**Avaya Solution & Interoperability Test Lab**

# Application Notes for Network Physics NetSensory Solution Insight for VoIP in an Avaya IP Telephony Environment – Issue 1.0

## Abstract

These Application Notes describe the configuration steps required for Network Physics NetSensory Solution Insight for VoIP to interoperate in an Avaya IP Telephony environment, consisting of Avaya Communication Manager, Avaya 4610SW IP Telephones and Avaya 9600 Series IP Telephones. In the compliance testing, NetSensory monitored the IP traffic from the Avaya IP telephones, and produced information to help identify network performance problems.

Information in these Application Notes has been obtained through Developer*Connection* compliance testing and additional technical discussions. Testing was conducted via the Developer*Connection* Program at the Avaya Solution and Interoperability Test Lab.

# 1. Introduction

NetSensory Solution Insight for VoIP is a network monitor and analysis application from Network Physics. The interoperability testing is in an Avaya IP Telephony environment, consisting of Avaya Communication Manager, Avaya 4610SW IP Telephones and Avaya 9600 Series IP Telephones. In the compliance testing, NetSensory monitored the IP traffic from the Avaya IP telephones, and produced information to help identify network performance problems.

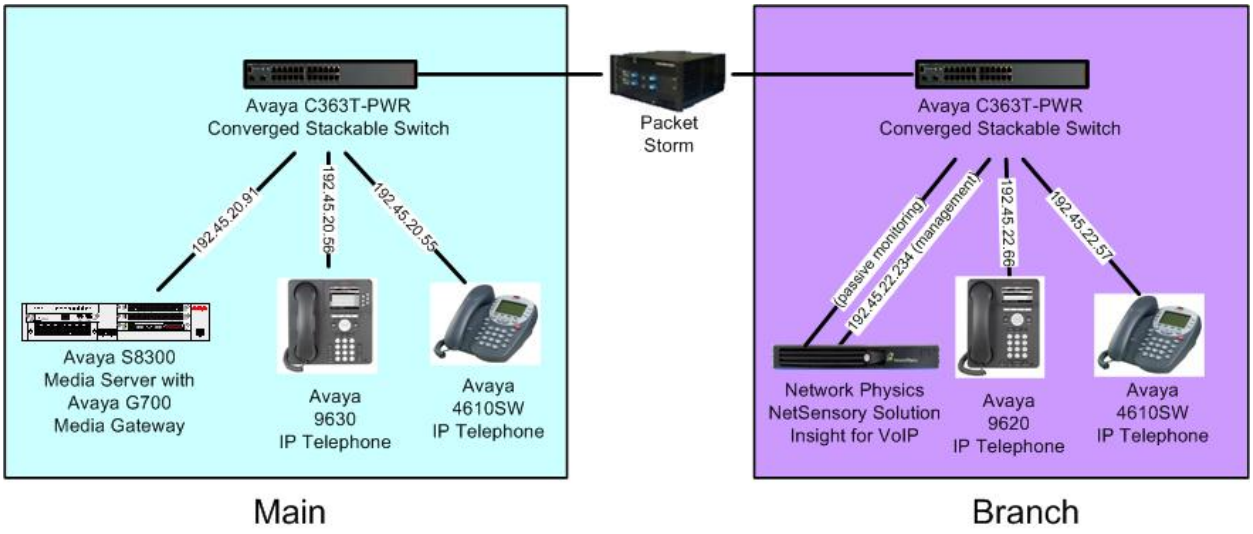



**Figure 1: Network Physics NetSensory Solution Insight for VoIP in an Avaya IP Telephony Environment**

In the test configuration shown in **Figure 1**, NetSensory monitored the Avaya 4610SW IP and Avaya 9620 IP telephones at the Branch site. The Packet Storm was used as a tool to inject network impairments, such as jitter/delay/loss, into the network for calls between the Main and Branch sites.

For the compliance testing, NetSensory was running on the Network Physics NP-2000 platform with NetSensory Enterprise OS. There were two connections from NetSenory to the Avaya C363T-PWR Converged Stackable Switch. One connection was used to connect to the NetSensory management interface, and the other to connect to the NetSensory monitoring interface. The port that connects to the Packet Storm on the Avaya C363T-PWR Converged Stackable Switch in the Branch site was mirrored to the port connecting to the NetSensory passive monitoring interface. This would enable NetSensory to receive a copy of all IP traffic between the two sites. A single copper span port from the NetSensory monitoring interface was used in the compliance testing.

The Avaya IP Telephony infrastructure is not the focus of these Application Notes and will not be described. Furthermore, the port mirroring on the Avaya C363T-PWR Converged Stackable Switch and the network impairment injection from the Packet Storm will also not be described.

## 2. Equipment and Software Validated

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

| Equipment | Software |
|---|---|
| Avaya S8300 Media Server with<br>G700 Media Gateway | Avaya Communication Manager 3.1.2,<br>R013x.01.2.632.1 |
| Avaya C363T-PWR Converged Stackable Switches | 4.3.12 |
| Avaya 4610SW IP Telephones (H.323) | 2.7 |
| Avaya 9620 IP Telephone (H.323) | 1.2 |
| Avaya 9630 IP Telephone (H.323) | 1.2 |
| Packet Storm | 10.5v1 |
| Network Physics NetSensory Solution Insight for VoIP<br>with NP-2000 NetSensory Enterprise | 1.0.224<br>5.3.2 |

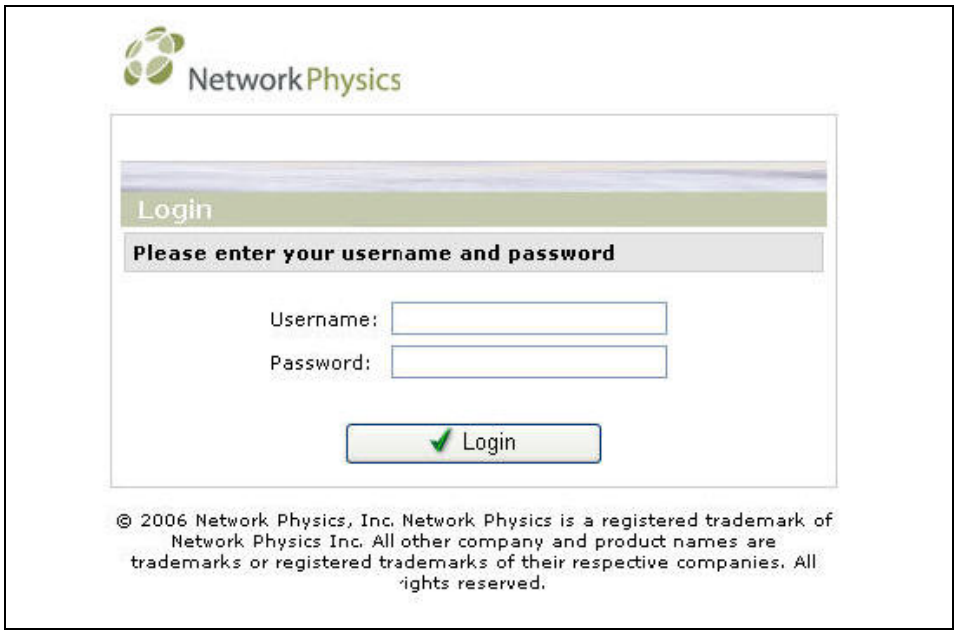
# 3. Configure Network Physics NetSensory

This section provides the procedures for configuring NetSensory Solution Insight for VoIP from Network Physics. The procedures fall into the following areas:

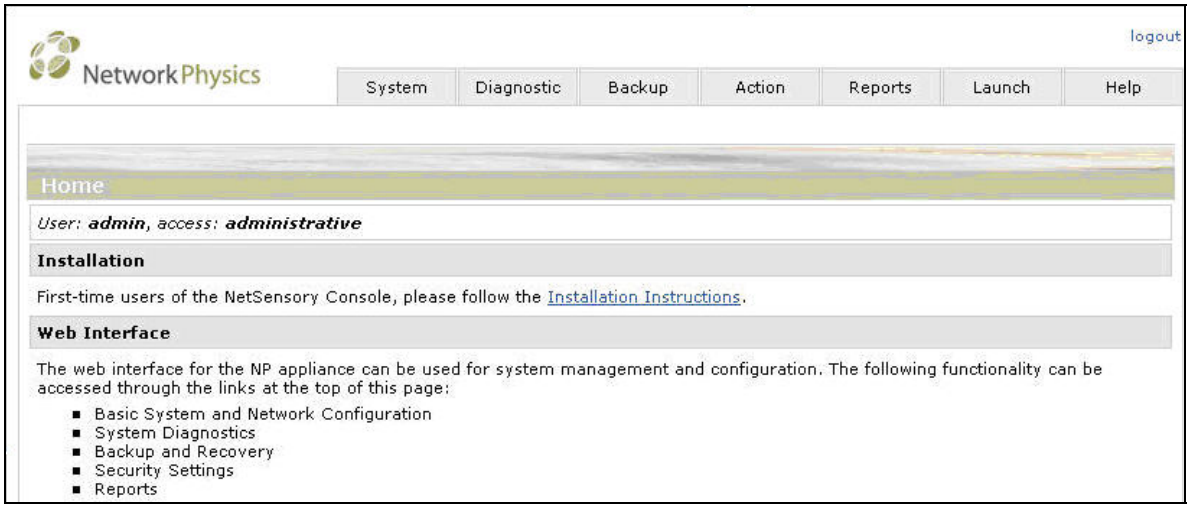
- Verify system configuration
- Launch NetSensory Console
- Create new project

## 3.1. Verify System Configuration

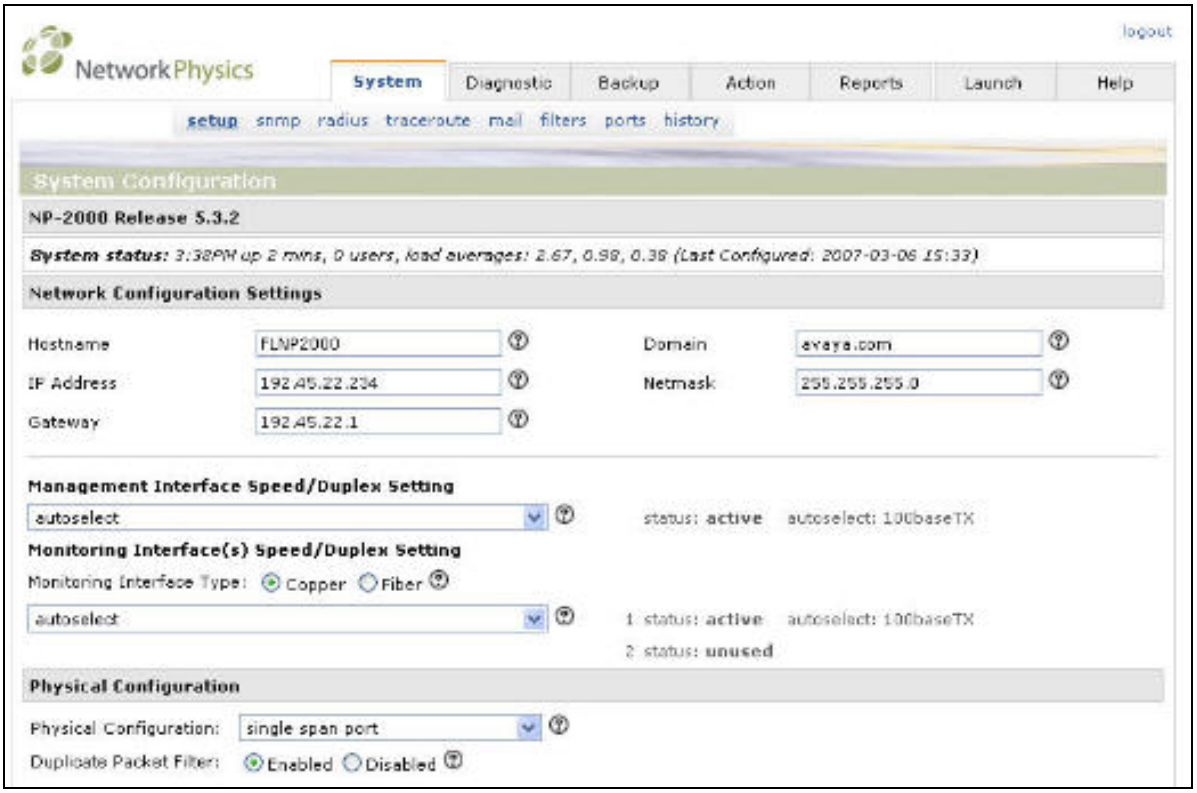
Access the NetSensory web based interface by using the URL "http://ip-address:8080" in an Internet browser window, where "ip-address" is the IP address of NetSensory. Enter the appropriate credentials, and click **Login**.



The **Home** screen is displayed next, as shown below. Select the **System** tab.

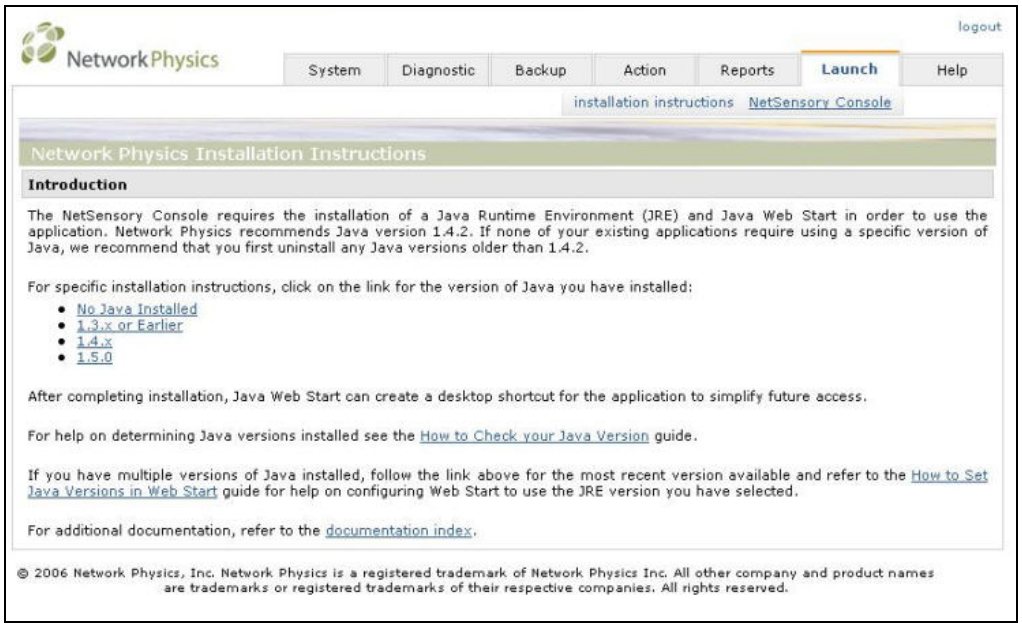



The **System Configuration** screen is displayed. Verify the values of the fields in the **Network Configuration Settings** section, which were entered as part of NetSensory installation. These values should match the network configuration. Check the remaining fields for default values. Verify that the **Monitoring Interface Type** is set to "Copper", the **Physical Configuration** is set to "single span port", and that the **Duplicate Packet Filter** is set to "Enabled". Should any modification be necessary, enter the new values and scroll down to the bottom of the screen to click **Apply** (not shown).

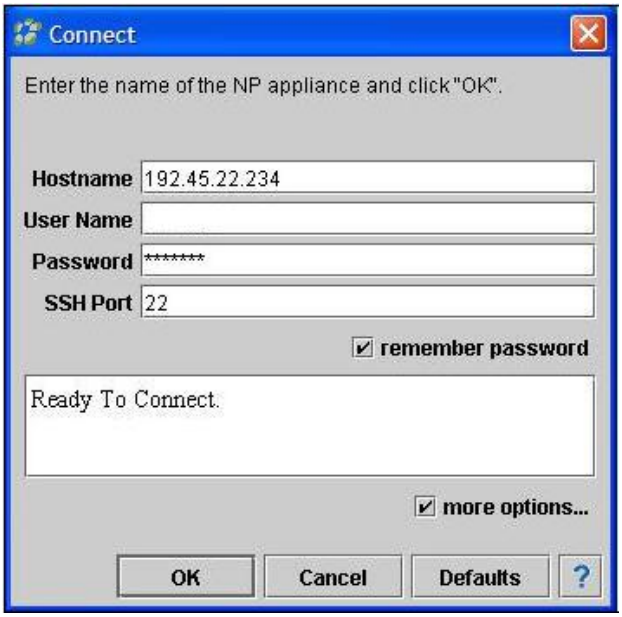


## 3.2. Launch NetSensory Console

Select the **Launch** tab, followed by **NetSensory Console** to connect to the NetSensory Console. The NetSensory Console is a Java-based application that enables exploring of network data and building of detailed traffic analysis by organizing the network view into projects.

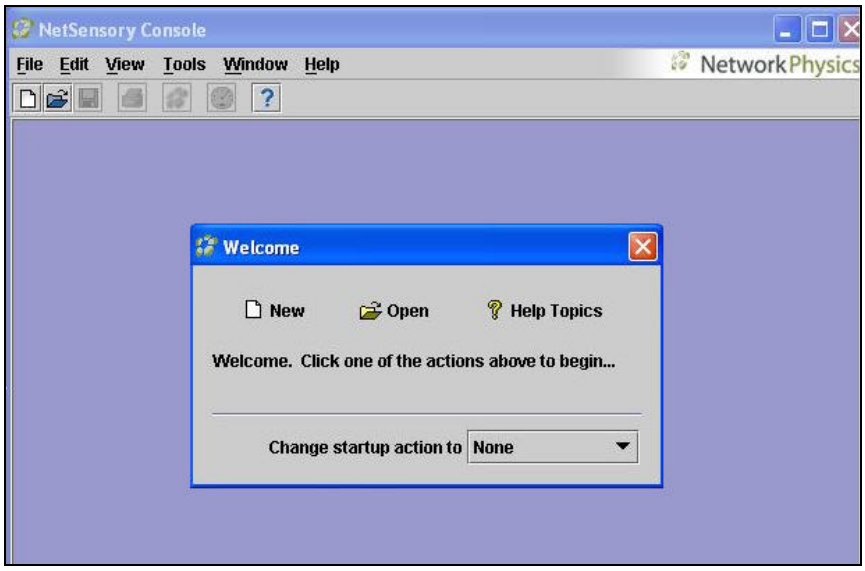



The **Connect** dialog box is displayed. For the **Hostname** field, enter the IP address of the NetSensory management interface. Enter appropriate credentials for the **User Name** and **Password** fields. Maintain the default values in the remaining fields, and click **OK**.

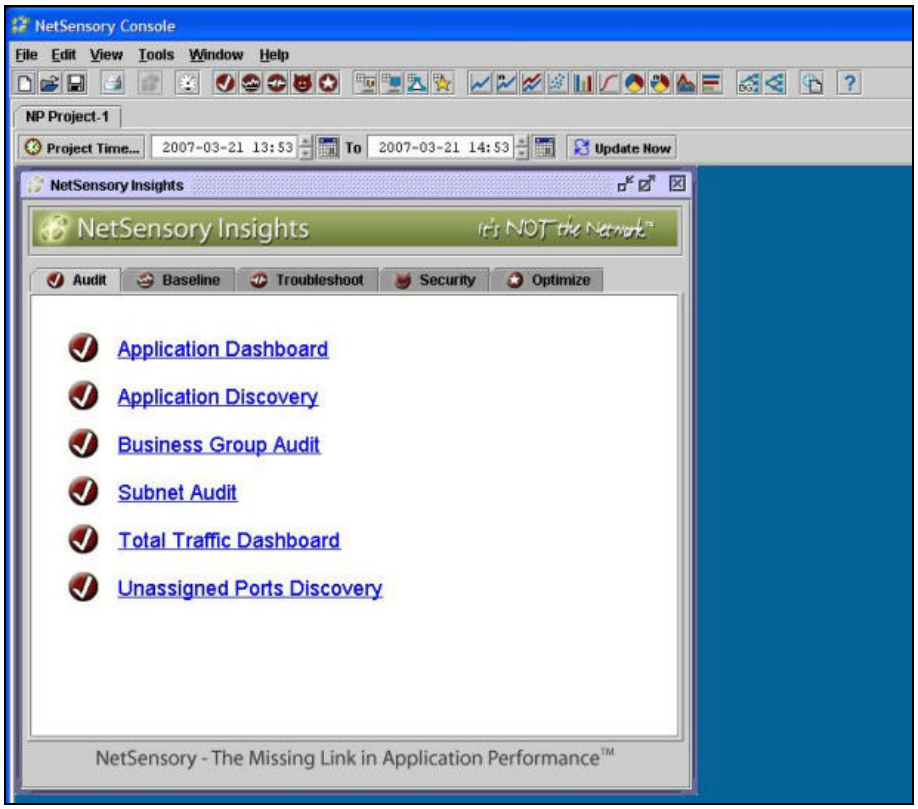


## 3.3. Create New Project

The **NetSensory Console** screen is displayed next. In the **Welcome** dialog box, select **New** to create a new project.




The **NetSensory Console** screen is displayed again, and updated with a default project name of "NP Project-1" and **NetSensory Insights** menu selections.



# 4. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing.

The feature testing focused on verifying NetSensory's capture and analysis of IP packets from the Avaya 4610SW and Avaya 9620 IP telephones. The call scenarios included registration, audio codecs with and without IP media shuffling (also referred to as direct IP-IP audio connection), encryption, and network impairments.

The serviceability testing focused on verifying the ability of NetSensory to recover from adverse conditions, such as disconnecting the Ethernet cables to NetSensory.

## 4.1. General Test Approach

All tests were performed manually. The Packet Storm was used to inject network impairments, such as jitter/delay/loss, into the network for calls between the two sites.

The serviceability test cases were performed manually by disconnecting and reconnecting the LAN cable to NetSensory.

The verification of all tests included checking of proper display of call data at NetSensory, and of comparing the reported network impairments from NetSensory with the network audio quality data reported on the Avaya 4610SW and Avaya 9620 IP telephones.

## 4.2. Test Results

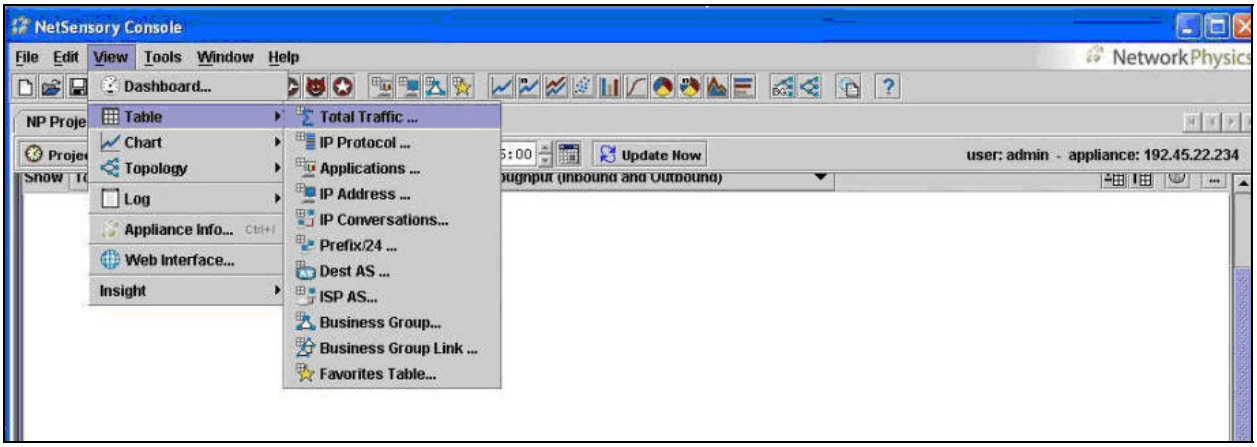
All test cases were executed and passed. Encrypted RTP packets had no impact on NetSensory as only the RTP packet headers were analyzed and not the content.

# 5. Verification Steps

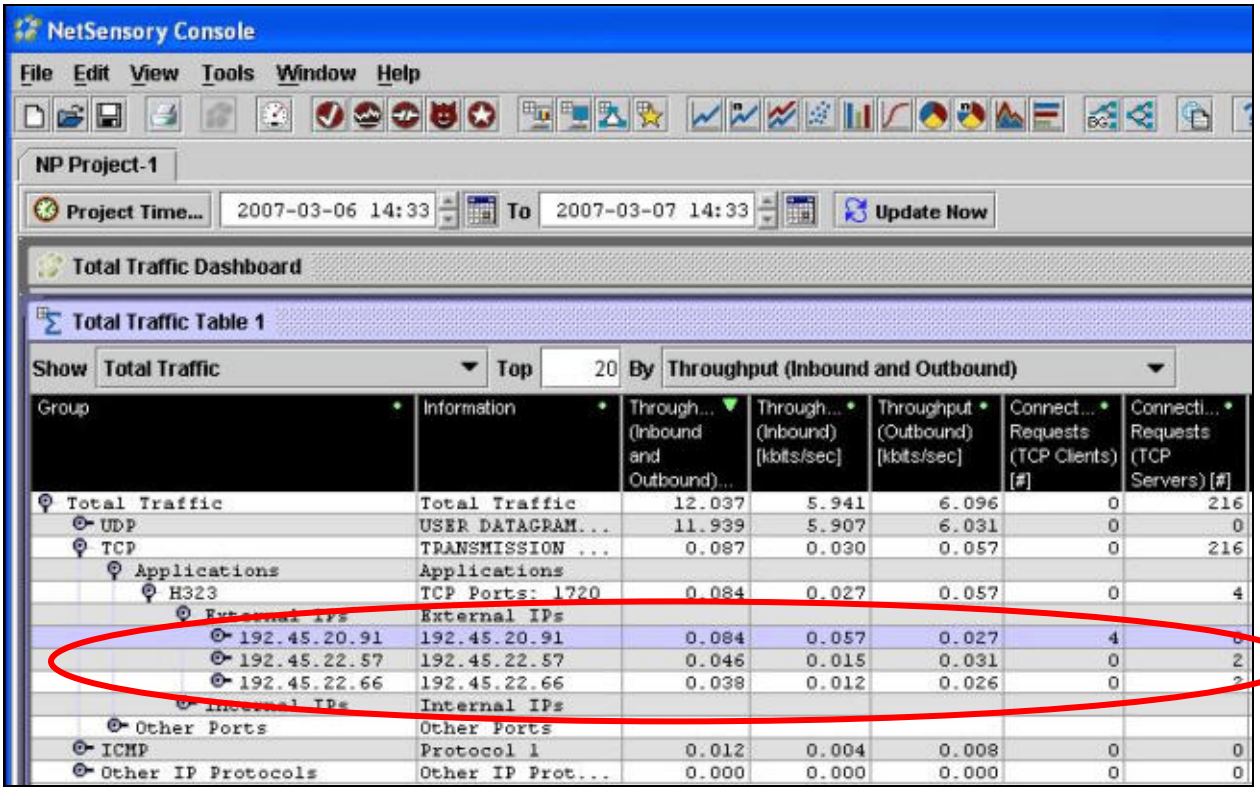
This section provides the tests that can be performed to verify proper configuration of NetSensory. Prior to verification, connect the two telephones monitored by NetSensory and make a few calls to enable registration and media packets to be captured.

## 5.1. Verify H.323 Registration

The H.323 registration data can be verified using the NetSensory Console interface. From the **NetSensory Console** screen, select **View > Table > Total Traffic** as shown below.



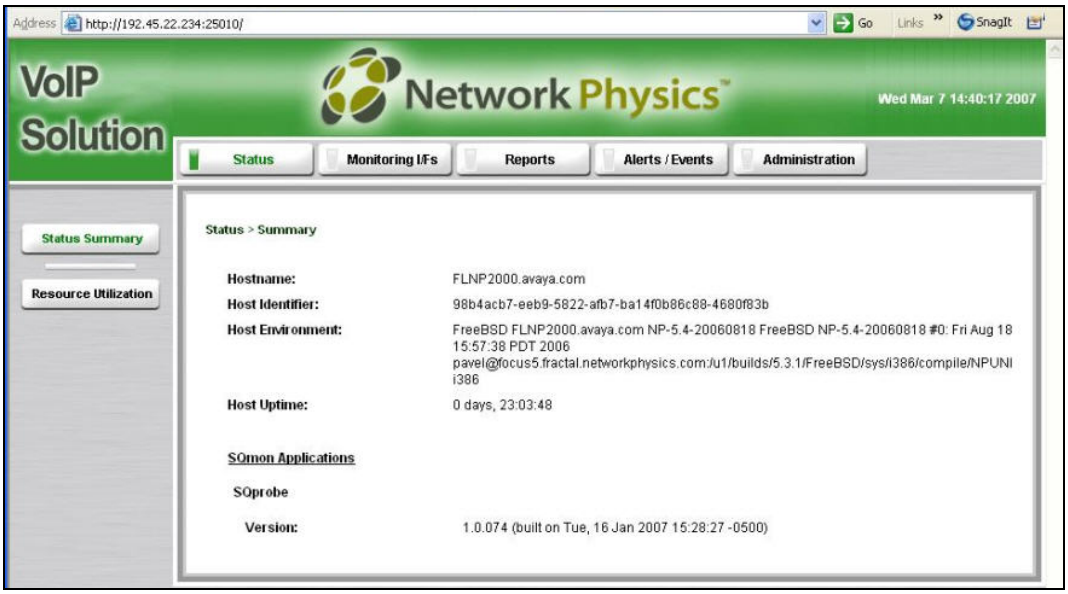
The screen is updated with **Total Traffic Dashboard** information. Expand on **Total Traffic > TCP > Applications > H323 > External IPs**. Verify that there are entries associated with the two Avaya IP telephones at the Branch site (in this case, IP addresses "192.45.22.57" and "192.45.22.66"), and that there is an entry for the Avaya Communication Manager device that the two Avaya IP telephones registered to (in this case, the two telephones registered to the S8300 Media Server processor with IP address of "192.45.20.91").



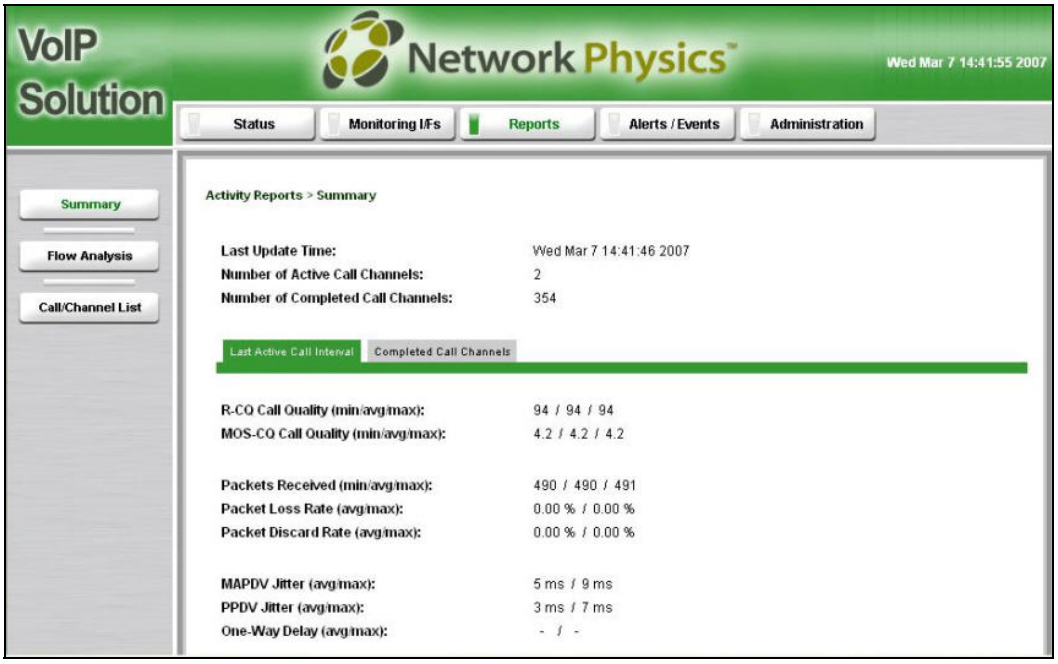

| Group | Information | Through... (Inbound and Outbound)... | Through... (Inbound) [kbits/sec] | Throughput (Outbound) [kbits/sec] | Connect... Requests (TCP Clients) [#] | Connecti... Requests (TCP Servers) [#] |
|---|---|---|---|---|---|---|
| Total Traffic | Total Traffic | 12.037 | 5.941 | 6.096 | 0 | 216 |
| UDP | USER DATAGRAM... | 11.939 | 5.907 | 6.031 | 0 | 0 |
| TCP | TRANSMISSION ... | 0.087 | 0.030 | 0.057 | 0 | 216 |
| Applications | Applications | | | | | |
| H323 | TCP Ports: 1720 | 0.084 | 0.027 | 0.057 | 0 | 4 |
| External IPs | External IPs | | | | | |
| 192.45.20.91 | 192.45.20.91 | 0.084 | 0.057 | 0.027 | 4 | 0 |
| 192.45.22.57 | 192.45.22.57 | 0.046 | 0.015 | 0.031 | 0 | 2 |
| 192.45.22.66 | 192.45.22.66 | 0.038 | 0.012 | 0.026 | 0 | 2 |
| Internal IPs | Internal IPs | | | | | |
| Other Ports | Other Ports | | | | | |
| ICMP | Protocol 1 | 0.012 | 0.004 | 0.008 | 0 | 0 |
| Other IP Protocols | Other IP Prot... | 0.000 | 0.000 | 0.000 | 0 | 0 |

## 5.2. Verify Media Channels

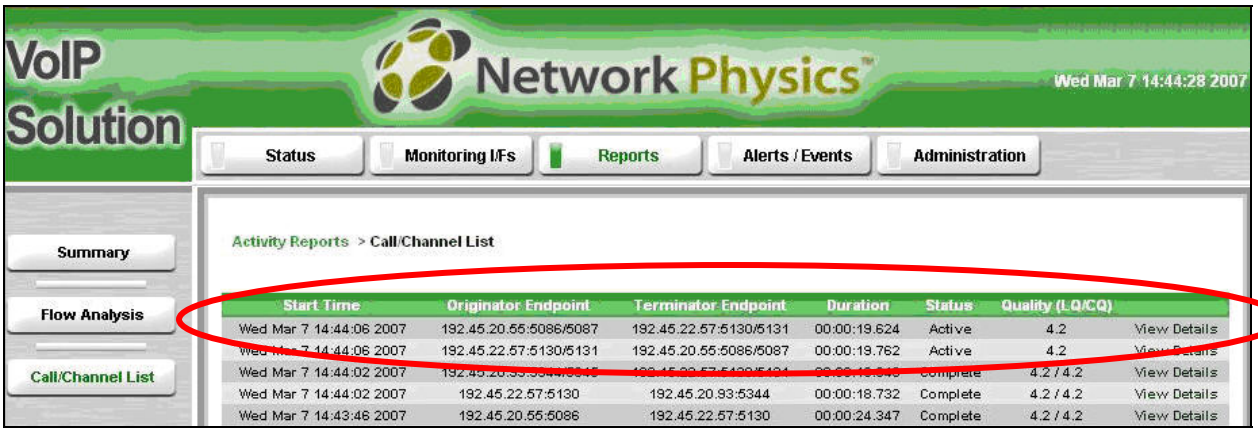
Establish an active call between the Main and Branch sites. The media channels can be verified using the NetSensory VoIP Solution interface. Access the NetSensory VoIP Solution interface by using the URL "http://ip-address:25010" in an Internet browser window, where "ip-address" is the IP address of NetSensory.




Select the **Reports** tab in the top menu bar, followed by **Summary** in the left pane. Verify that the **Number of Active Call Channels** is "2" to denote the two media channels for the current active call.

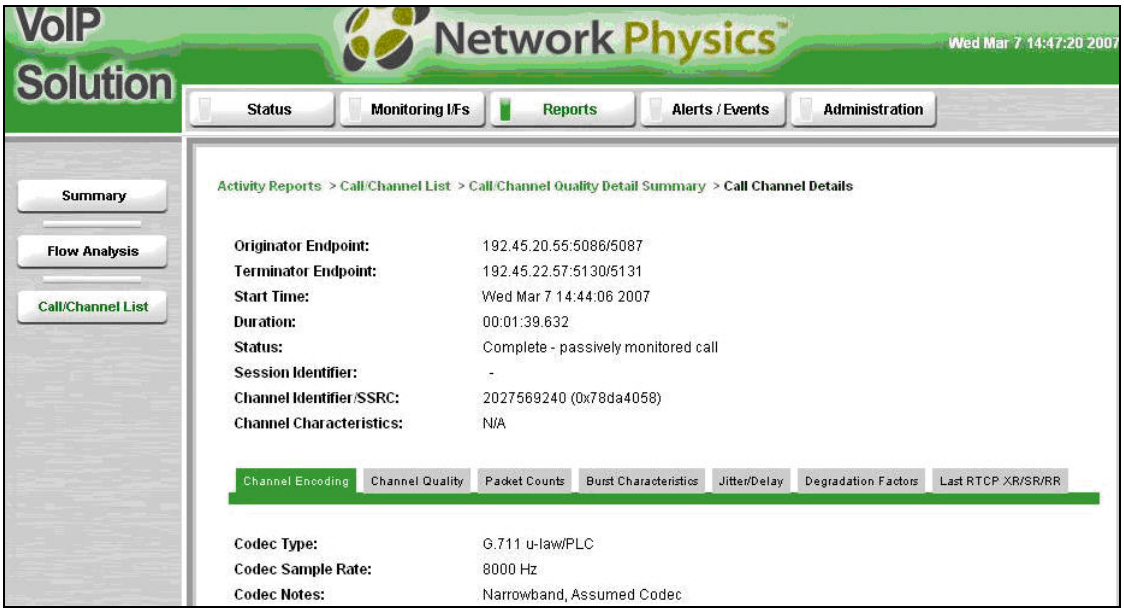


Select **Call/Channel List** from the left pane. The media channel data is displayed into the right pane. Verify that the top two lines are associated with the two channels for the current active call. Verify that the IP addresses of the two telephones are listed in the **Originator Endpoint** and **Terminator Endpoint** fields, and that the status of both channels is "Active" as shown below. Click on **View Details** on one of the media channels.

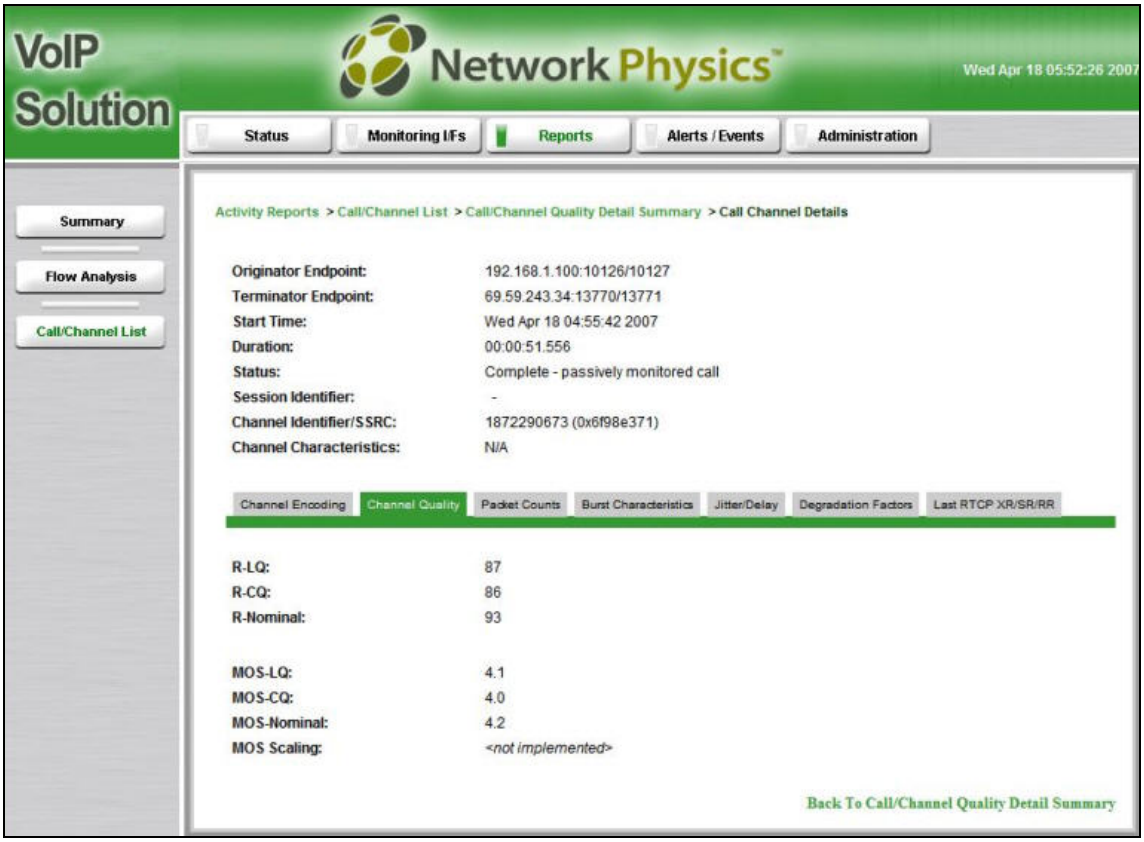



The right pane is updated with channel quality summary information. Click **More Details** on one of the media channels.

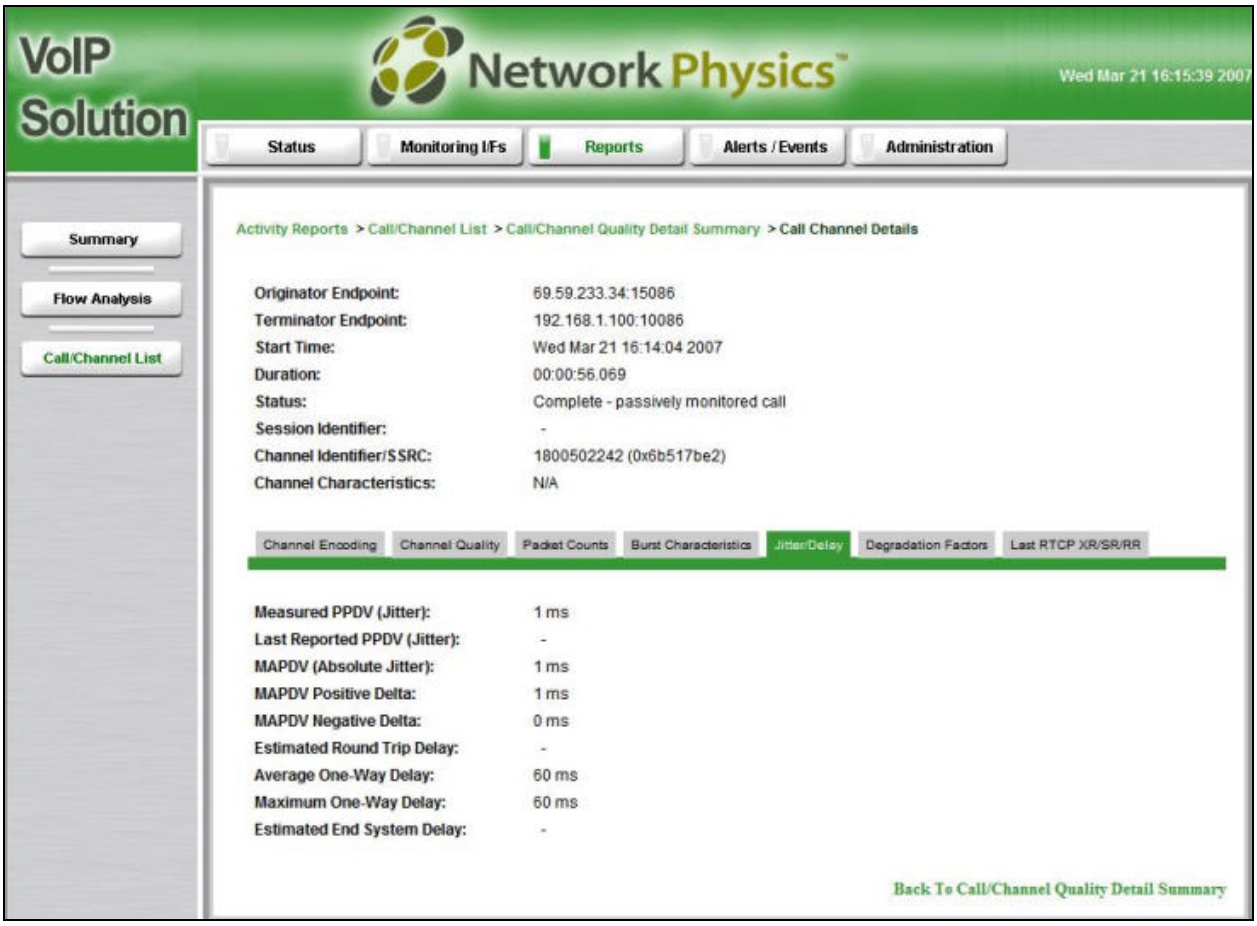
The right pane is updated with additional channel quality information. Click on the **Channel Encoding** tab toward the bottom of the right pane, and verify the **Codec Type** value.




Click on the **Channel Quality** tab, and verify the voice channel quality scores. Refer to the appropriate NetSensory documentation for detailed description of the various measurements.



Click on the **Jitter/Delay** tab, and verify the reported jitter/delay against the reported jitter/delay from the Avaya 4610SW and Avaya 9620 IP telephones.



# 6. Support

Technical support on Network Physics NetSensory Solution Insight for VoIP can be obtained through the following:

- **Phone:** (888) 390-5665
- **Web:** http://www.networkphysics.com/support
- **Email:** support@networkphysics.com

# 7. Conclusion

These Application Notes describe the configuration steps required for Network Physics NetSensory Solution Insight for VoIP 1.0 to interoperate in an Avaya IP Telephony environment, consisting of Avaya Communication Manager 3.1.2, Avaya 4610SW IP Telephones, and Avaya 9600 Series IP Telephones. All feature and serviceability test cases were completed successfully.

# 8. Additional References

This section references the product documentation relevant to these Application Notes.

- *Administrator Guide for Avaya Communication Manager*, Document 03-300509, Issue 2.1, May 2006, available at http://support.avaya.com

- *NetSensory Professional and Enterprise Release 5.3 Operation Manual*, available on NetSensory installation CD.

- *Operations Guide for NetSensory Insight Solutions for VoIP*, available on NetSensory installation CD.

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.