Avaya Solution & Interoperability Test Lab

Application Notes for the Viola Networks NetAlly Lifecycle Manager with Avaya Communication Manager - Issue 1.1

Abstract

These Application Notes describe the configuration procedures required for the Viola Networks NetAlly Lifecycle Manager to interoperate with Avaya Communication Manager. NetAlly Lifecycle Manager is an integrated software suite that provides VoIP assessment, monitoring and management for IP telephony environments before, during and after deployment.

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 configuration procedures required for the Viola Networks NetAlly Lifecycle Manager 5.1, herein referred to as NetAlly, to interoperate with Avaya Communication Manager 3.1.2. NetAlly is an integrated software suite that provides VoIP assessment, monitoring and management for IP telephony environments before, during and after deployment. NetAlly is a modular software solution that can be installed as a complete system, or one application at a time, a VoIP management solution to be built to match the IP Telephony size. During the compliance test, NetAlly's Passive VoIP Monitoring Application module was tested. NetAlly's Passive VoIP Monitoring Application provides centralized visibility into VoIP service levels delivered to every IP Telephone or VoIP gateway. By collecting call statistics and routing for every VoIP call made in the Avaya IP Telephony environment, NetAlly can generate call quality alerts, monitor trends, diagnose service problems and publish reports to document service level performance and diagnostic testing results.

Figure 1 illustrates the network configuration used to verify the Viola Networks solution. The figure shows three separate communication systems, each running Avaya Communication Manager on separate Avaya Media Servers. Site A is comprised of an Avaya S8700 Media Server and an Avaya G650 Media Gateway, which has connections to Avaya 4600 Series IP Telephones and Avaya 6400 Series Digital Telephones. Site B is comprised of an Avaya S8300 Media Server with an Avaya G350 Media Gateway, which has connections to Avaya 4600 Series IP Telephones and Avaya 6400 Series Digital Telephone. Site C is comprised of an Avaya S8300 Media Server with an Avaya G250 Media Gateway, which has connections to an Avaya 4600 Series IP Telephone and Avaya Analog Telephone. Site C is setup as LSP to Site A. An IP trunk connects the two Avaya Communication Manager systems between Site A and Site B.

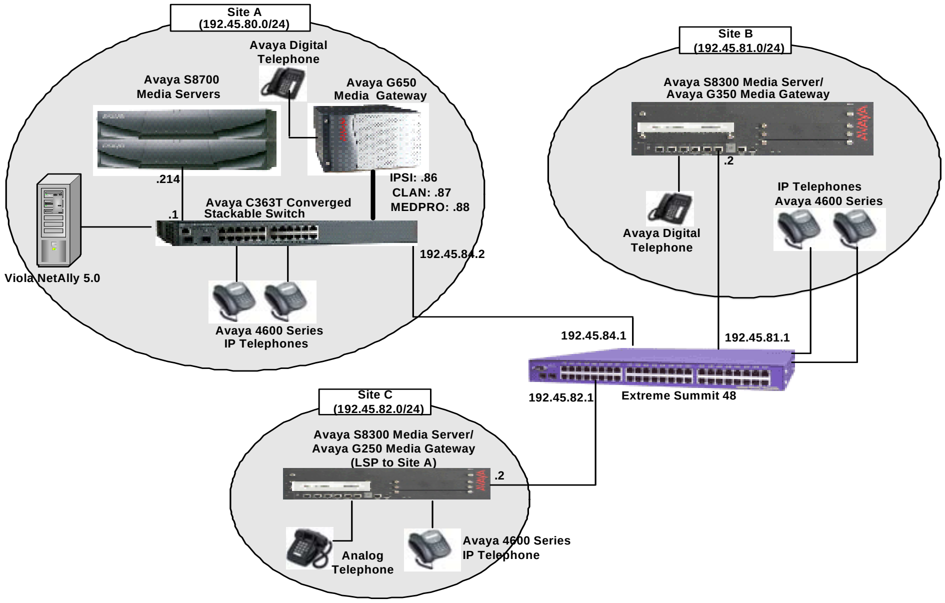


Figure 1. Test configuration of NetAlly with Avaya Communication Manager

2. Equipment and Software Validated

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

Equipment	Software
Avaya S8700 Media Server	Communication Manager 3.1.2 (R013x.01.2.632.1)
Avaya G650 Media Gateway	
TN2312BP IP Server Interface TN799DP C-LAN Interface TN2302AP IP Media Processor TN2602AP IP Media Processor	HW11 FW030 HW20 FW017 HW01 FW108 HW02 FW007
Avaya S8300 Media Server with Avaya G350 Media Gateway	Communication Manager 3.1.2 (R013x.01.2.632.1)
Avaya S8300 Media Server with Avaya G250 Media Gateway (LSP Mode)	Communication Manager 3.1.2 (R013x.01.2.632.1)
Avaya 4600 Series IP Telephones	
4620 4621 4625	2.6 2.6 2.5
Avaya 6400 Series Digital Telephones	-
Avaya Analog Telephones	-
Avaya C363T-PWR Converged Stackable Switch	4.5.14
Extreme Summit 48	4.1.21
NetAlly Lifecycle Manager OS – Windows Server 2003	5.1

3. Configuring Avaya Communication Manager

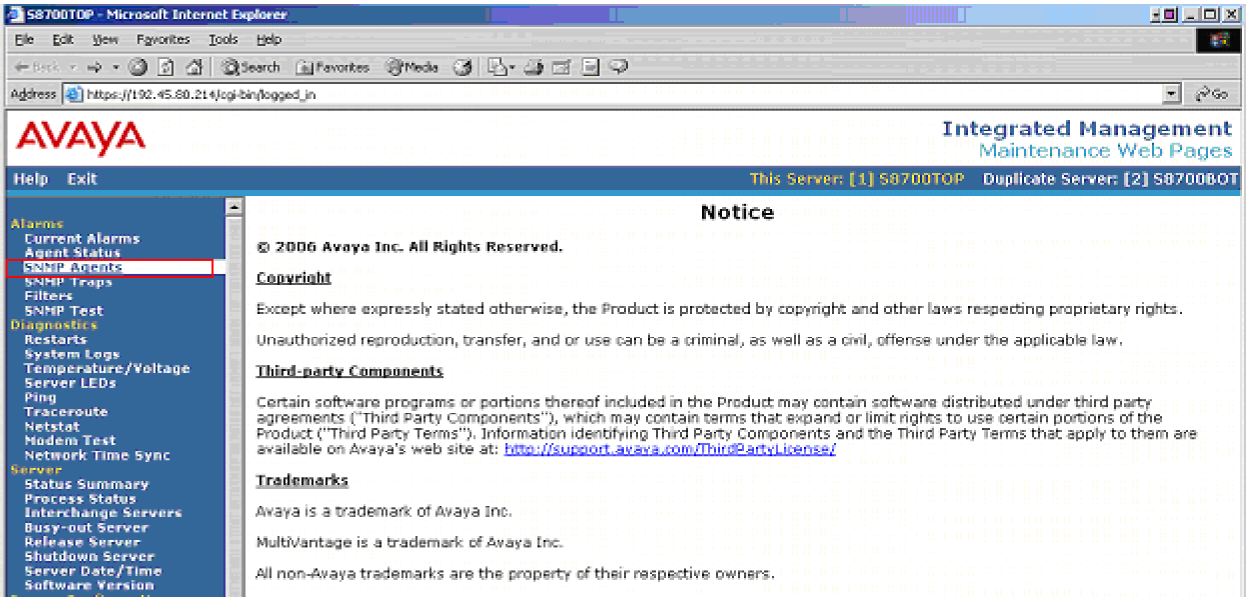
This section provides the procedures for configuring Avaya Communication Manager. Since NetAlly utilizes RTCP packet to calculate and report the quality of the call stream, a RTCP monitor server need to be created in Avaya Communication Manager. The following screen describes the setting of the RTCP monitor server. All the configuration changes in Avaya Communication Manager are performed through the System Access Terminal (SAT). Log into the SAT and use the **change system-parameters ip-options** command to configure the RTCP monitor server. Provide the following information:

- **Default Server IP Address** field - NetAlly Traffic Agent IP Address
- **Default Server Port –** 5005 This port number must match with the NetAlly Traffic Agent RTCP Listening Port. The default value for the default server port is 5005.
- **Default RTCP Report Period(secs) –** 5 The report period indicates Avaya Communication Manager forwards RTCP packet to the RTCP monitor server, which is NetAlly Traffic Agent. The default value for the Default RTCP Report Period(secs) field is 5.

Default values may be used in the remaining fields.

```
change system-parameters ip-options                             Page   1 of   2
                          IP-OPTIONS SYSTEM PARAMETERS

 IP MEDIA PACKET PERFORMANCE THRESHOLDS
    Roundtrip Propagation Delay (ms)    High: 800      Low: 400
                    Packet Loss (%)     High: 40       Low: 15
                    Ping Test Interval (sec): 20
    Number of Pings Per Measurement Interval: 10

 RTCP MONITOR SERVER
         Default Server IP Address: 192.45 .80 .15
               Default Server Port: 5005
  Default RTCP Report Period(secs): 5

AUTOMATIC TRACE ROUTE ON
           Link Failure? y


 H.248 MEDIA GATEWAY                   H.323 IP ENDPOINT
  Link Loss Delay Timer (min): 5        Link Loss Delay Timer (min): 5
                                          Primary Search Time (sec): 75
                                Periodic Registration Timer (min): 20
```

For NetAlly to create an IP Telephony table, SNMP needs to be enabled on the Avaya S8300 and S8700 Media Servers. Once SNMP is enabled, NetAlly utilizes SNMP to extract information from Avaya Communication Manager. Enabling SNMP for the Avaya S8700 and S8300 Media Servers can be configured through the server's web interface. To access the web interface, launch a web browser and connect to the media server by entering https://<media server IP address>. Supply the login and password for an account with super-user privileges. After logging in, a window is displayed with four option. Select the **Maintenance** option. A main menu is presented along the left hand side of the screen. In the Alarms section, click on **SNMP Agents** to display the SNMP Agent page.



Notice

© 2006 Avaya Inc. All Rights Reserved.

Copyright

Except where expressly stated otherwise, the Product is protected by copyright and other laws respecting proprietary rights.

Unauthorized reproduction, transfer, and or use can be a criminal, as well as a civil, offense under the applicable law.

Third-party Components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information identifying Third Party Components and the Third Party Terms that apply to them are available on Avaya's web site at: http://support.avaya.com/ThirdPartyLicense/

Trademarks

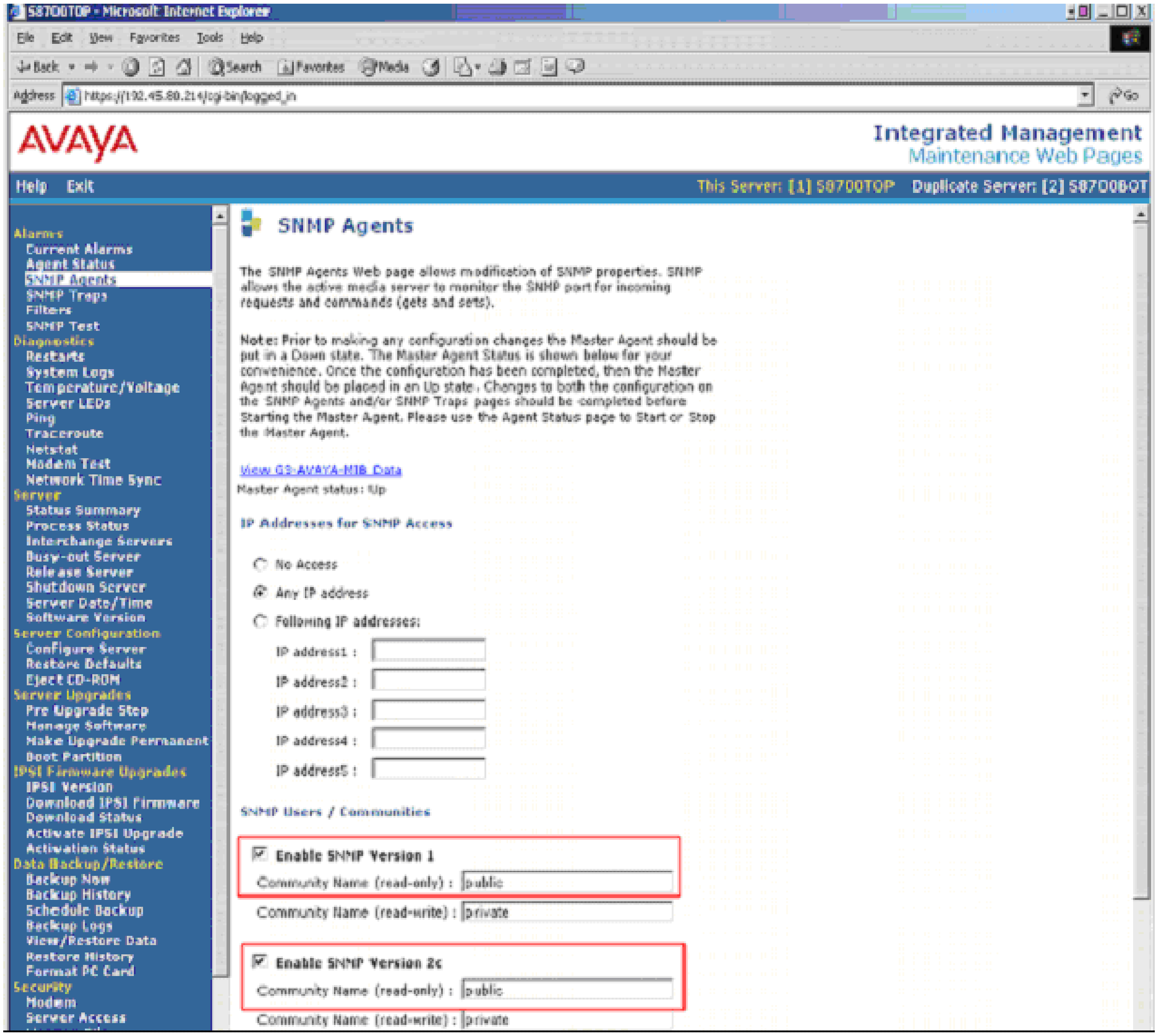
Avaya is a trademark of Avaya Inc.

MultiVantage is a trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners.

Enable SNMP version 1 and version 2c by clicking the check box. Set the community name to **public** on both version of SNMP. The community name configured in the Avaya media server has to match with NetAlly.

Click the **Submit** button at the bottom of the page to submit the form.



SNMP Agents

The SNMP Agents Web page allows modification of SNMP properties. SNMP allows the active media server to monitor the SNMP port for incoming requests and commands (gets and sets).

Note: Prior to making any configuration changes the Master Agent should be put in a Down state. The Master Agent Status is shown below for your convenience. Once the configuration has been completed, then the Master Agent should be placed in an Up state. Changes to both the configuration on the SNMP Agents and/or SNMP Traps pages should be completed before Starting the Master Agent. Please use the Agent Status page to Start or Stop the Master Agent.

View G3-AVAYA-MIB Data

Master Agent status: Up

IP Addresses for SNMP Access

○ No Access
● Any IP address
○ Following IP addresses:

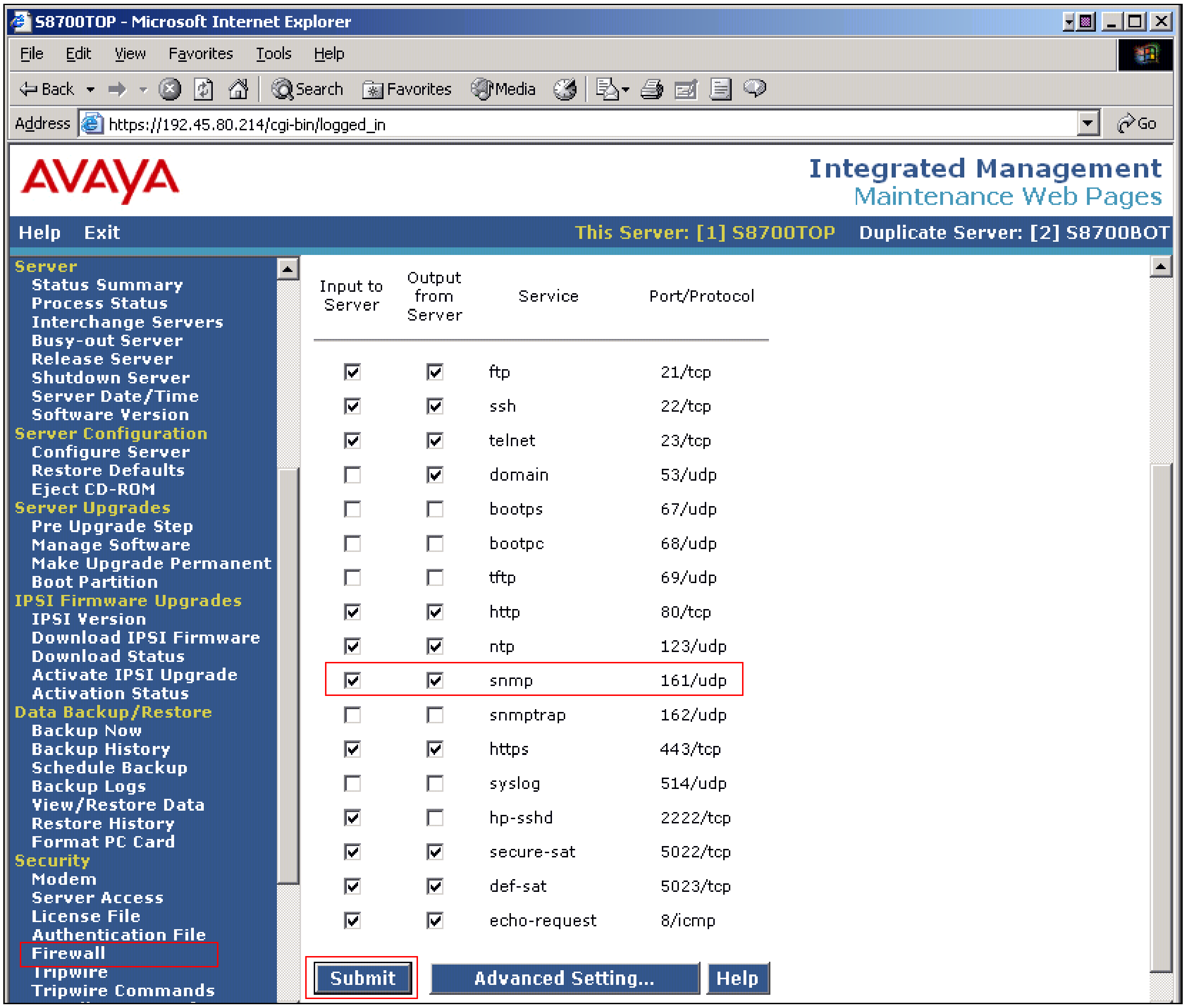
IP address1 :
IP address2 :
IP address3 :
IP address4 :
IP address5 :

SNMP Users / Communities

☑ Enable SNMP Version 1
Community Name (read-only) : public
Community Name (read-write) : private

☑ Enable SNMP Version 2c
Community Name (read-only) : public
Community Name (read-write) : private

The firewall in the Avaya Media Server must allow SNMP on UDP port 161. Click on the **Firewall** option in the Security section of the menu to display the Firewall page. Click on the **Input to Server** and **Output from Server** checkboxes for the snmp 161/udp field and click the **Submit** button.



Address: https://192.45.80.214/cgi-bin/logged_in

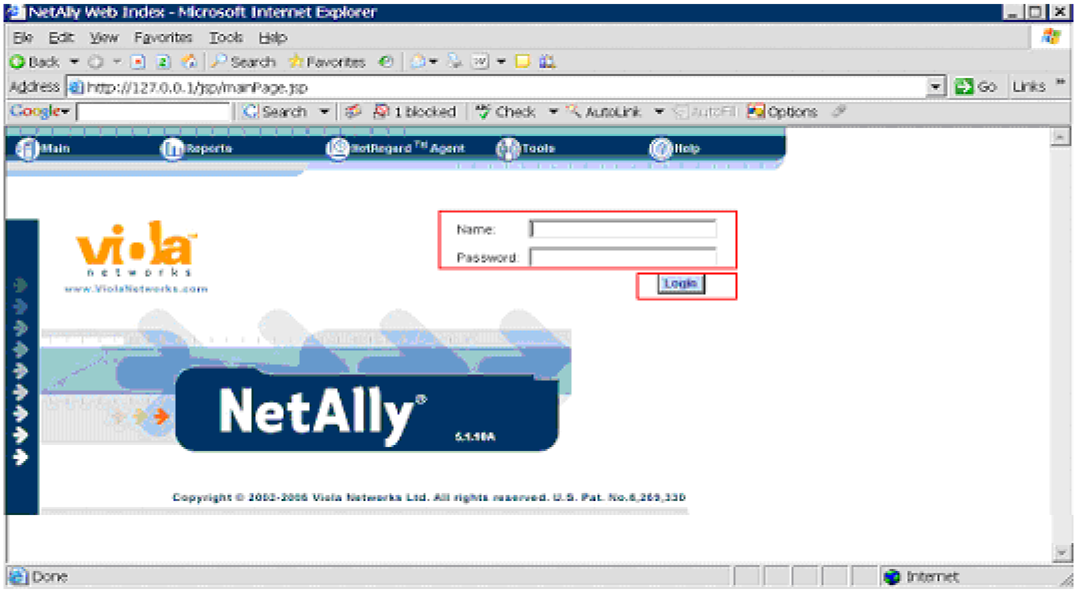
Input to Server	Output from Server	Service	Port/Protocol
☑	☑	ftp	21/tcp
☑	☑	ssh	22/tcp
☑	☑	telnet	23/tcp
☐	☑	domain	53/udp
☐	☐	bootps	67/udp
☐	☐	bootpc	68/udp
☐	☐	tftp	69/udp
☑	☑	http	80/tcp
☑	☑	ntp	123/udp
☑	☑	snmp	161/udp
☐	☐	snmptrap	162/udp
☑	☑	https	443/tcp
☐	☐	syslog	514/udp
☑	☐	hp-sshd	2222/tcp
☑	☑	secure-sat	5022/tcp
☑	☑	def-sat	5023/tcp
☑	☑	echo-request	8/icmp

4. Configuring the NetAlly Lifecycle Manager

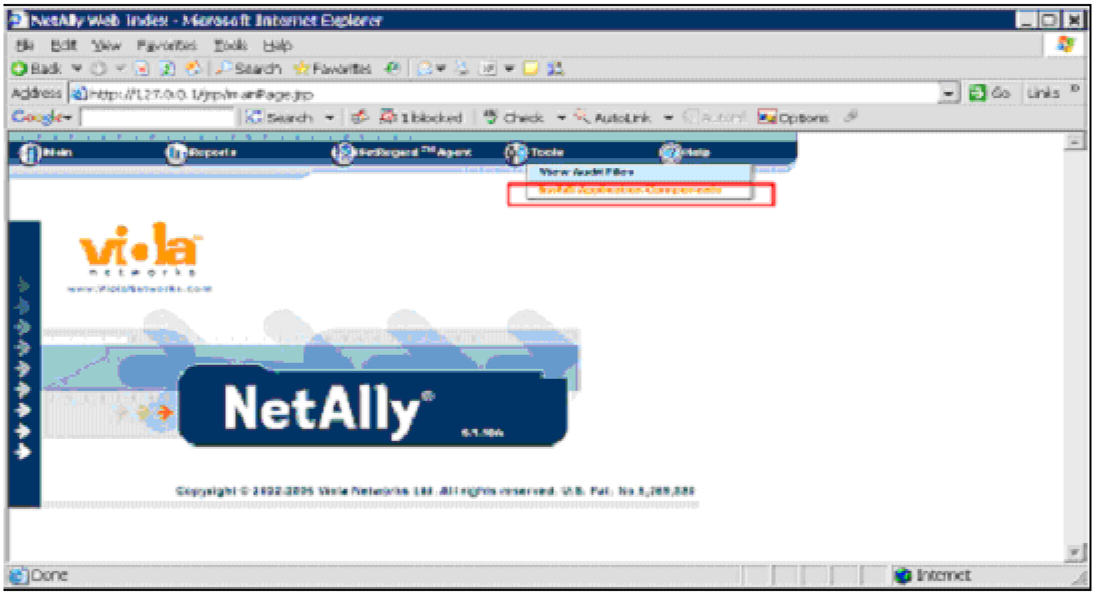
NetAlly Lifecycle Manager consists of three sub components; Test Center, User Interface and Traffic Agent. The Test Center installation is not covered in these Application Notes. Once the Test Center is installed, the Traffic Agent installation can be performed thru the web interface. VoIP assessment and monitoring feature can be configured thru the User Interface. Refer to [3] for further guidance.

4.1. Traffic Agent Installation

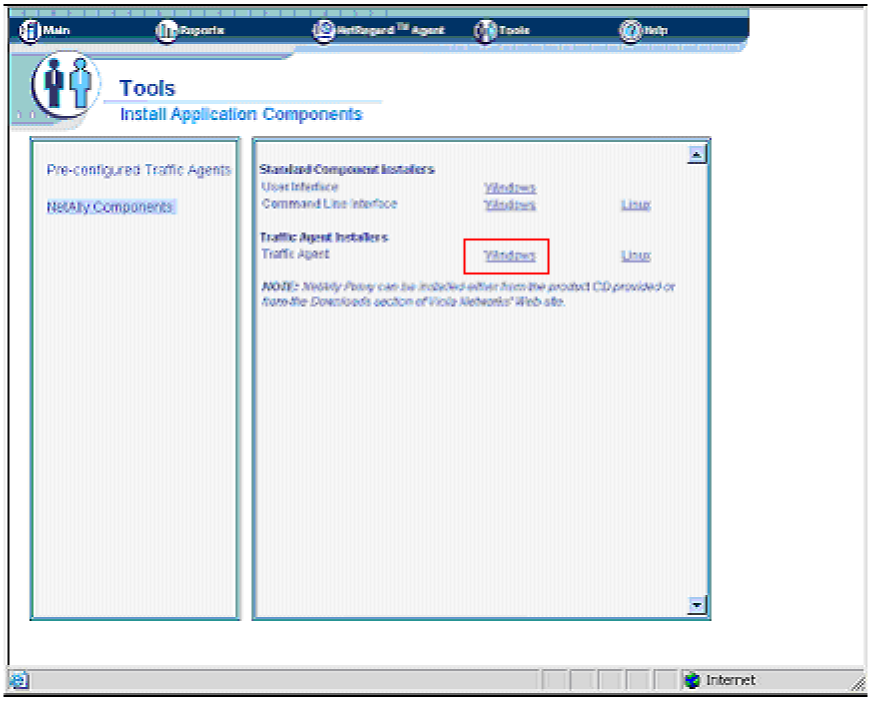
The function of a Traffic Agent is to receive RTCP message from Avaya Communication Manager on a specific port, and send the received messages to the Test Center. During the Traffic Agent installation, the main component was to specify the IP address of the Test Center. To install a Traffic Agent, launch a web browser and connect to NetAlly by entering http://<NetAlly Lifecycle Manager IP address>. Supply **Name** and **Password**, and click **Login** button to access the main menu page.


NetAlly Web Index - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://127.0.0.1/jsp/mainPage.jsp
Go Links
Main Reports NetRegard™ Agent Tools Help
Name:
Password:
Login
viola networks
www.ViolaNetworks.com
NetAlly
Copyright © 2002-2006 Viola Networks Ltd. All rights reserved. U.S. Pat. No.6,269,330
Done
Internet

Click **Tools → Install Application Components** to access the Install Application Component window.


NetAlly Web Index - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address http://127.0.0.1/jsp/mainPage.jsp
Main Reports NetRegard™ Agent Tools Help
View Audit Files
Install Application Components
viola networks
NetAlly
Done
Internet

Select the **Windows** option under the Traffic Agent Installers section to start the installation process of the Traffic Agent.



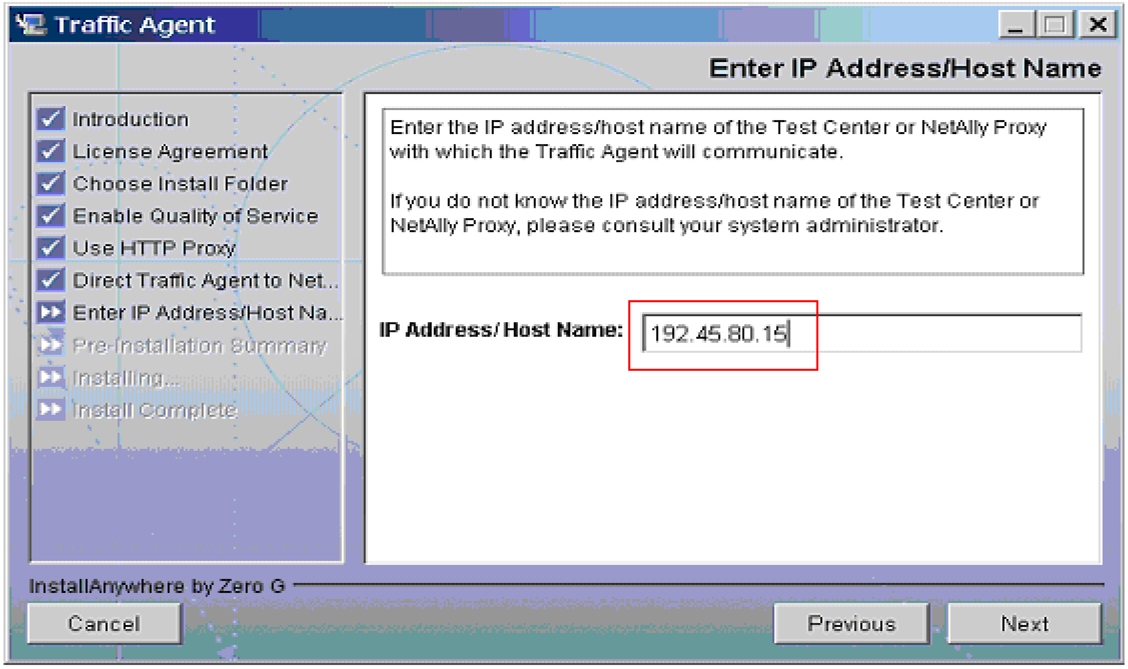
Tools

Install Application Components

Standard Component Installers		
User Interface	Windows	
Command Line Interface	Windows	Linux
Traffic Agent Installers		
Traffic Agent	Windows	Linux

NOTE: NetAlly Proxy can be installed either from the product CD provided or from the Downloads section of Viola Networks' Web site.

There are several windows that are associated with the installation process. However, the following screen is the only one where non-default values must be entered. In this window, provide the IP address of the Test Center.



Enter IP Address/Host Name

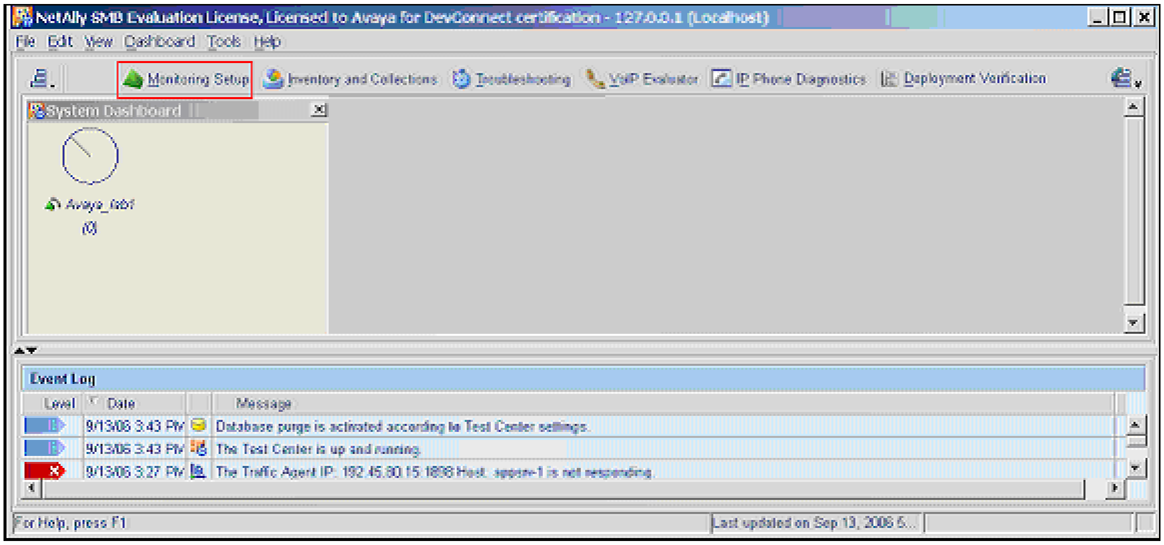
Enter the IP address/host name of the Test Center or NetAlly Proxy with which the Traffic Agent will communicate.

If you do not know the IP address/host name of the Test Center or NetAlly Proxy, please consult your system administrator.

IP Address/ Host Name: 192.45.80.15

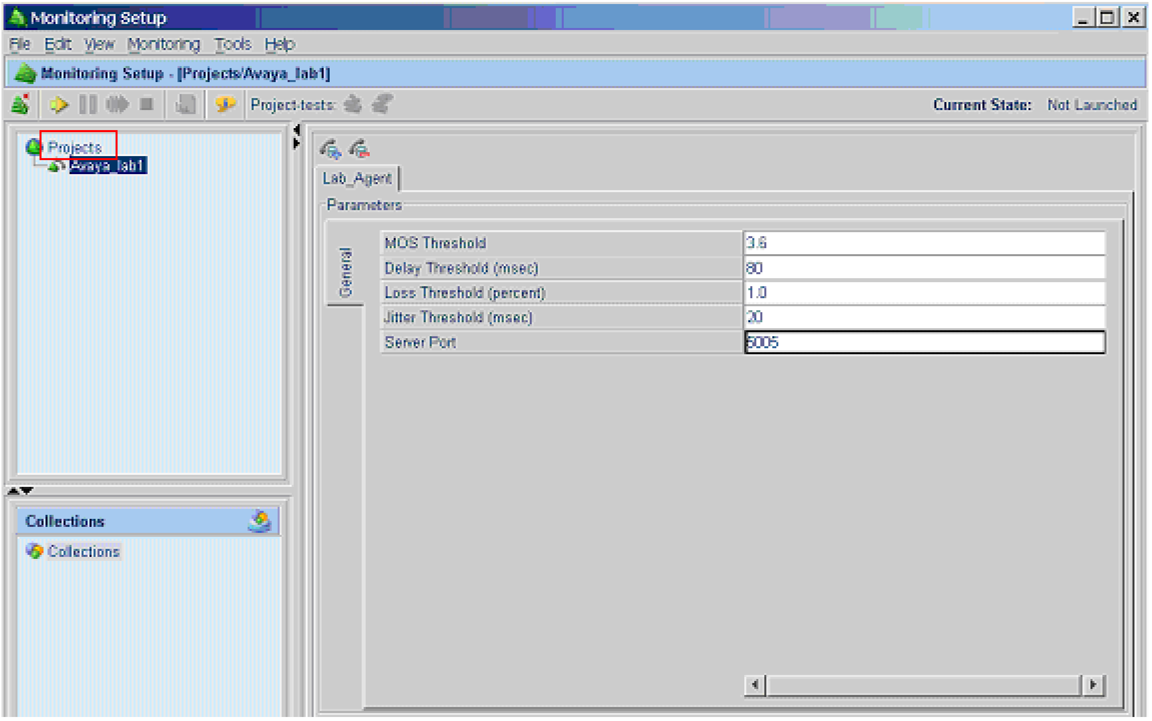
4.2. User Interface Configuration

After the Traffic Agent installation is completed, navigate to Windows **Start → All Program → Viola Networks NetAlly → User Interface.** Supply the Name and Password, and click **Login** button to access the User Interface window. Select **Monitoring Setup** from the top menu. The Monitoring Setup window will appear.


NetAlly SMB Evaluation License, Licensed to Avaya for DevConnect certification - 127.0.0.1 (Localhost)
File Edit View Dashboard Tools Help
Monitoring Setup
Inventory and Collections
Troubleshooting
VoIP Evaluator
IP Phone Diagnostics
Deployment Verification
System Dashboard
Avaya_lab1
(0)
Event Log
For Help, press F1
Last updated on Sep 13, 2006 5...

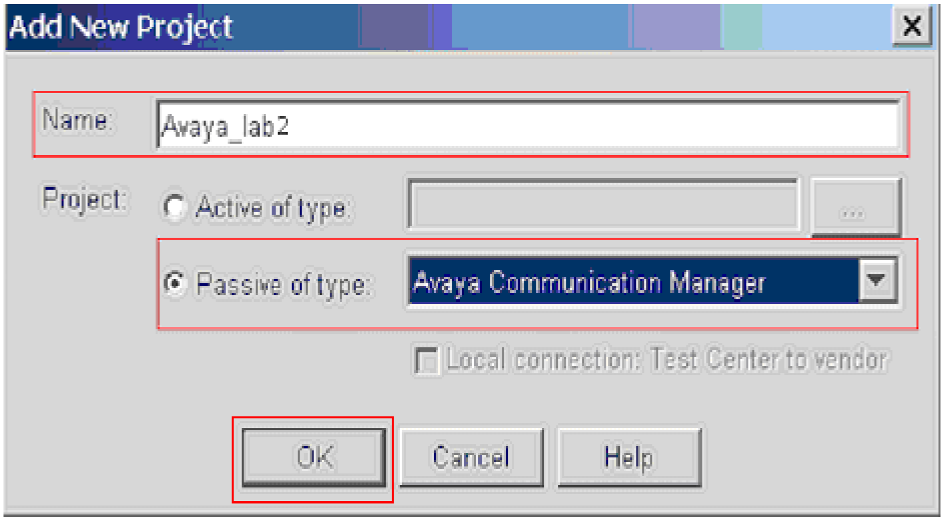
Level	Date		Message
	9/13/06 3:43 PM		Database purge is activated according to Test Center settings.
	9/13/06 3:43 PM		The Test Center is up and running.
	9/13/06 3:27 PM		The Traffic Agent IP: 192.45.80.15:1898 Host: appsrv-1 is not responding.

To create a new project, click the **Projects** menu. Using the right mouse button, click and select **New Project**. The New Project window will appear.


Monitoring Setup
File Edit View Monitoring Tools Help
Monitoring Setup - [Projects/Avaya_lab1]
Project-tests:
Current State: Not Launched
Projects
Avaya_lab1
Collections
Collections
Lab_Agent
Parameters
General

MOS Threshold	3.6
Delay Threshold (msec)	80
Loss Threshold (percent)	1.0
Jitter Threshold (msec)	20
Server Port	5005

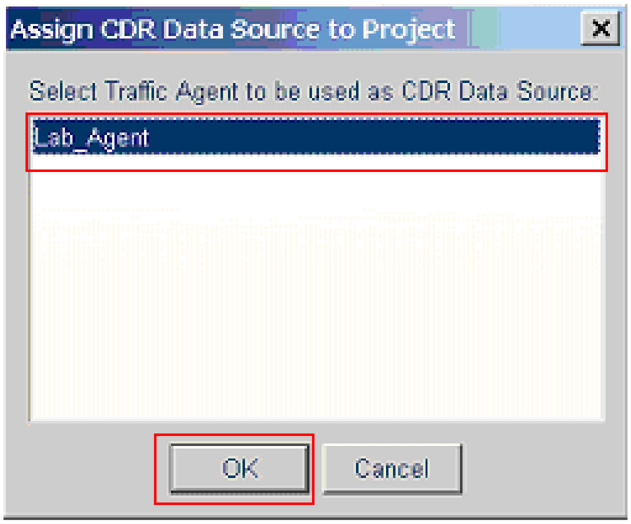
In the Add New Project window, provide the project name. Click the **Passive of Type** field, and select **Avaya Communication Manager**, using the drop-down menu. Click **OK,** and the Assign CDR Data Source to Project window will appear.



Name: Avaya_lab2

● Passive of type: Avaya Communication Manager

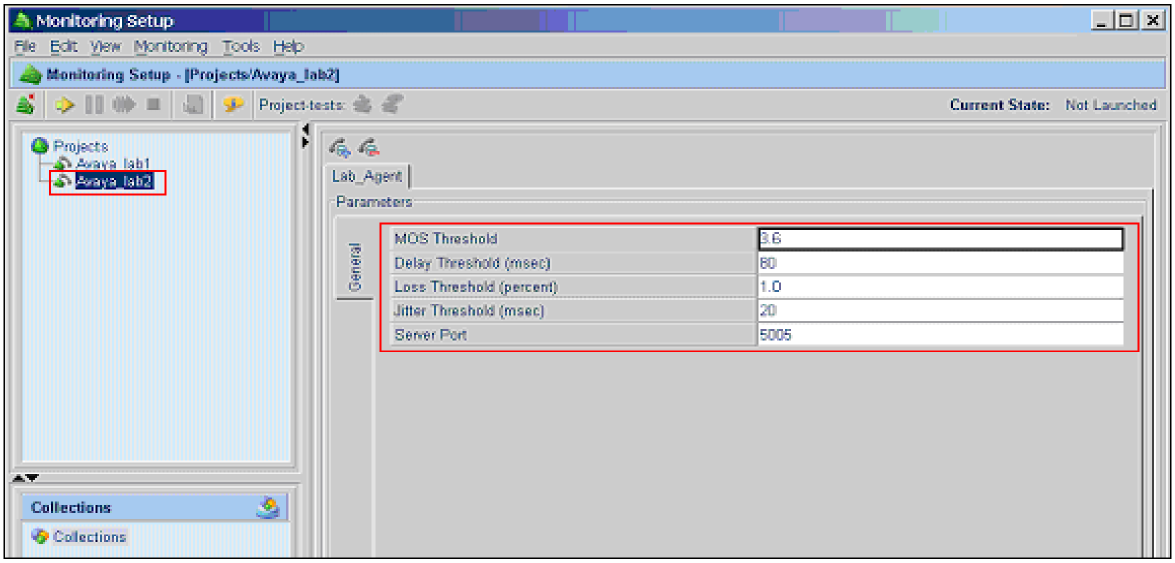
Assign a Traffic Agent to the project by selecting it from the following window.



Select Traffic Agent to be used as CDR Data Source:

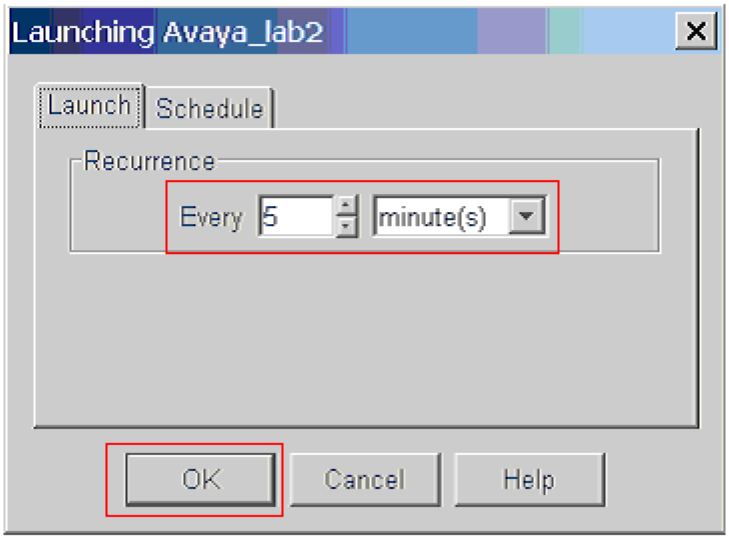
Lab_Agent

From the User Interface window, select **Monitoring Setup**. Provide Avaya IP Telephony thresholds for MOS, Delay, Packet Loss and Jitter. The Server Port provided in this window must match with Avaya Communication Manager's **Default Server Port**, created in Section 3. With the right mouse button, click the project name in the left pane and select the **Launch** option.



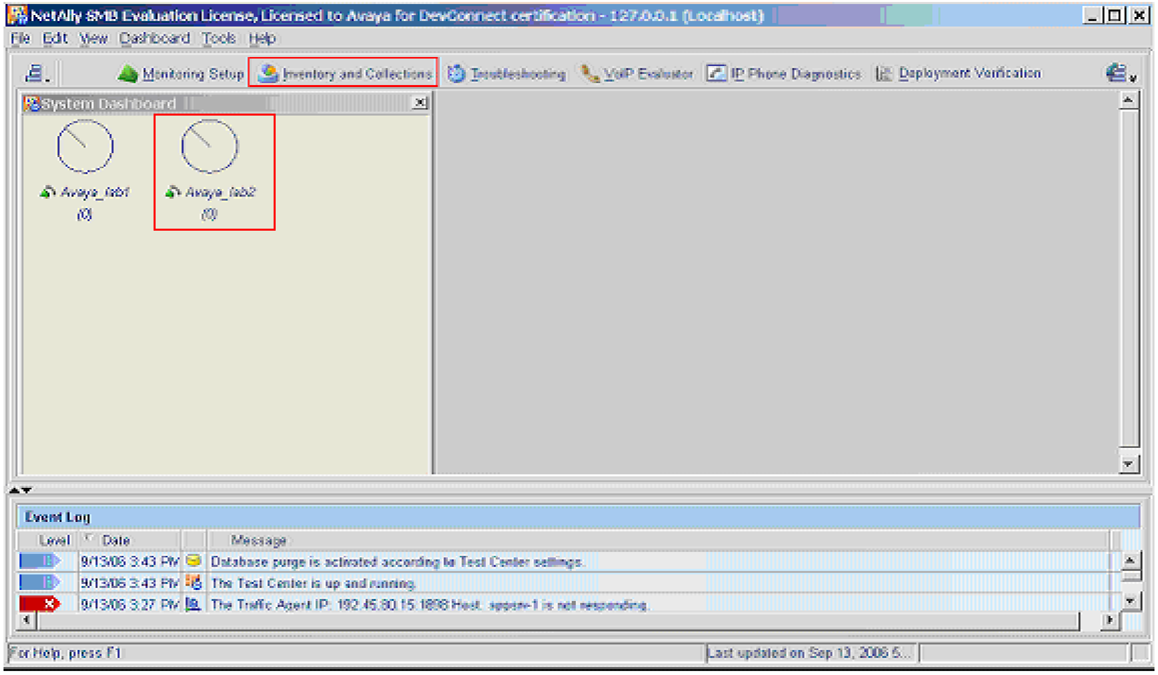
MOS Threshold	3.6
Delay Threshold (msec)	80
Loss Threshold (percent)	1.0
Jitter Threshold (msec)	20
Server Port	5005

In the screen below, the schedule for the Traffic Agent to send the received RTCP message to the Test Center is specified. The following screen below describes the recurrence value that the Traffic Agent forwards RTCP messages, received from Avaya Communication Manager, to the Test Center. This process completes the project configuration. Click the **OK** button



Every 5 minute(s)

After the completion of adding a project, Avaya_lab2, the new project is added into the System Dashboard section of the User Interface window. From the User Interface window, select **Inventory and Collections**.


NetAlly SMB Evaluation License, Licensed to Avaya for DevConnect certification - 127.0.0.1 (Localhost)
File Edit View Dashboard Tools Help
Monitoring Setup
Inventory and Collections
Troubleshooting
VoIP Evaluator
IP Phone Diagnostics
Deployment Verification
System Dashboard
Avaya_lab1
(0)
Avaya_lab2
(0)
Event Log

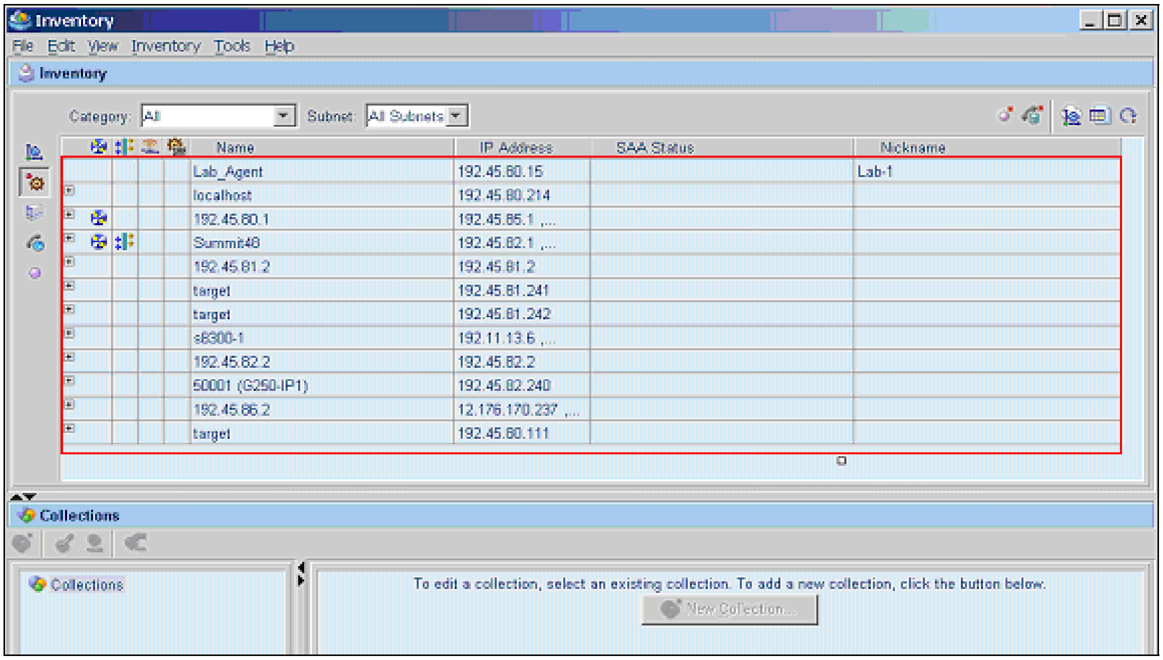
Level	Date		Message
I	9/13/06 3:43 PM		Database purge is activated according to Test Center settings.
I	9/13/06 3:43 PM		The Test Center is up and running.
✕	9/13/06 3:27 PM		The Traffic Agent IP: 192.45.80.15:1898 Host: [illegible] is not responding.

For Help, press F1

Last updated on Sep 13, 2006 5...

The Inventory window displays the results from the following process performed by NetAlly Lifecycle Manager:

- Network Discovery
- SNMP MIB browse on Avaya Communication Manager



Category: All

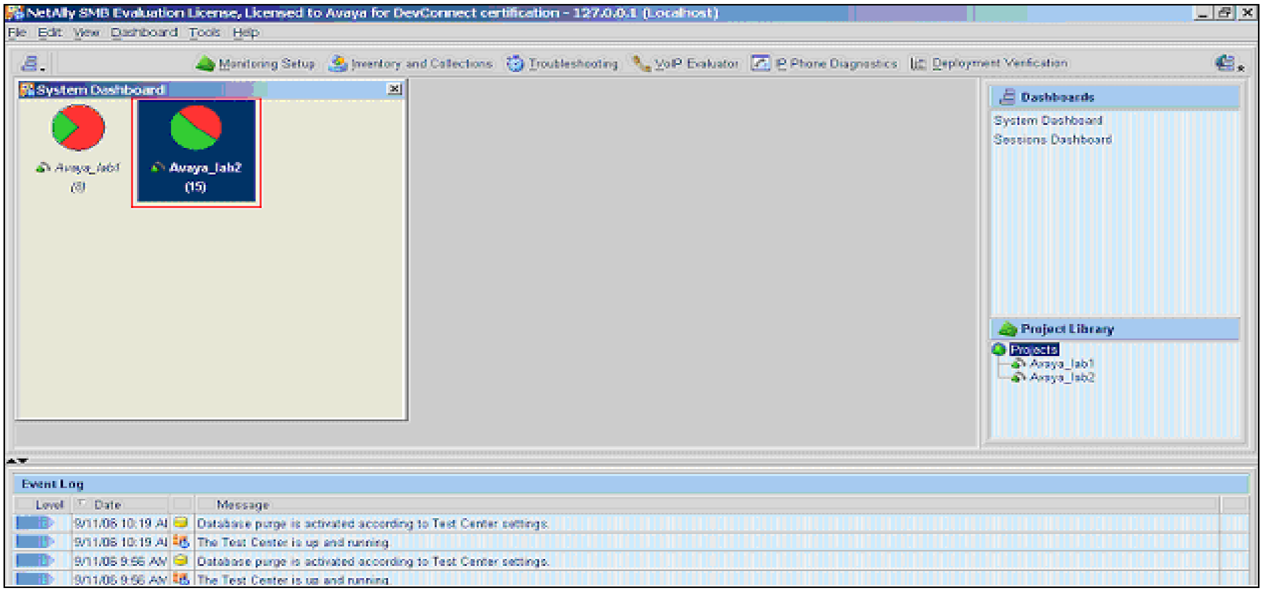
Subnet: All Subnets

Name	IP Address	SAA Status	Nickname
Lab_Agent	192.45.80.15		Lab-1
localhost	192.45.80.214		
192.45.80.1	192.45.85.1 ,...		
Summit48	192.45.82.1 ,...		
192.45.81.2	192.45.81.2		
target	192.45.81.241		
target	192.45.81.242		
s8300-1	192.11.13.6 ,...		
192.45.82.2	192.45.82.2		
50001 (G250-IP1)	192.45.82.240		
192.45.86.2	12.176.170.237 ,...		
target	192.45.80.111		

To edit a collection, select an existing collection. To add a new collection, click the button below.

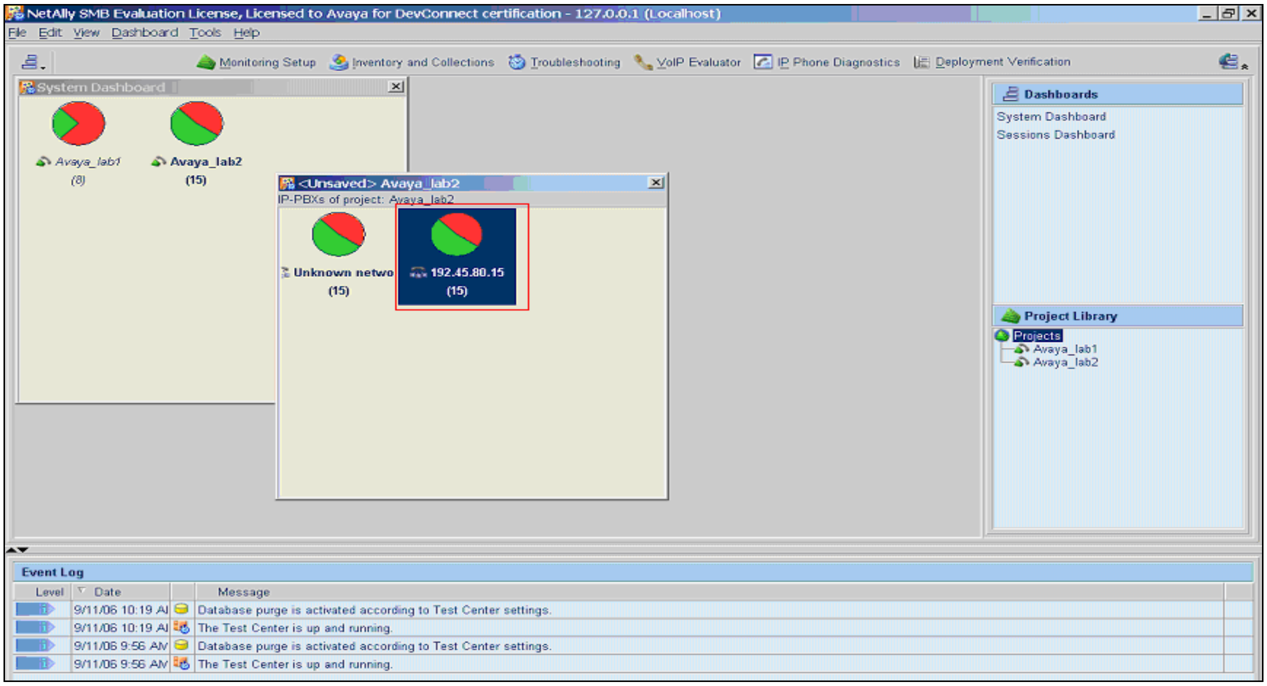
4.3. Generating Call statistics

This section describes steps to collect statistics on each call between stations. Navigate to Windows **Start** → **All Program** → **Viola Networks NetAlly** → **User Interface.** Supply the Name and Password, and click **Login** button to access the User Interface window. Double click a project in the System Dashboard window to drill down to the Project Dashboard.



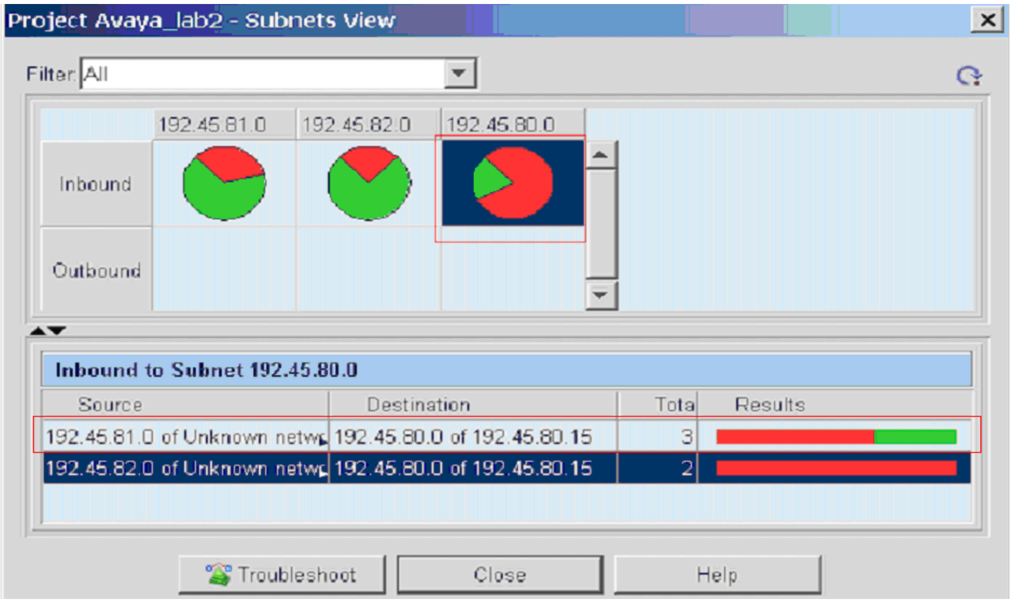
```
9/11/06 10:19 AI  Database purge is activated according to Test Center settings.
9/11/06 10:19 AI  The Test Center is up and running.
9/11/06 9:56 AM   Database purge is activated according to Test Center settings.
9/11/06 9:56 AM   The Test Center is up and running.
```

From the Project Dashboard window, select the Test Center to drill down to the Subnets View.



```
9/11/06 10:19 AI  Database purge is activated according to Test Center settings.
9/11/06 10:19 AI  The Test Center is up and running.
9/11/06 9:56 AM   Database purge is activated according to Test Center settings.
9/11/06 9:56 AM   The Test Center is up and running.
```

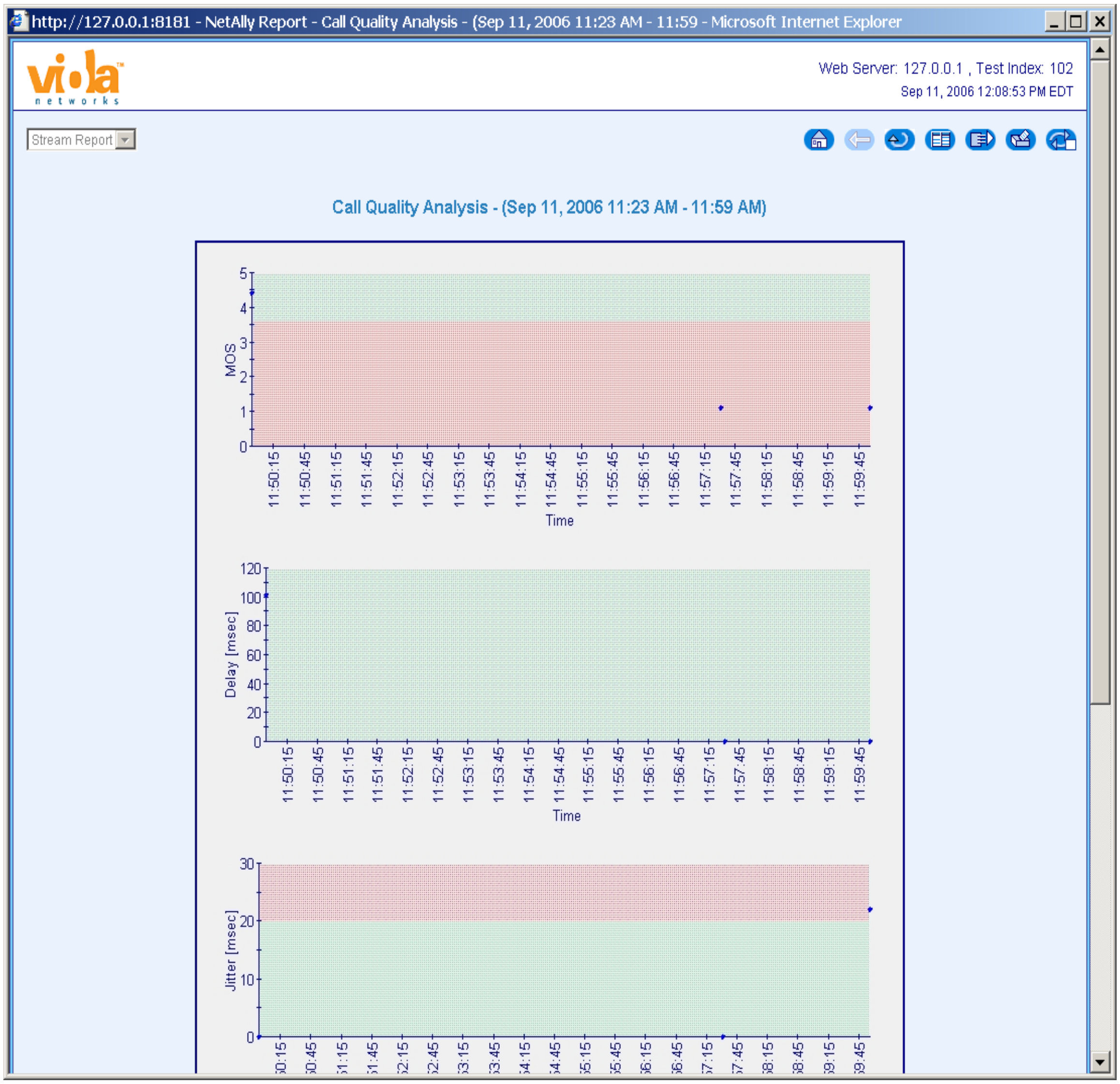
The Subnets View page provides all streams associated with different subnets. The following Subnets View window indicates RTCP packets came from two sources (subnet 192.45.81.0 and subnet 192.45.82.0). Drill down more by selecting a subnet and choose the source of the RTCP packet.



Inbound to Subnet 192.45.80.0

Source	Destination	Tota	Results
192.45.81.0 of Unknown netwo	192.45.80.0 of 192.45.80.15	3	🟥🟩
192.45.82.0 of Unknown netwo	192.45.80.0 of 192.45.80.15	2	🟥

The Call Quality Analysis window displays the call quality values (MOS, Delay, Jitter, and Network Loss) of each call. In the Call Quality Analysis window, each dot represents a call. By double clicking the dot, the Stream Detailed Report page displays.

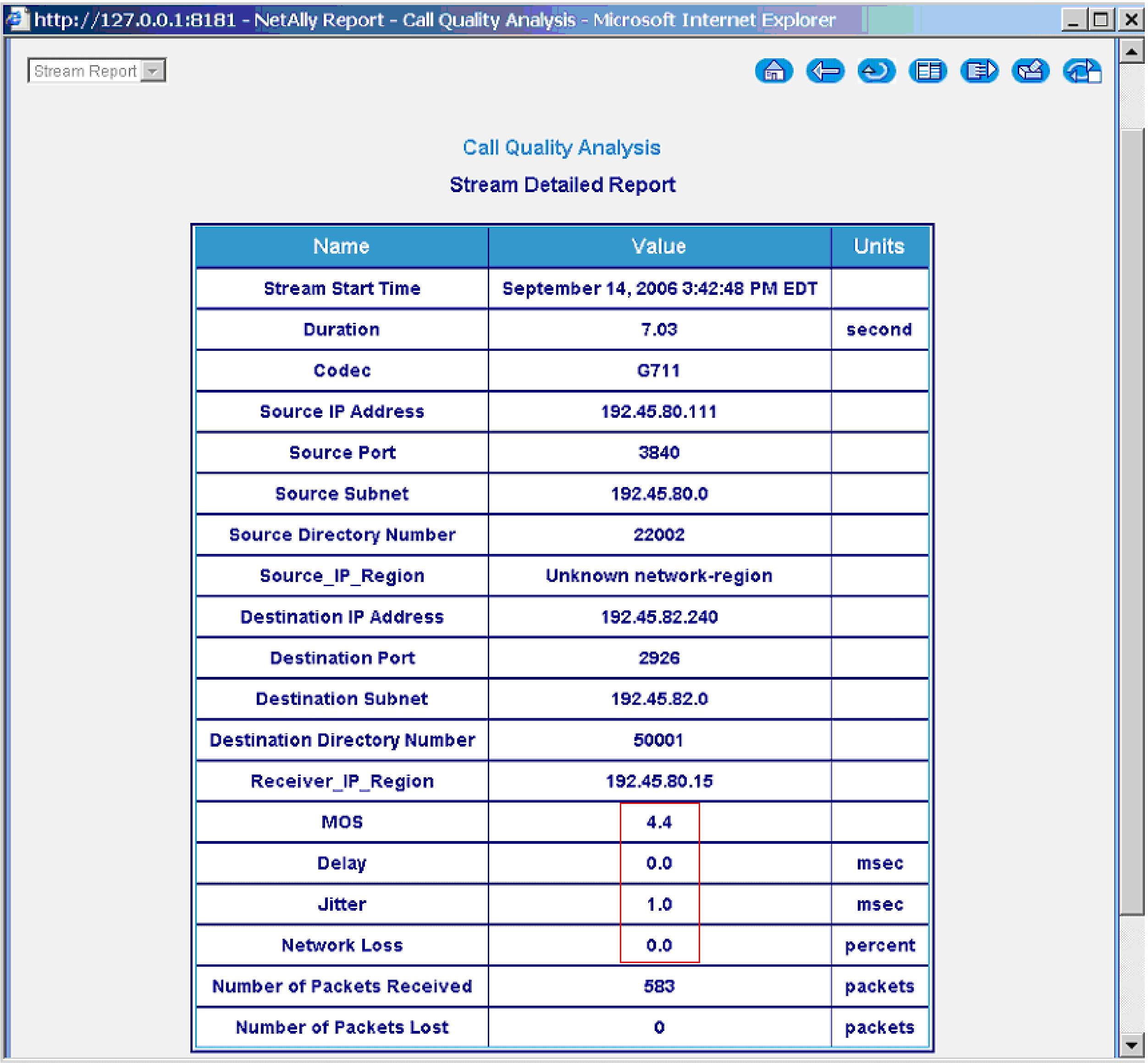


http://127.0.0.1:8181 - NetAlly Report - Call Quality Analysis - (Sep 11, 2006 11:23 AM - 11:59 - Microsoft Internet Explorer

Web Server: 127.0.0.1 , Test Index: 102
Sep 11, 2006 12:08:53 PM EDT

Call Quality Analysis - (Sep 11, 2006 11:23 AM - 11:59 AM)

The following screen displays a sample stream detailed report.


http://127.0.0.1:8181 - NetAlly Report - Call Quality Analysis - Microsoft Internet Explorer
Stream Report

Call Quality Analysis

Stream Detailed Report

Name	Value	Units
Stream Start Time	September 14, 2006 3:42:48 PM EDT	
Duration	7.03	second
Codec	G711	
Source IP Address	192.45.80.111	
Source Port	3840	
Source Subnet	192.45.80.0	
Source Directory Number	22002	
Source_IP_Region	Unknown network-region	
Destination IP Address	192.45.82.240	
Destination Port	2926	
Destination Subnet	192.45.82.0	
Destination Directory Number	50001	
Receiver_IP_Region	192.45.80.15	
MOS	4.4	
Delay	0.0	msec
Jitter	1.0	msec
Network Loss	0.0	percent
Number of Packets Received	583	packets
Number of Packets Lost	0	packets

5. Interoperability Compliance Testing

The interoperability compliance testing included feature and serviceability testing. The feature testing evaluated the ability of NetAlly to provide quality of calls placed to and from stations. The serviceability testing introduced failure scenarios to see if NetAlly can resume recording after failure recovery.

5.1. General Test Approach

The general approach was to place various types of calls to and from stations, collect VoIP call quality data from NetAlly, and compare collected values with Avaya IP telephone’s Network

Audio Quality values. For feature testing, the types of calls included internal calls, inbound trunk calls, outbound trunk calls, transferred calls, conferenced calls. During the compliance test, the PacketStorm was utilized to simulate network delay and packet drop. For serviceability testing, failures such as cable pulls and resets were applied.

5.2. Test Results

NetAlly Lifecycle Manager successfully provided VoIP call quality data on various types of calls discussed in Section 5.1. For serviceability testing, NetAlly Lifecycle Manager was able to resume collecting VoIP call quality data after restoration of connectivity to the CLAN, and after resets of the NetAlly Lifecycle Manager and Avaya S8700 Media Server.

6. Verification Steps

The following steps were used to verify the configuration.

- Use the **ping** command to verify connectivity from the NetAlly Lifecycle Manager to all devices.
- Verify that calls can be successfully completed between the IP and Digital telephones.
- Compare VoIP quality data from the following sources:
  - PackStorm
  - Avaya IP telephone’s Network Audio Quality data
  - NetAlly Lifecycle Manager

7. Support

Technical support for the NetAlly Lifecycle Manager can be obtained by contacting Viola Networks Support via the support link at http://support.violanetworks.com or by calling the support telephone number at 978-620-1635.

8. Conclusion

These Application Notes illustrate the procedures for configuring the NetAlly Lifecycle Manager to monitor and correctly provide VoIP call quality statistics on the various types of calls placed to and from stations. In the configuration described in these Application Notes, NetAlly Lifecycle Manager employs SNMP to discover Avaya IP telephony network. During compliance testing, NetAlly Lifecycle Manager successfully monitored call streams and provide VoIP call quality data.

9. References

This section references the Avaya and Viola Networks documentation that are relevant to these Application Notes.

The following Avaya product documentation can be found at http://support.avaya.com.

[1] *Administration for Network Connectivity for Avaya Communication Manager*, Issue 10, June 2005, Document Number 555-233-504.

[2] *Administrator Guide for Avaya Communication Manager*, Issue 1, June 2005, Document Number 03-300509

Viola Networks provided the following Viola Networks product documentation. For additional product and company information, visit http://www.violanetworks.com.

[3] NetAlly Users Guide: Release 5.1

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.