' dialog box is open in the foreground, containing a table with columns: Name, Details, and Status. The table has one row: 'Adding NetScout_Test_Pro...' with 'Learn Device Type' in the details and '0%' in the status. Below the table are buttons for 'Details', 'Clear', 'Close', and 'Help'.</p>

Step	Description												
7.	<p>The probe will now be listed. Highlight the entry and click Details.</p>  <p>The screenshot shows the 'Device Configuration' window in the iGenius Server application. The window title is 'iGenius Server [192.45.50.11] - Current User: Administrator'. The main area contains a table with the following data:</p> <table border="1"> <thead> <tr> <th>Name</th> <th>IP Address</th> <th>Status</th> <th>Device Type</th> <th>Notes</th> <th>System Description</th> </tr> </thead> <tbody> <tr> <td>NetScout_Test_Probe</td> <td>192.45.50.93</td> <td>Active</td> <td>NetScout Probe</td> <td></td> <td>NetScout Model 8241ET V6.0.1 (Build 103 - Extended H3)</td> </tr> </tbody> </table> <p>Below the table are several buttons: Add, Details, Configure, Delete, Disable, Health, Remote Login, and a disabled 'Spinning' button. At the bottom right are 'Close' and 'Help' buttons. A status bar at the bottom left indicates '1 Devices found'.</p>	Name	IP Address	Status	Device Type	Notes	System Description	NetScout_Test_Probe	192.45.50.93	Active	NetScout Probe		NetScout Model 8241ET V6.0.1 (Build 103 - Extended H3)
Name	IP Address	Status	Device Type	Notes	System Description								
NetScout_Test_Probe	192.45.50.93	Active	NetScout Probe		NetScout Model 8241ET V6.0.1 (Build 103 - Extended H3)								

Step	Description
8.	<p>Verify the interfaces listed for the probe. Click Re-learn to complete loading the configuration. When complete, click OK.</p> 

6. Configure Avaya Communication Manager

The following steps describe how to toggle the Direct IP-IP Audio Connections field as per end customer requirements. If the end customer determines that only IP telephone calls to and from the media server are to be monitored (as is the case when calls require the media gateway, i.e. analog or digital tunks), then the Direct IP-IP Audio Connections can be set to **yes**. Otherwise, if calls between IP telephones on the same edge device are to be monitored, then set the Direct IP-IP Audio Connections field to **no**. Note that setting this field to **no** will require additional VoIP resources on the gateway and WAN bandwidth.

Direct IP-IP Audio Connections must be administered in the IP network region. For completeness, it is recommended to set the IP Audio Hairpinning field to the same value. For this configuration, this value shall be set to **no**, in order to monitor the IP telephone media streams.

Basic administration, such as initial provisioning of the media server and the adding of IP telephones, is assumed and is therefore beyond the scope of these Application Notes.

Step	Description
1.	<p>Connect to the System Access Terminal (SAT) and log in with the proper credentials and terminal type. The following screen will be displayed:</p> <div data-bbox="321 520 1487 1037" style="border: 1px solid black; padding: 20px; text-align: center;"><pre>This system is restricted to authorized users for legitimate business purposes. Unauthorized access is a criminal violation of the law. Copyright (c) 1992 - 2003 Avaya Inc. Unpublished & Not for Publication All Rights Reserved</pre></div>

Step	Description
2.	<p>Enter the command change ip-network-region 1. Set the Intra-region and Inter-region Direct IP-IP Audio Connections and IP Audio Hairpinning fields to the desired value, in this case no and n, respectively.</p> <pre data-bbox="324 436 1484 1066"> change ip-network-region 1 Page 1 of 19 IP NETWORK REGION Region: 1 Location: Home Domain: Name: Intra-region IP-IP Direct Audio: no Inter-region IP-IP Direct Audio: no IP Audio Hairpinning? n AUDIO PARAMETERS Codec Set: 1 UDP Port Min: 2048 UDP Port Max: 3028 RTCP Reporting Enabled? y RTCP MONITOR SERVER PARAMETERS Use Default Server Parameters? y DIFFSERV/TOS PARAMETERS Call Control PHB Value: 34 Audio PHB Value: 46 802.1P/Q PARAMETERS Call Control 802.1p Priority: 7 Audio 802.1p Priority: 6 AUDIO RESOURCE RESERVATION PARAMETERS RSVP Enabled? n H.323 IP ENDPOINTS H.323 Link Bounce Recovery? y Idle Traffic Interval (sec): 20 Keep-Alive Interval (sec): 5 Keep-Alive Count: 5 ESC-x=Cancel Esc-e=Submit Esc-p=Prev Pg Esc-n=Next Pg Esc-h=Help Esc-r=Refresh </pre>

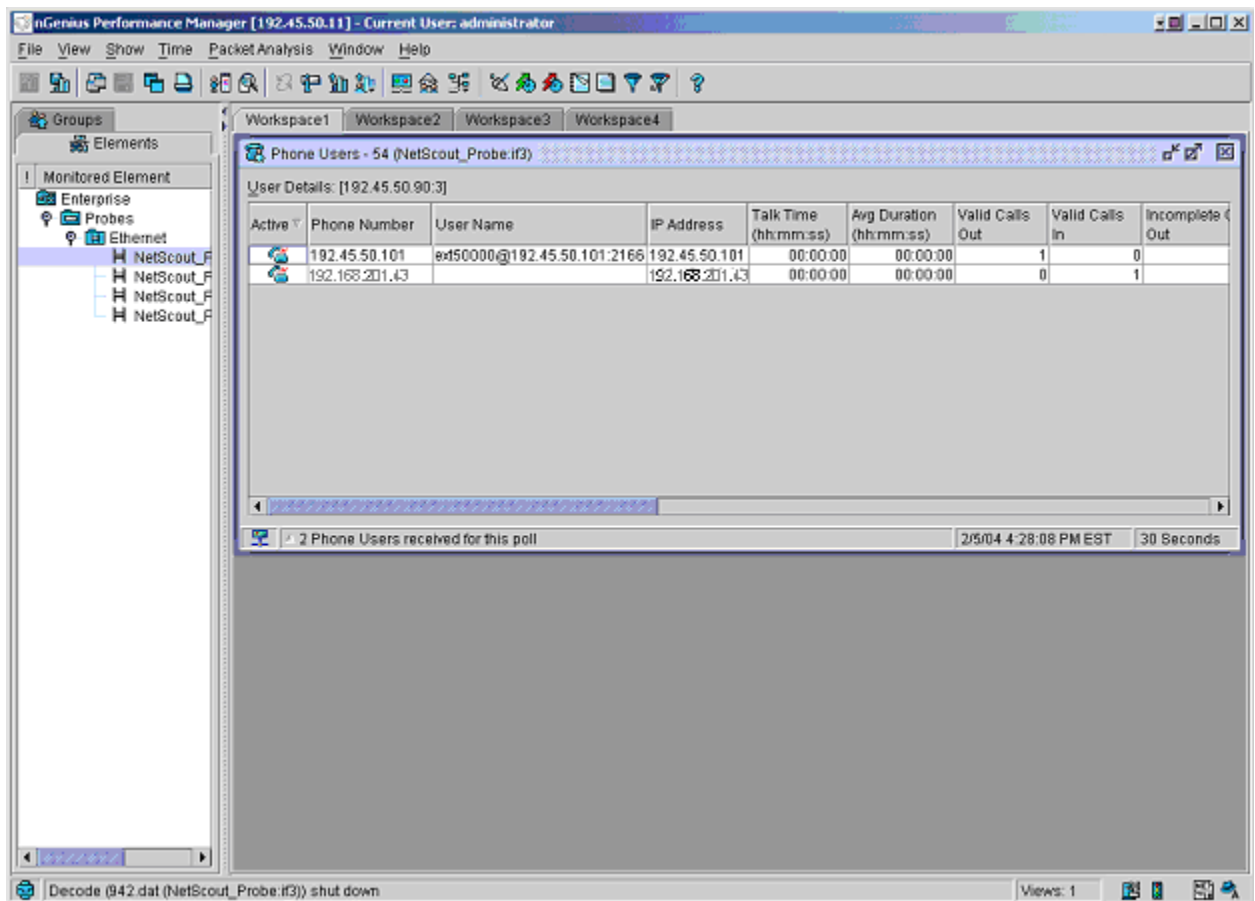
7. Interoperability Compliance Testing

Interoperability compliance tests included feature, functionality, and performance testing. Feature and functionality testing examined the nGenius client's ability to monitor IP telephone features such as making, receiving, transferring, and conferencing calls. Feature and functionality testing was verified using manual methods. Performance testing was conducted using a bulk call generator to place calls to IP telephones and verifying the results shown by the nGenius client.

8. Verification Steps

This configuration was verified in a test environment with the use of network tools. In the field, the following verification steps can be performed to test the interoperability at stages where incorrect configuration is most likely.

- a) Network Connectivity – Ping between the media server and the nGenius server, from the nGenius server to the nGenius Probe, and from the nGenius server to the IP Telephone. Verify all devices ping each other successfully.
- b) Telephony Connectivity: Station – Place calls to and from the IP Telephone. Verify that the calls are shown by the nGenius Client. A sample screen is shown below, indicating an active call between an IP telephone and the media gateway's VoIP resource.



9. Support

Technical support at NetScout can be reached at 1-888-357-7667. Alternatively, they can be reached by sending email to support@netscout.com.

10. Conclusion

These Application Notes describe the configuration steps required to configure NetScout nGenius and Avaya Communication Manager to successfully interoperate. Features and functionality were tested, and performance testing was conducted to validate the solution.

11. Additional References

The following documents may be used for more information:

- “Application Notes for NetScout nGenius with Avaya Communication Manager and Extreme Summit48,” available at <http://www1.avaya.com/enterprise/resourcelibrary/applicationnotes/devconnect.html>
- Administration for Network Connectivity for Avaya MultiVantage™ Software – Document ID 555-233-504, available at <http://support.avaya.com>.
- Administrators Guide for Avaya MultiVantage™ Software – Document ID 555-233-506, available at <http://support.avaya.com>.
- NetScout nGenius Probe Agent Administrator Guide
- NetScout Probe Hardware Guide

©2004 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 Developer*Connection* Program at devconnect@avaya.com.