Application Notes for NetCordia NetMRI with Avaya Communication Manager - Issue 1.0

Abstract

These Application Notes describe the configuration procedures required for NetCordia NetMRI to interoperate with Avaya Communication Manager. NetMRI is a network analysis appliance that can quickly and independently determine network health issues and suggest corrective action.

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 NetCordia NetMRI 1.5p4 to interoperate with Avaya Communication Manager 3.1.2. The purpose of the testing was to verify that NetMRI recorded each phone call and the performance metrics recorded match those from the endpoints. In addition, it was verified that NetMRI could discover and properly identify the devices in the lab, and could determine which phones were registered to which call server.

NetMRI is a network analysis appliance that can quickly and independently determine network health issues and suggest corrective action. NetMRI analyzes router/switch configurations in single or mixed vendor networks to optimize the network and VoIP performance as well.

Figure 1 illustrates the network configuration used to verify the NetCordia solution. The figure shows two separate communication systems, each running Avaya Communication Manager on separate Avaya Media Servers. Site A is comprised of the NetCordia NetMRI, a pair of Avaya S8700 Media Servers and an Avaya G650 Media Gateway, which has connections to the following: Avaya 4600 Series IP Telephones and an Avaya 6400 Series Digital Telephone. 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 an 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 an Analog Telephone. Site C is setup as Local Survivable Processor (LSP) to Site A. An IP trunk connects the two Avaya Communication Manager systems.

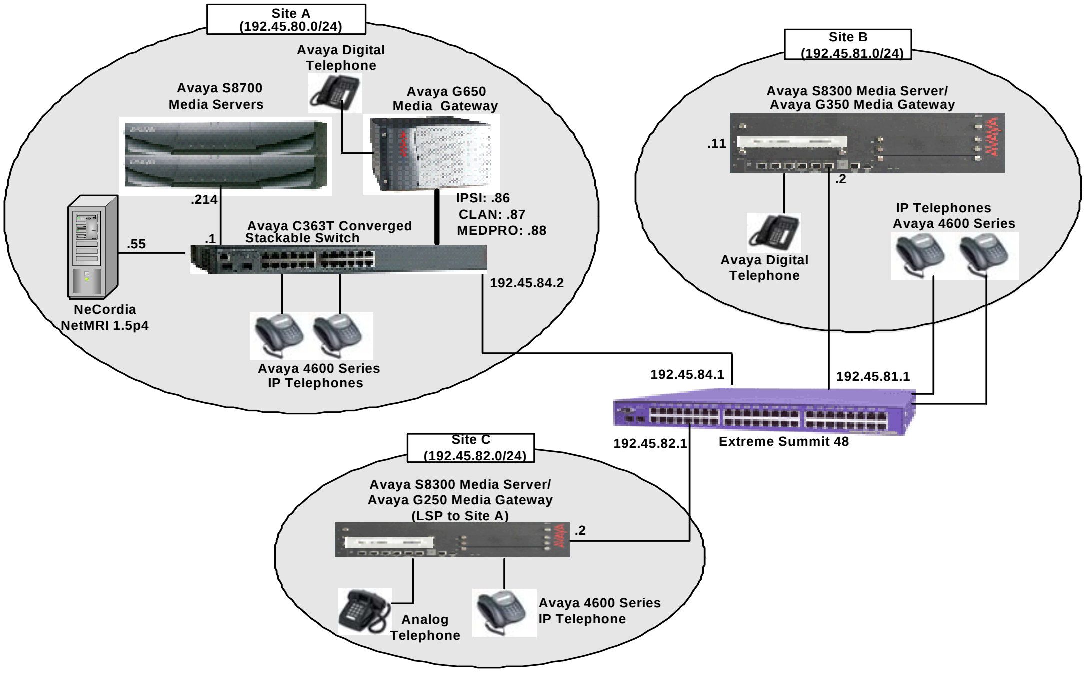


Figure 1. Test configuration of NetMRI with Avaya Communication Manager

2. Equipment and Software Validated

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

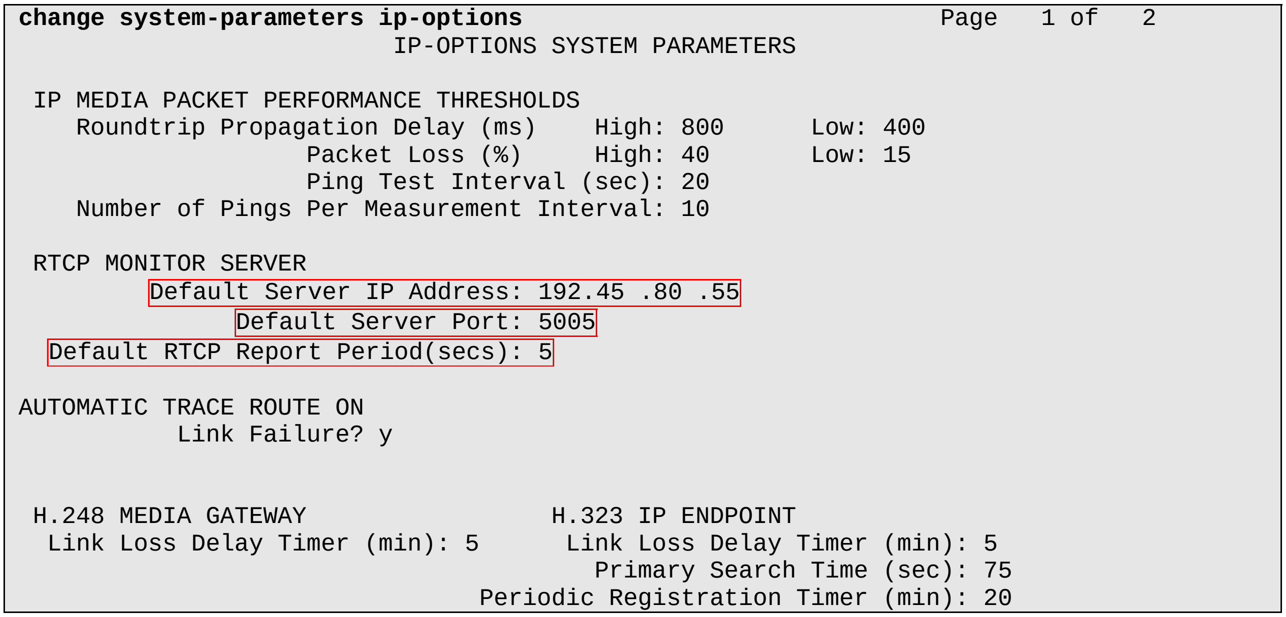
Equipment		Software
Avaya S8700 Media Server		Communication Manager 3.1.2 (R013x.01.2.632.1)
Avaya G650 Media Gateway		
	TN2312BP IP Server Interface	HW11 FW030
	TN799DP C-LAN Interface	HW20 FW017
	TN2302AP IP Media Processor	HW01 FW108
	TN2602AP IP Media Processor	HW02 FW007
Avaya S8300 Media Server 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	2.6
	4621	2.6
	4625	2.5
Avaya 6400 Series Digital Telephones		-
Analog Telephones		-
Avaya C363T-PWR Converged Stackable Switch		4.5.14
Extreme Summit 48		4.1.21
NetCordia NetMRI OS –RedHat Linux 9		1.5p4

3. Configuring Avaya Communication Manager

This section provides the procedures for configuring Avaya Communication Manager. Since NetMRI utilizes RTCP packets to calculate and report the quality of the call stream, RTCP monitor server parameters must be administered 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 parameters. Provide the following information:

- **Default Server IP Address** - IP address of the NetMRI server
- **Default Server Port** – 5005 [This port number must match with the NetMRI Traffic Agent RTCP Listening Port. The default value for the Default Server Port field is 5005.]
- **Default RTCP Report Period(secs)** – 5 [The report period indicates how often Avaya Communication Manager endpoints forward RTCP packets to the RTCP monitor server, which is the NetMRI server. The default value for the Default RTCP Report Period(secs) field is 5.]

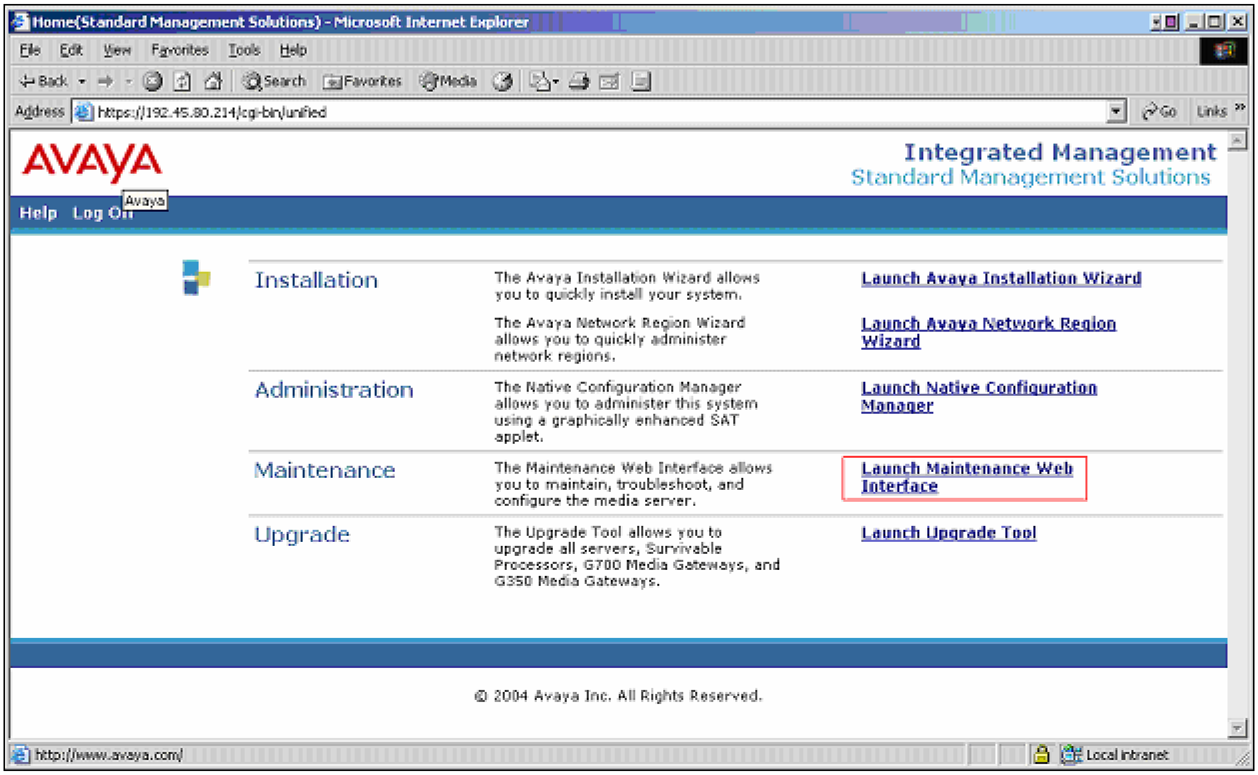
Default values may be used in the remaining fields.



```
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 .55
               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
```

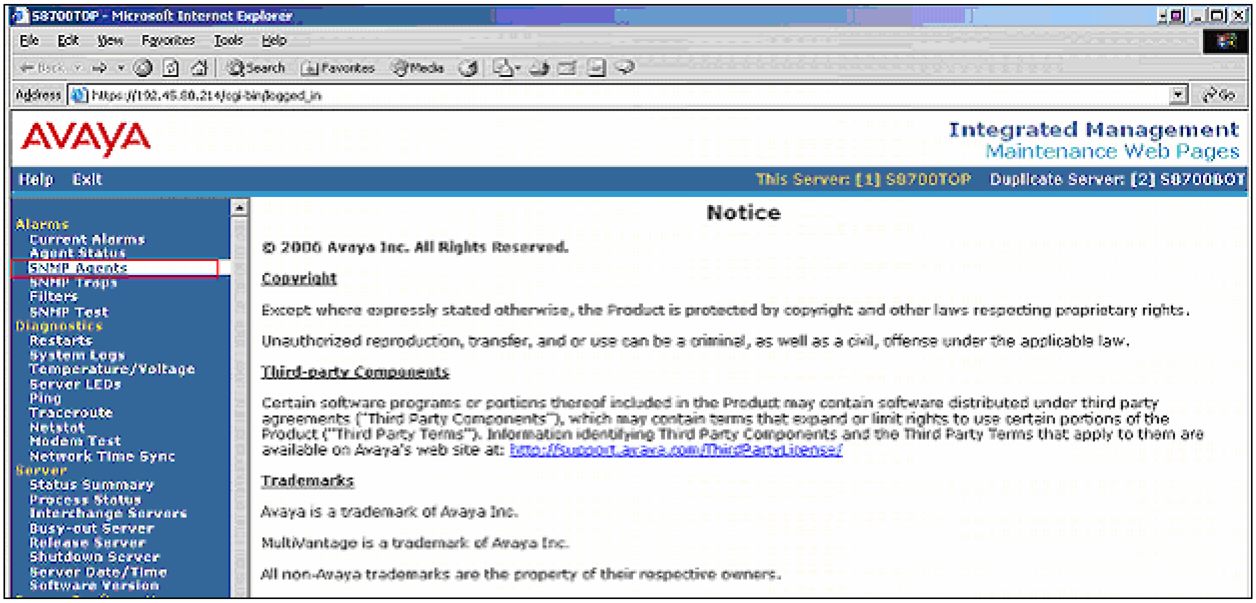
For NetMRI to create an IP Telephony table, SNMP needs to be enabled on the Avaya S8700 and S8300 Media Servers. NetMRI utilize a network discovery tool and SNMP to find VoIP endpoints in the network. Once SNMP is enabled, NetMRI utilizes SNMP to extract information from Avaya Communication Manager. 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. For an S8700 Media Server pair, the SNMP trap destinations need to be configured on each media server. Select **Launch Maintenance Web Interface** from the screen.


Home(Standard Management Solutions) - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://192.45.80.214/cgi-bin/unified
Go Links
AVAYA
Integrated Management
Standard Management Solutions
Help Log Off
Avaya
© 2004 Avaya Inc. All Rights Reserved.
http://www.avaya.com/
Local intranet

Installation	The Avaya Installation Wizard allows you to quickly install your system.	Launch Avaya Installation Wizard
	The Avaya Network Region Wizard allows you to quickly administer network regions.	Launch Avaya Network Region Wizard
Administration	The Native Configuration Manager allows you to administer this system using a graphically enhanced SAT applet.	Launch Native Configuration Manager
Maintenance	The Maintenance Web Interface allows you to maintain, troubleshoot, and configure the media server.	Launch Maintenance Web Interface
Upgrade	The Upgrade Tool allows you to upgrade all servers, Survivable Processors, G700 Media Gateways, and G350 Media Gateways.	Launch Upgrade Tool

In the Alarms section, click on the **SNMP Agents** link 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

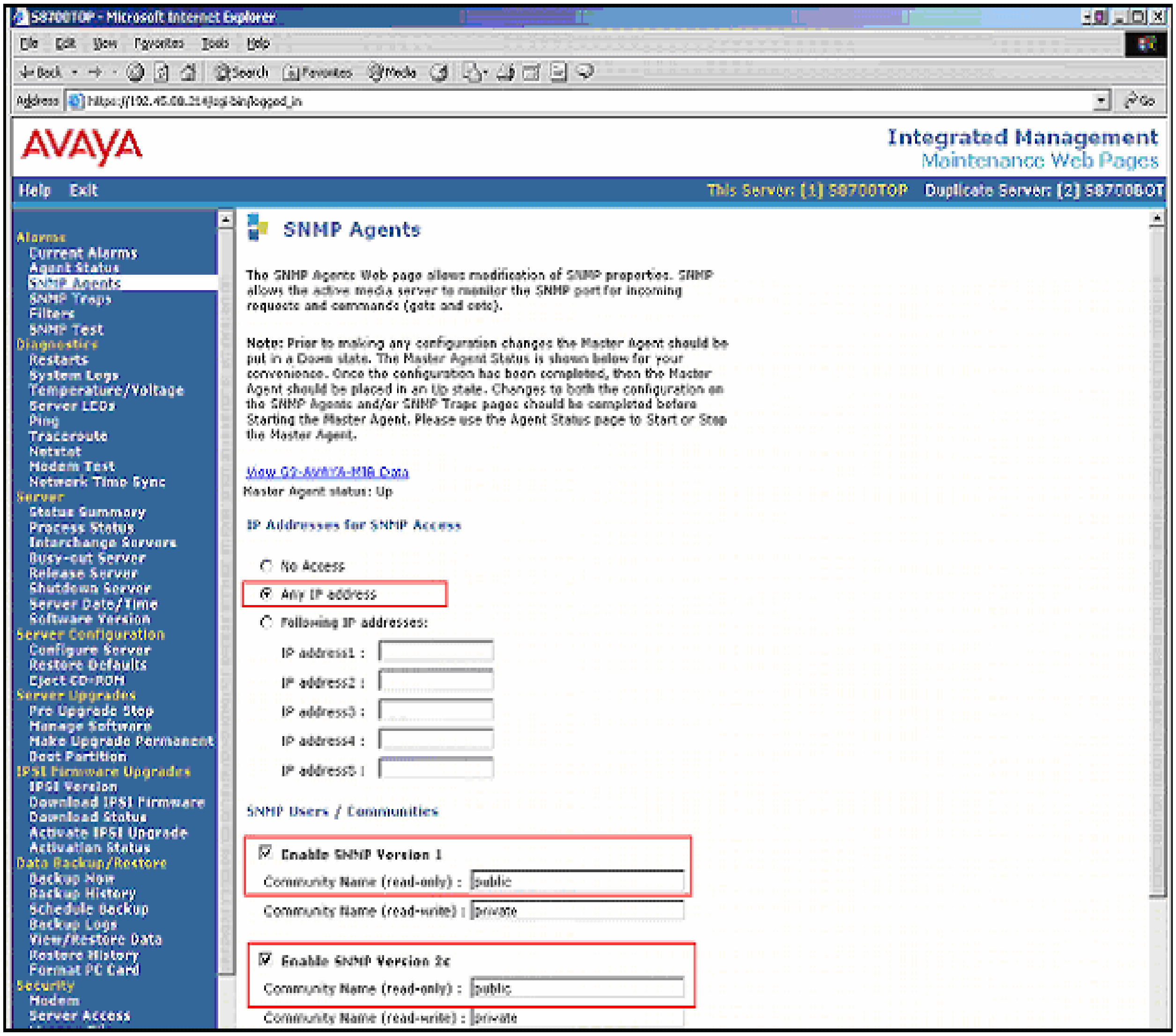
Avaya is a trademark of Avaya Inc.

MultiVantage is a trademark of Avaya Inc.

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

In the “SNMP Agents” page, select **Any IP Address** under the “IP Addresses for SNMP Access” section. This implies that any device can perform SNMP request to the Avaya media servers. For security purposes, an administrator may restrict the access by specifying IP address(s) under the “Following IP addresses” field for the SNMP access. Enable SNMP version 2c by clicking the check box. Set the “Community Name (read-only)” field to **public** on SNMP version 2c. The community name configured in the Avaya media server has to match with NetMRI.

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

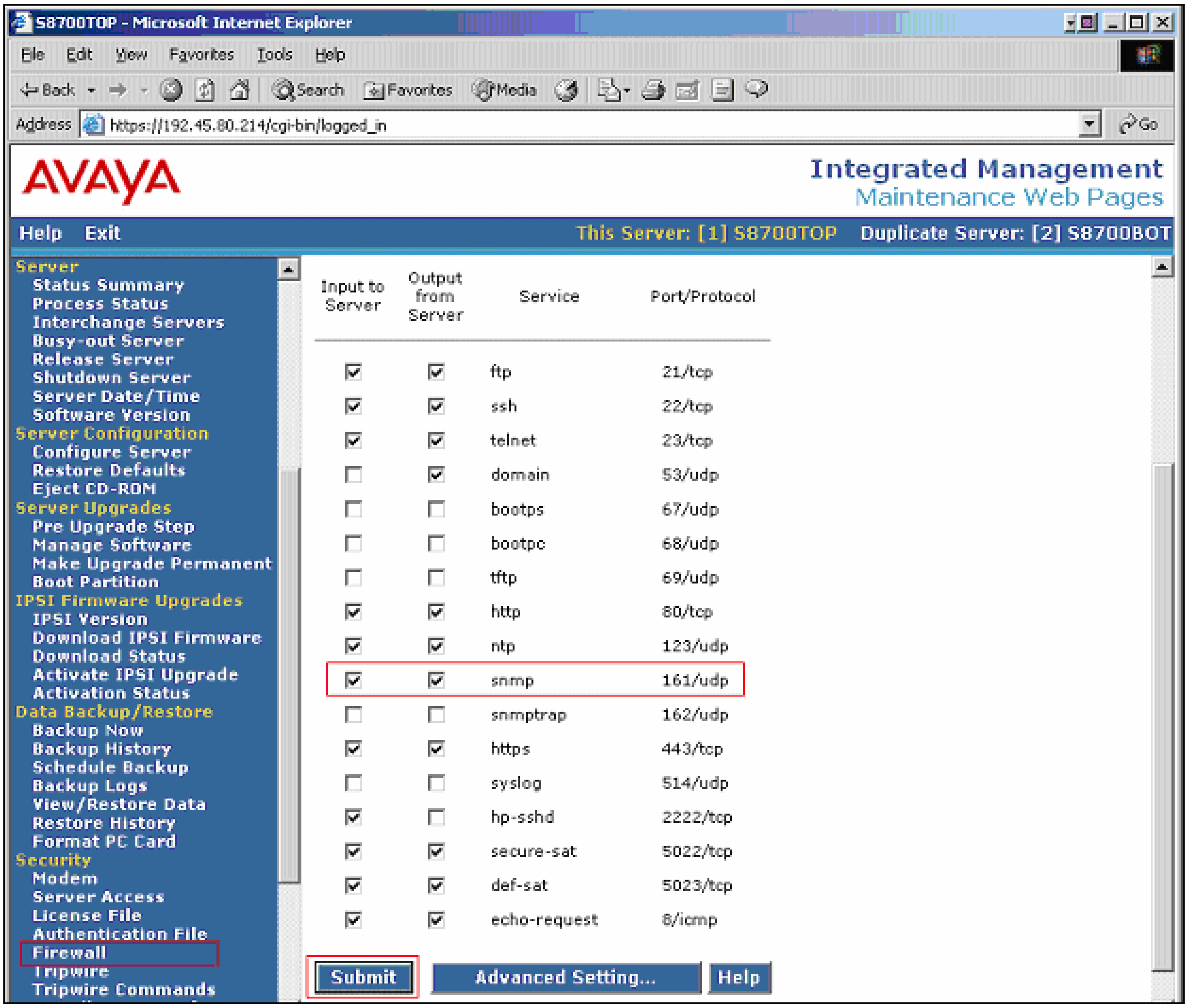
Community Name (read-write) : private

☑ 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.



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 NetMRI

The steps in this section describe the configuration of NetMRI to receive RTCP packets from the VoIP endpoints, and record performance metrics. For additional information on configuring the NetCordia NetMRI, refer to [3].

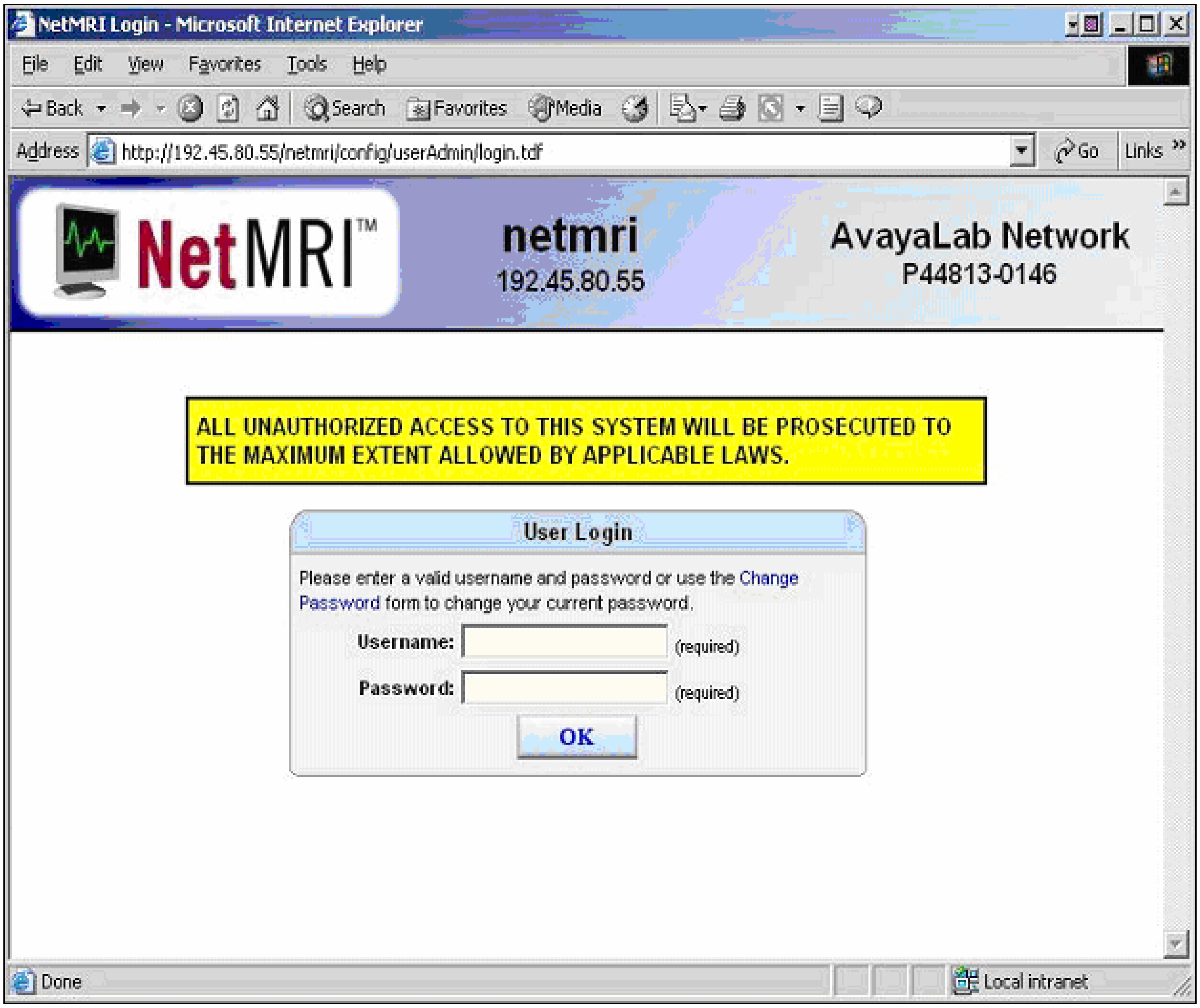
The configuration for NetMRI consists of the following components:

- Network Discovery - NetMRI discovers all endpoints in the network.
- SNMPwalk - Once all endpoints are discovered, NetMRI performs an SNMPwalk on the Avaya Media Server, using the MIB OID to identify the VoIP endpoints that are registered to the gateway.

- Monitoring – NetMRI receives RTCP packets from the VoIP endpoints and provides VoIP call quality data. The port for receiving RTCP packets from VoIP endpoints is fixed at 5005.

4.1. NetMRI Network Discovery

To configure NetMRI network discovery, launch a web browser and connect to NetMRI by entering http://<NetMRI Lifecycle Manager IP address>. Supply **Username** and **Password**, and click the **OK** button to access the NetMRI Issues page.



http://192.45.80.55/netmri/config/userAdmin/login.tdf

netmri
192.45.80.55

AvayaLab Network
P44813-0146

ALL UNAUTHORIZED ACCESS TO THIS SYSTEM WILL BE PROSECUTED TO THE MAXIMUM EXTENT ALLOWED BY APPLICABLE LAWS.

User Login

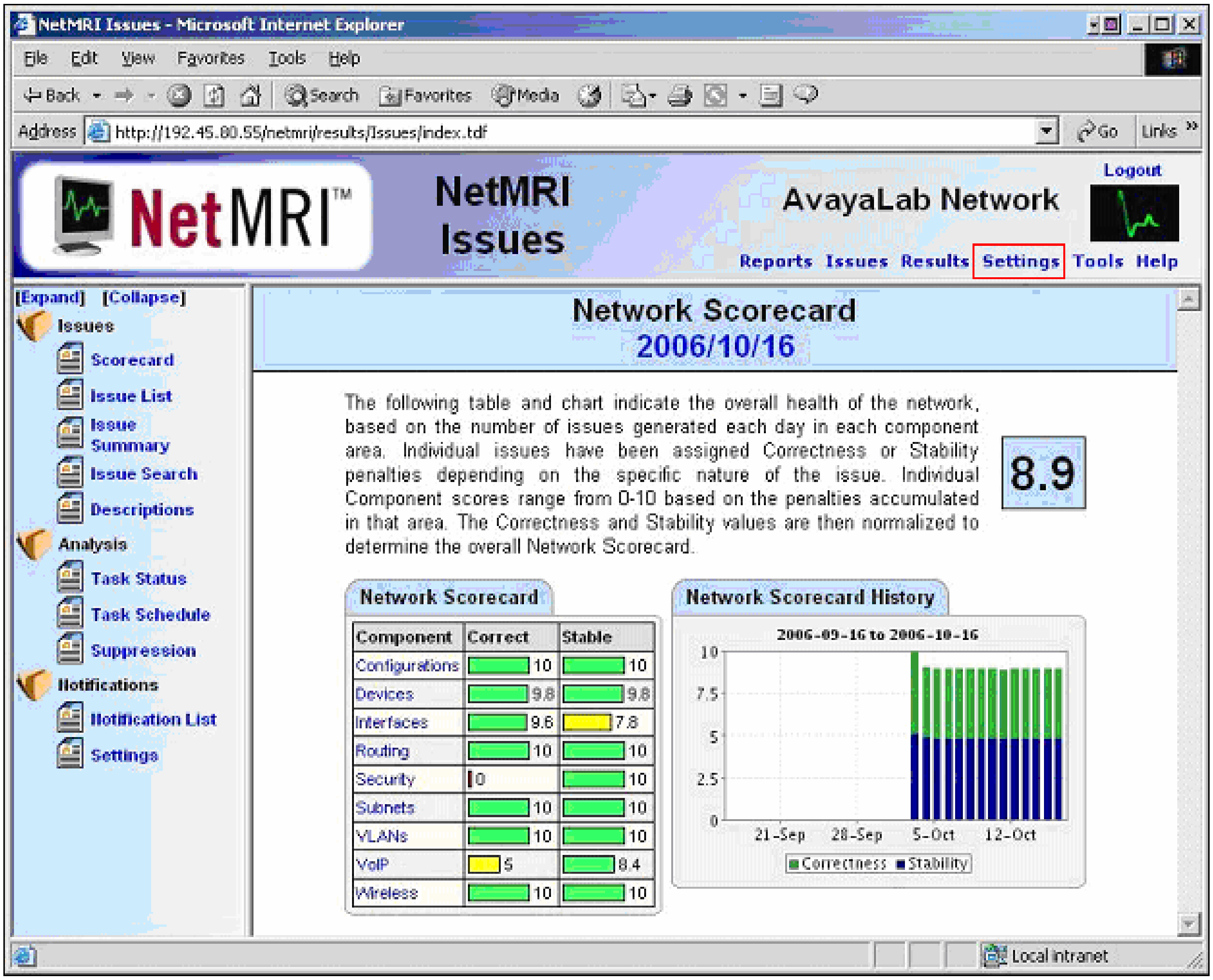
Please enter a valid username and password or use the Change Password form to change your current password.

Username: (required)

Password: (required)

OK

The following “NetMRI Issues” page shows the table and chart that indicate the overall health of the network, based on the number of issues generated each day in each component area. To perform the discovery function, select **Settings** from the top menu.



Network Scorecard
2006/10/16

The following table and chart indicate the overall health of the network, based on the number of issues generated each day in each component area. Individual issues have been assigned Correctness or Stability penalties depending on the specific nature of the issue. Individual Component scores range from 0-10 based on the penalties accumulated in that area. The Correctness and Stability values are then normalized to determine the overall Network Scorecard.

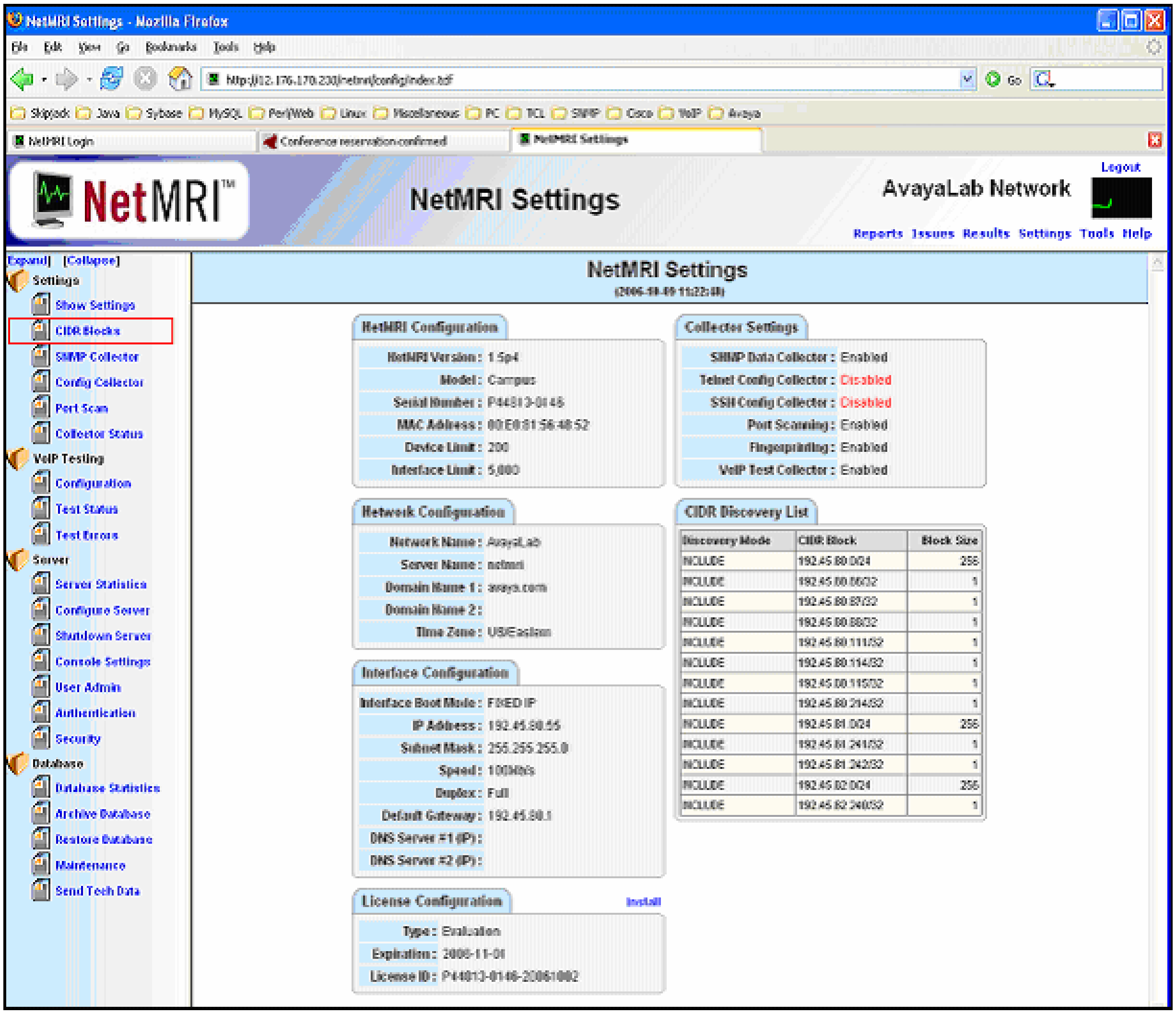
8.9

Network Scorecard

Component	Correct	Stable
Configurations	10	10
Devices	9.8	9.8
Interfaces	9.6	7.8
Routing	10	10
Security	0	10
Subnets	10	10
VLANs	10	10
VoIP	5	8.4
Wireless	10	10

Network Scorecard History

Select the **CIDR Blocks** link in the left pane of the window to add networks to be included for performing discovery.



NetMRI Settings
(2006-10-09 11:22:48)

NetMRI Configuration

NetMRI Version :	1.5p4
Model :	Campus
Serial Number :	P44813-0146
MAC Address :	00:E0:81:56:48:52
Device Limit :	200
Interface Limit :	5,000

Collector Settings

SNMP Data Collector :	Enabled
Telnet Config Collector :	Disabled
SSH Config Collector :	Disabled
Port Scanning :	Enabled
Fingerprinting :	Enabled
VoIP Test Collector :	Enabled

Network Configuration

Network Name :	AvayaLab
Server Name :	netmri
Domain Name 1 :	avaya.com
Domain Name 2 :	
Time Zone :	US/Eastern

CIDR Discovery List

Discovery Mode	CIDR Block	Block Size
INCLUDE	192.45.80.0/24	256
INCLUDE	192.45.80.86/32	1
INCLUDE	192.45.80.87/32	1
INCLUDE	192.45.80.88/32	1
INCLUDE	192.45.80.111/32	1
INCLUDE	192.45.80.114/32	1
INCLUDE	192.45.80.115/32	1
INCLUDE	192.45.80.214/32	1
INCLUDE	192.45.81.0/24	256
INCLUDE	192.45.81.241/32	1
INCLUDE	192.45.81.242/32	1
INCLUDE	192.45.82.0/24	256
INCLUDE	192.45.82.240/32	1

Interface Configuration

Interface Boot Mode :	FIXED IP
IP Address :	192.45.80.55
Subnet Mask :	255.255.255.0
Speed :	100Mb/s
Duplex :	Full
Default Gateway :	192.45.80.1
DNS Server #1 (IP) :	
DNS Server #2 (IP) :	

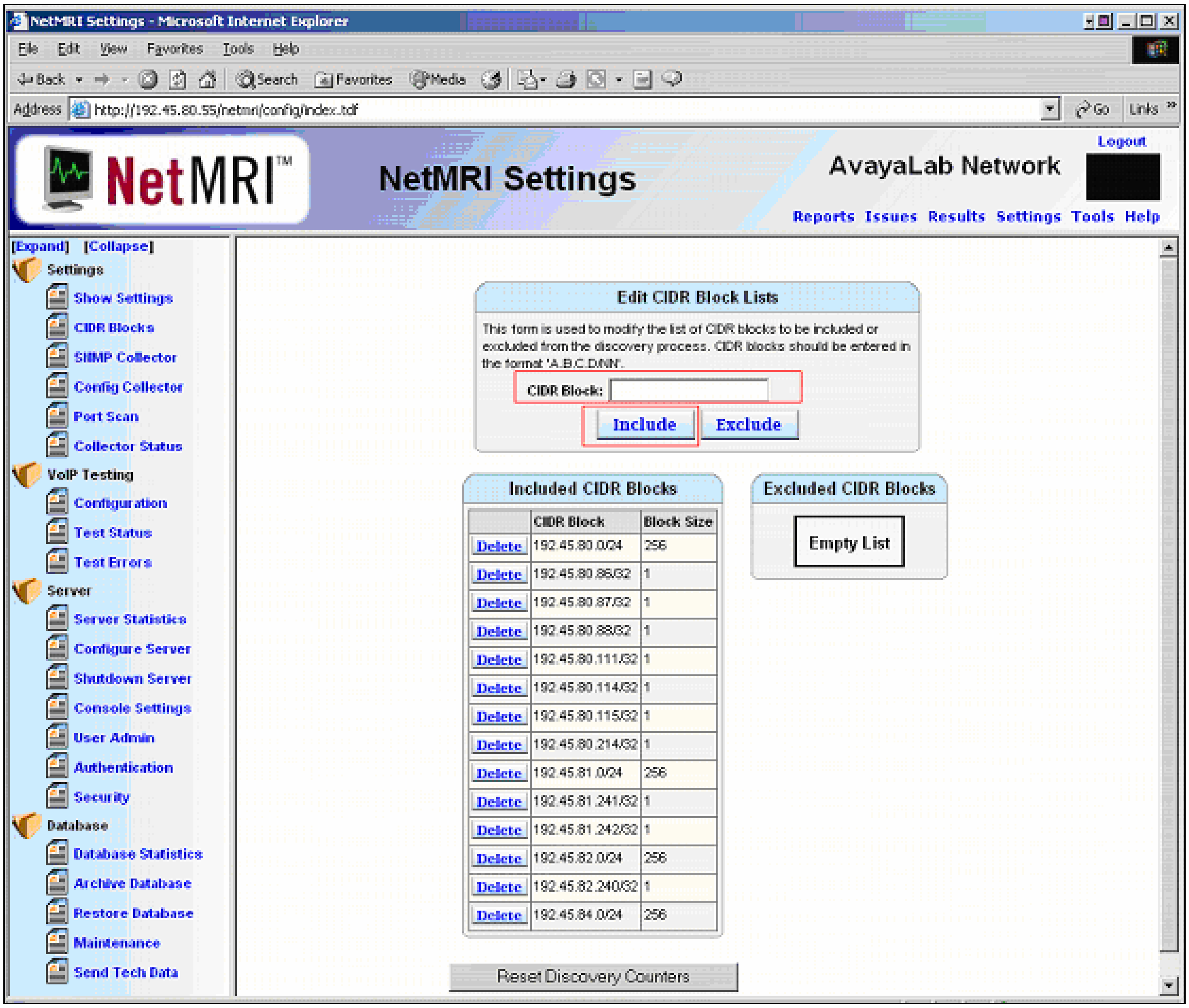
License Configuration

Type :	Evaluation
Expiration :	2006-11-01
License ID :	P44813-0146-20061002

The format for adding the CIDR block is as follows:

- Provide the **IP address** and **subnet mask** of the network in the “CIDR Blocks” field.
- Click the **Include** button.

Once the “Include” button is clicked, the discovery process begins on that network.



Edit CIDR Block Lists

This form is used to modify the list of CIDR blocks to be included or excluded from the discovery process. CIDR blocks should be entered in the format 'A.B.C.D/NN'.

CIDR Block:

Include Exclude

Included CIDR Blocks

	CIDR Block	Block Size
Delete	192.45.80.0/24	256
Delete	192.45.80.86/32	1
Delete	192.45.80.87/32	1
Delete	192.45.80.88/32	1
Delete	192.45.80.111/32	1
Delete	192.45.80.114/32	1
Delete	192.45.80.115/32	1
Delete	192.45.80.214/32	1
Delete	192.45.81.0/24	256
Delete	192.45.81.241/32	1
Delete	192.45.81.242/32	1
Delete	192.45.82.0/24	256
Delete	192.45.82.240/32	1
Delete	192.45.84.0/24	256

Excluded CIDR Blocks

Empty List

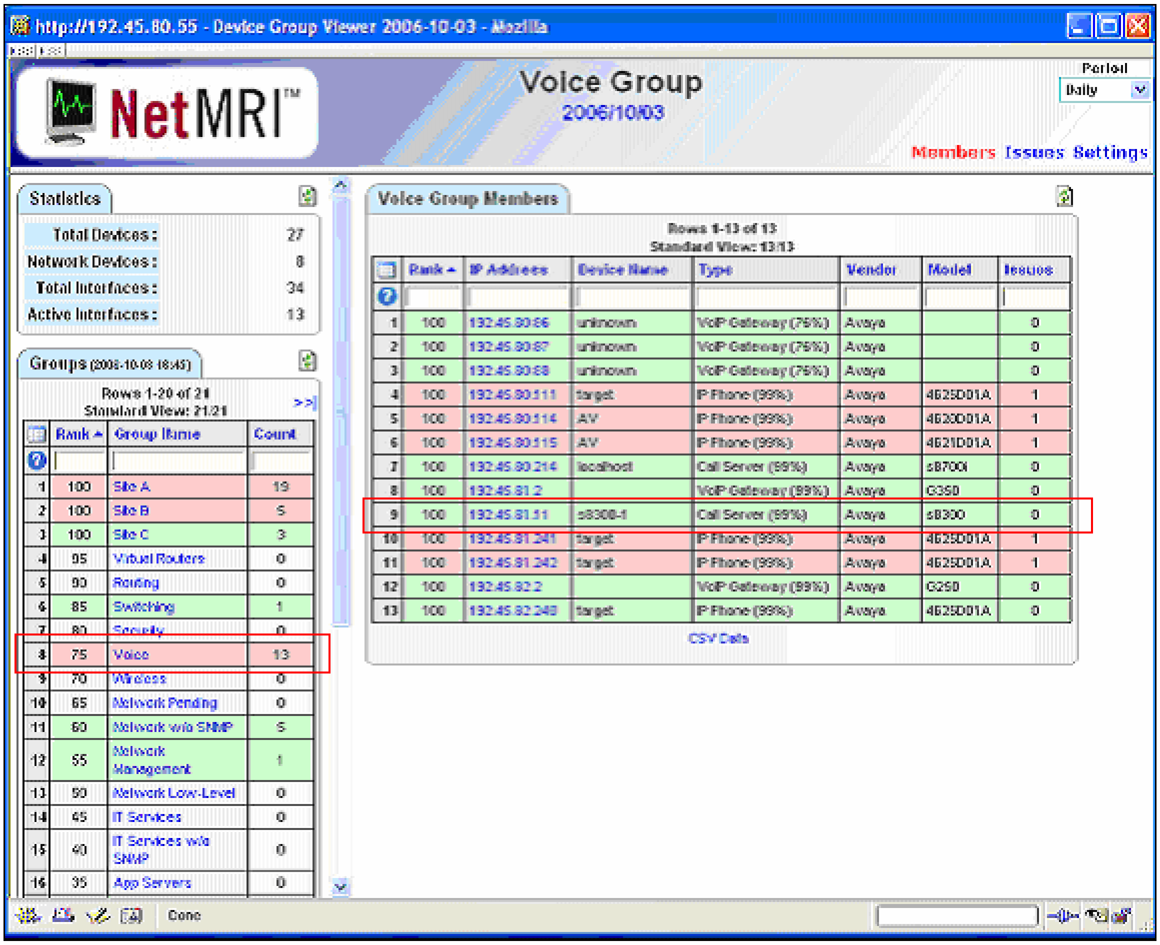
Reset Discovery Counters

4.2. NetMRI VoIP Discovery

The following screen displays the Voice group membership, which is the result of the discovery and SNMPwalk. The Voice group is a pre-defined system group that includes any devices used in a VoIP network. Device Groups categorize devices into user-definable groups. To view this page, navigate to the **Results → Network → Device Groups** page. Select **Voice** from the Groups table. The Voice Group Members table appears in the right pane of the window, as shown below.

This page contained VoIP devices along with some color codes. Any device that has been included in a NetMRI Issue is highlighted in red. The issue raised for these devices is the NetMRI VoIP Call Performance Threshold Exceeded issue. The analysis task that generates this issue was run at the end of the testing period.

Additional details about the device may be obtained by clicking on the IP address of any device listed in the Voice Group Members table. In this example, the IP address (192.45.81.11), which is the Avaya S8300 Media Server, is selected.



Statistics

Total Devices:	27
Network Devices:	8
Total Interfaces:	34
Active Interfaces:	13

Groups (2006-10-03 18:45)

Rows 1-20 of 21
Standard View: 21/21

	Rank	Group Name	Count
1	100	Site A	19
2	100	Site B	5
3	100	Site C	3
4	95	Virtual Routers	0
5	90	Routing	0
6	85	Switching	1
7	80	Security	0
8	75	Voice	13
9	70	Wireless	0
10	65	Network Pending	0
11	60	Network w/o SNMP	5
12	55	Network Management	1
13	50	Network Low-Level	0
14	45	IT Services	0
15	40	IT Services w/o SNMP	0
16	35	App Servers	0

Voice Group Members

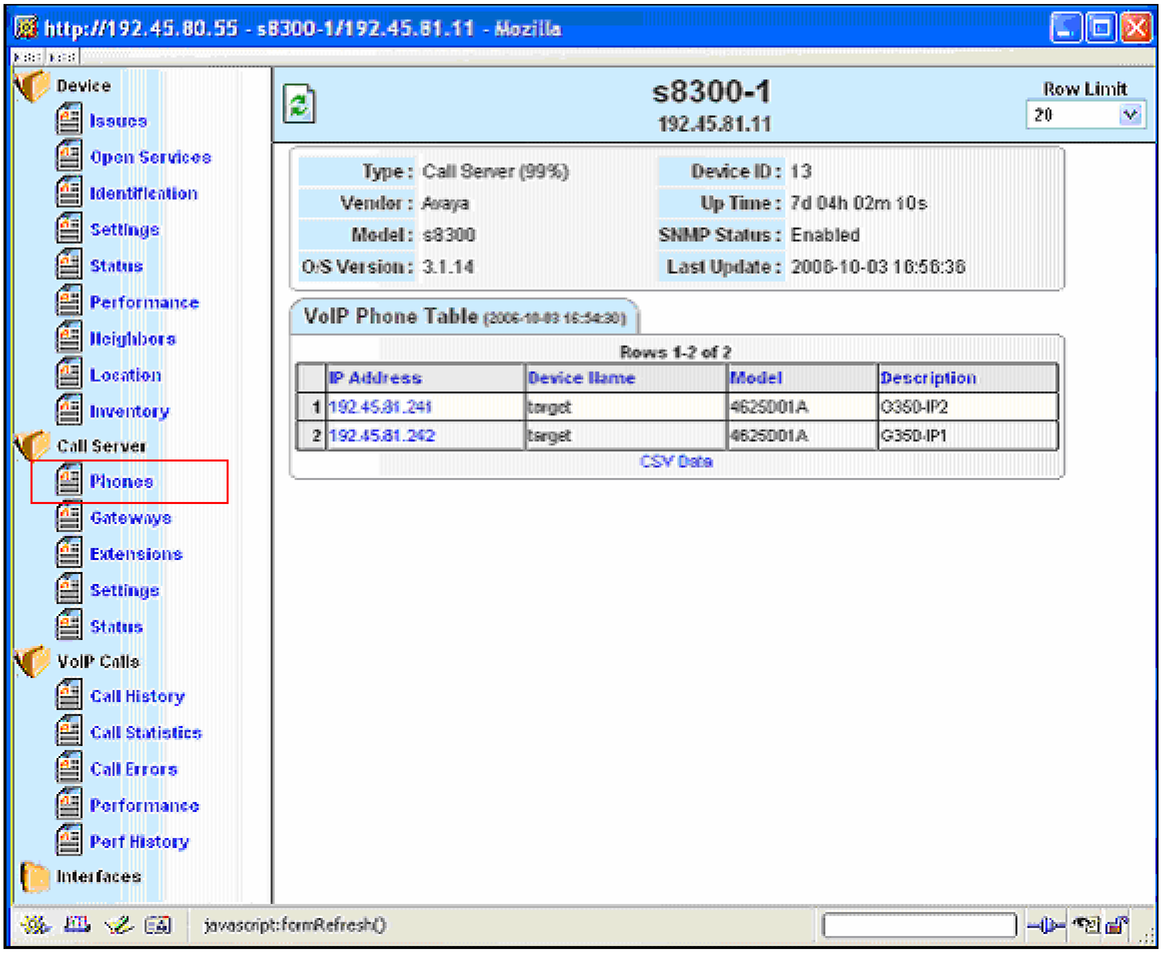
Rows 1-13 of 13
Standard View: 13/13

	Rank	IP Address	Device Name	Type	Vendor	Model	Issues
1	100	192.45.80.66	unknown	VoIP Gateway (75%)	Avaya		0
2	100	192.45.80.67	unknown	VoIP Gateway (75%)	Avaya		0
3	100	192.45.80.68	unknown	VoIP Gateway (75%)	Avaya		0
4	100	192.45.80.111	target	IP Phone (99%)	Avaya	4625D01A	1
5	100	192.45.80.114	AV	IP Phone (99%)	Avaya	4620D01A	1
6	100	192.45.80.115	AV	IP Phone (99%)	Avaya	4621D01A	1
7	100	192.45.80.214	localhost	Call Server (99%)	Avaya	s8700	0
8	100	192.45.81.2		VoIP Gateway (99%)	Avaya	G350	0
9	100	192.45.81.11	s8300-1	Call Server (99%)	Avaya	s8300	0
10	100	192.45.81.241	target	IP Phone (99%)	Avaya	4625D01A	1
11	100	192.45.81.242	target	IP Phone (99%)	Avaya	4625D01A	1
12	100	192.45.82.2		VoIP Gateway (99%)	Avaya	G250	0
13	100	192.45.82.248	target	IP Phone (99%)	Avaya	4625D01A	0

CSV Data

The Device Viewer page, which is the result of clicking on the IP address of this device from the Voice Group Members table previously discussed, is displayed. The Device Viewer page displays the discovery information about a device at the top of the page. This includes the device type, vendor, model, and O/S version information. The next two screens show various pages for this device as related to the collection of VoIP data.

By selecting the **Phones** link under the Call Server section, the Device Viewer page displays the VoIP Phone Table. The VoIP Phones Table provides a list of registered phones.



s8300-1
192.45.81.11

Type :	Call Server (99%)	Device ID :	13
Vendor :	Avaya	Up Time :	7d 04h 02m 10s
Model :	s8300	SNMP Status :	Enabled
O/S Version :	3.1.14	Last Update :	2006-10-03 16:56:36

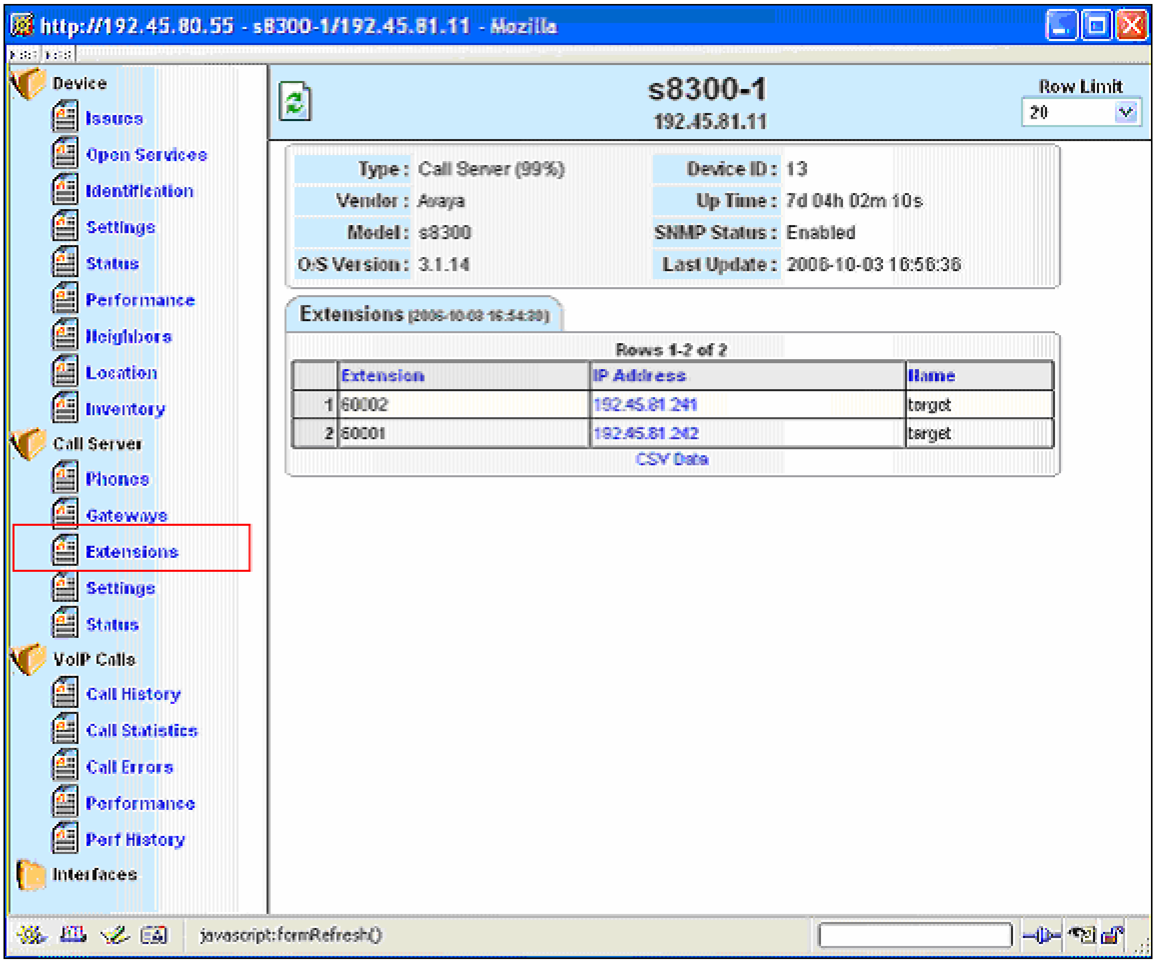
VoIP Phone Table (2006-10-03 16:54:30)

Rows 1-2 of 2

	IP Address	Device Name	Model	Description
1	192.45.81.241	target	4625D01A	G350-IP2
2	192.45.81.242	target	4625D01A	G350-IP1

CSV Data

The following screen is another example of providing all registered phones in terms of extension number. This can be accomplished by clicking the **Extensions** link under the Call Server section.



s8300-1
192.45.81.11

Type :	Call Server (99%)	Device ID :	13
Vendor :	Avaya	Up Time :	7d 04h 02m 10s
Model :	s8300	SNMP Status :	Enabled
O/S Version :	3.1.14	Last Update :	2006-10-03 16:56:36

Extensions (2006-10-03 16:54:30)

Rows 1-2 of 2

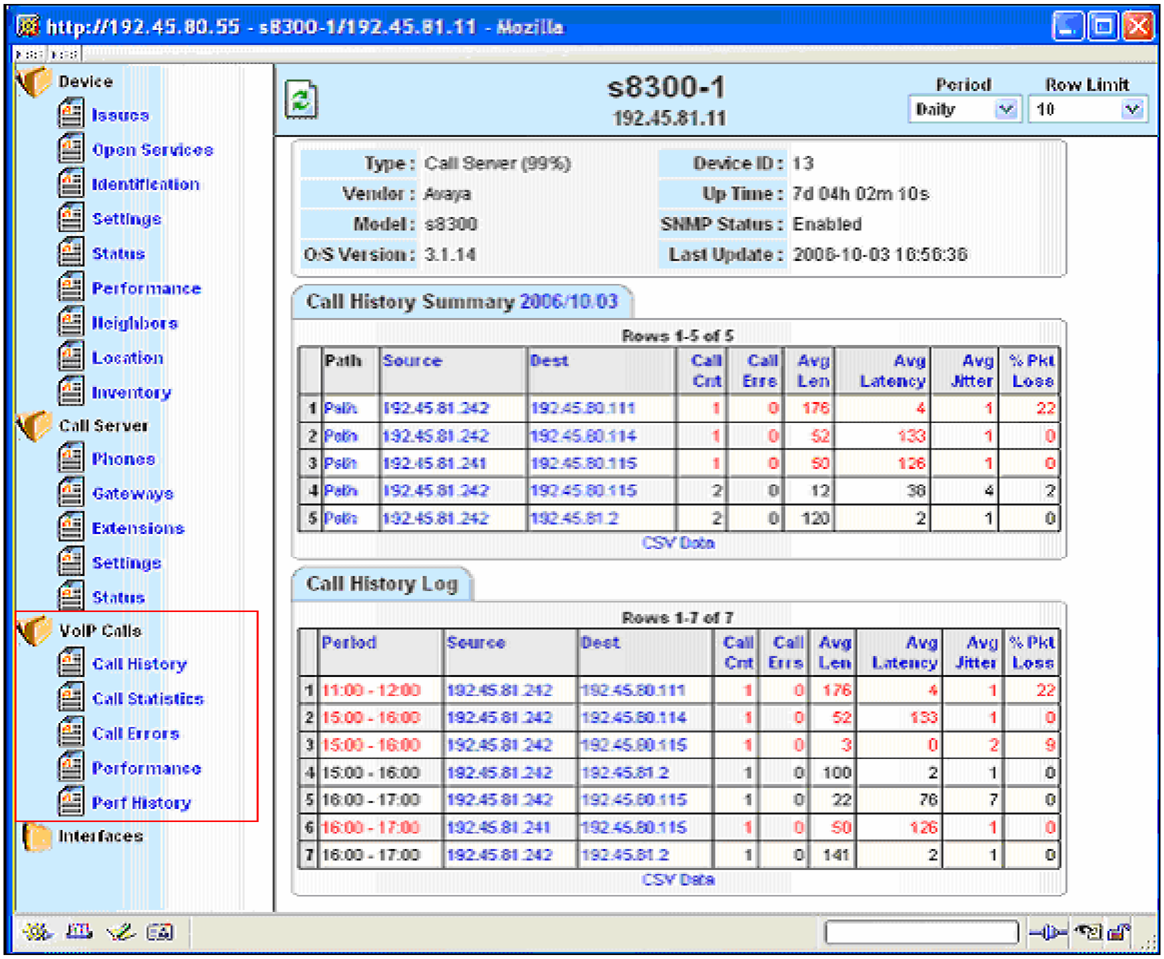
	Extension	IP Address	Name
1	60002	192.45.81.241	target
2	60001	192.45.81.242	target

CSV Data

4.3. NetMRI VoIP Calls Monitoring

NetMRI can monitor VoIP calls through several different ways, using the VoIP Calls section in the left pane of the window. To access the following sample page, navigate to the **Results → Network → Device Groups** page, select **Voice** from the Groups table in the left pane of the window, and select the IP address for the Avaya S8300 Media Server (192.45.81.11). This process will open the following window. The VoIP Calls section in the left pane of the window lists types of monitoring.

The Call History page displays calls made between two endpoints and the statistics for each on the selected date and time period. The first table shows calls between two endpoints grouped into one row. The number of calls, errors, average length, average latency, average jitter, and average packet loss of all calls is displayed. The second table displays the above information broken into hourly segments. If NetMRI cannot determine the IP address of one of the endpoints involved, the endpoint phone number will be displayed in its place. The link labeled "Path" in the chart launches the NetMRI path diagnostic chart. This chart shows the layer 2 and 3 path between the two selected endpoints highlighting any issues that NetMRI has discovered for any devices in the path that may affect the quality of a phone call between those two endpoints.



s8300-1
192.45.81.11

Period: Daily
Row Limit: 10

Type :	Call Server (99%)	Device ID :	13
Vendor :	Avaya	Up Time :	7d 04h 02m 10s
Model :	s8300	SNMP Status :	Enabled
O/S Version :	3.1.14	Last Update :	2006-10-03 16:56:36

Call History Summary 2006/10.03

Rows 1-5 of 5

	Path	Source	Dest	Call Cnt	Call Errs	Avg Len	Avg Latency	Avg Jitter	% Pkt Loss
1	Path	192.45.81.242	192.45.80.111	1	0	176	4	1	22
2	Path	192.45.81.242	192.45.80.114	1	0	52	133	1	0
3	Path	192.45.81.241	192.45.80.115	1	0	50	126	1	0
4	Path	192.45.81.242	192.45.80.115	2	0	12	38	4	2
5	Path	192.45.81.242	192.45.81.2	2	0	120	2	1	0

CSV Data

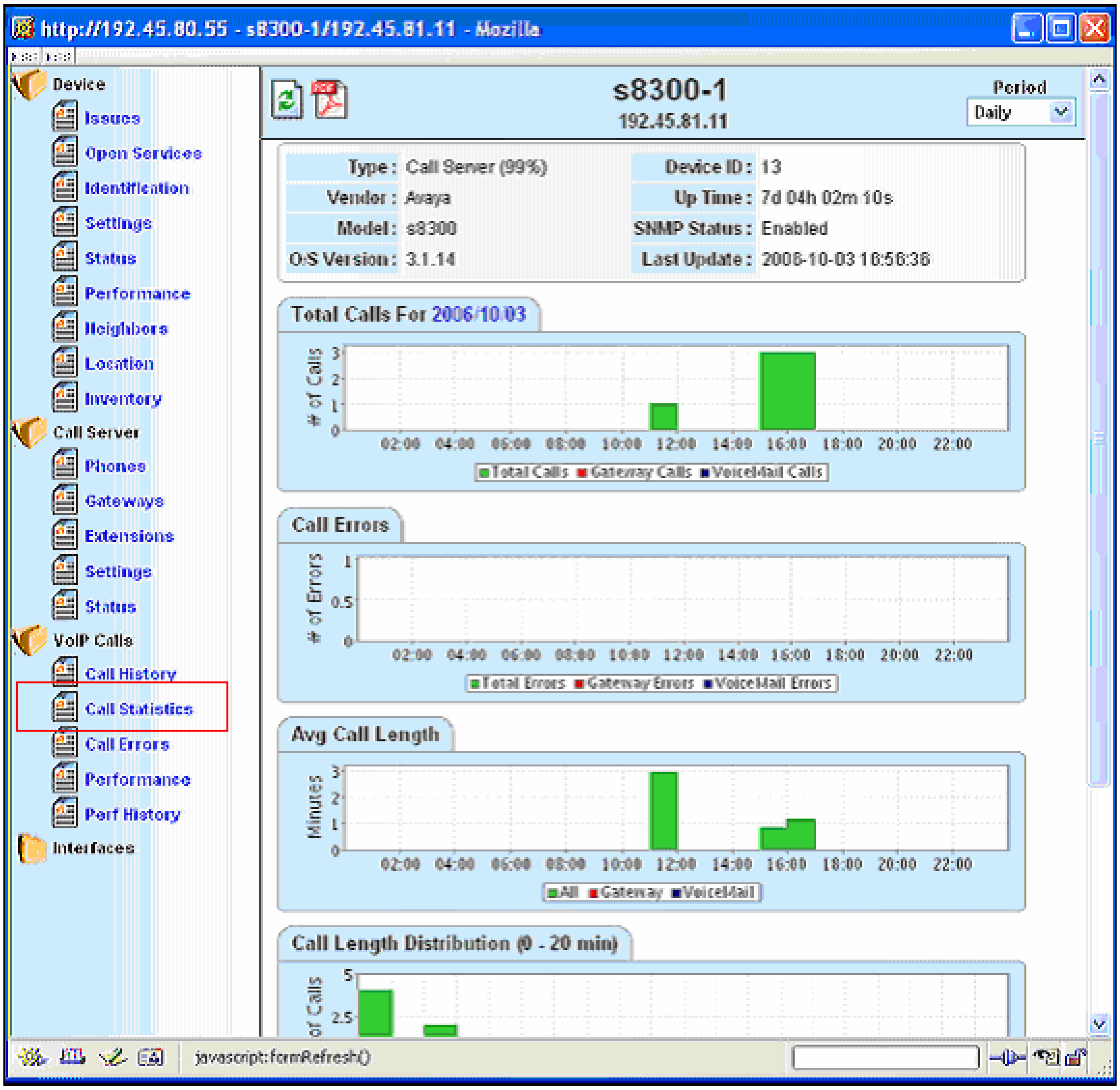
Call History Log

Rows 1-7 of 7

	Period	Source	Dest	Call Cnt	Call Errs	Avg Len	Avg Latency	Avg Jitter	% Pkt Loss
1	11:00 - 12:00	192.45.81.242	192.45.80.111	1	0	176	4	1	22
2	15:00 - 16:00	192.45.81.242	192.45.80.114	1	0	52	133	1	0
3	15:00 - 16:00	192.45.81.242	192.45.80.115	1	0	3	0	2	9
4	15:00 - 16:00	192.45.81.242	192.45.81.2	1	0	100	2	1	0
5	16:00 - 17:00	192.45.81.242	192.45.80.115	1	0	22	76	7	0
6	16:00 - 17:00	192.45.81.241	192.45.80.115	1	0	50	126	1	0
7	16:00 - 17:00	192.45.81.242	192.45.81.2	1	0	141	2	1	0

CSV Data

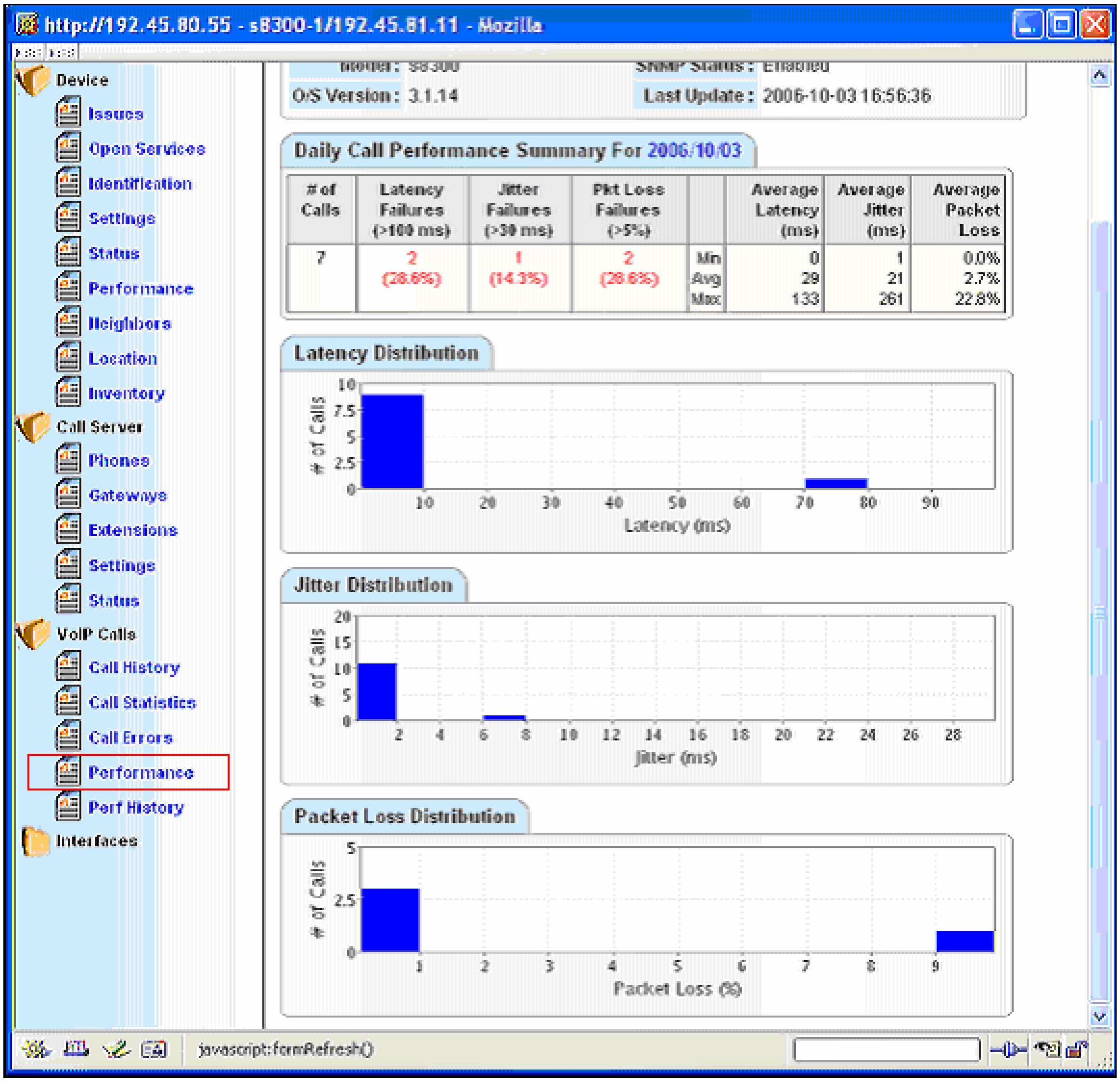
The Call Statistics page, shown below, groups all calls into various charts for display.



s8300-1
192.45.81.11

Type :	Call Server (99%)	Device ID :	13
Vendor :	Avaya	Up Time :	7d 04h 02m 10s
Model :	s8300	SNMP Status :	Enabled
O/S Version :	3.1.14	Last Update :	2006-10-03 16:56:36

The following screen displays the Performance page, which shows the average latency, jitter, and packet loss for calls made. It also indicates how many of those calls exceeded the error thresholds defined for each metric. Distribution charts for all calls within the thresholds are also displayed.



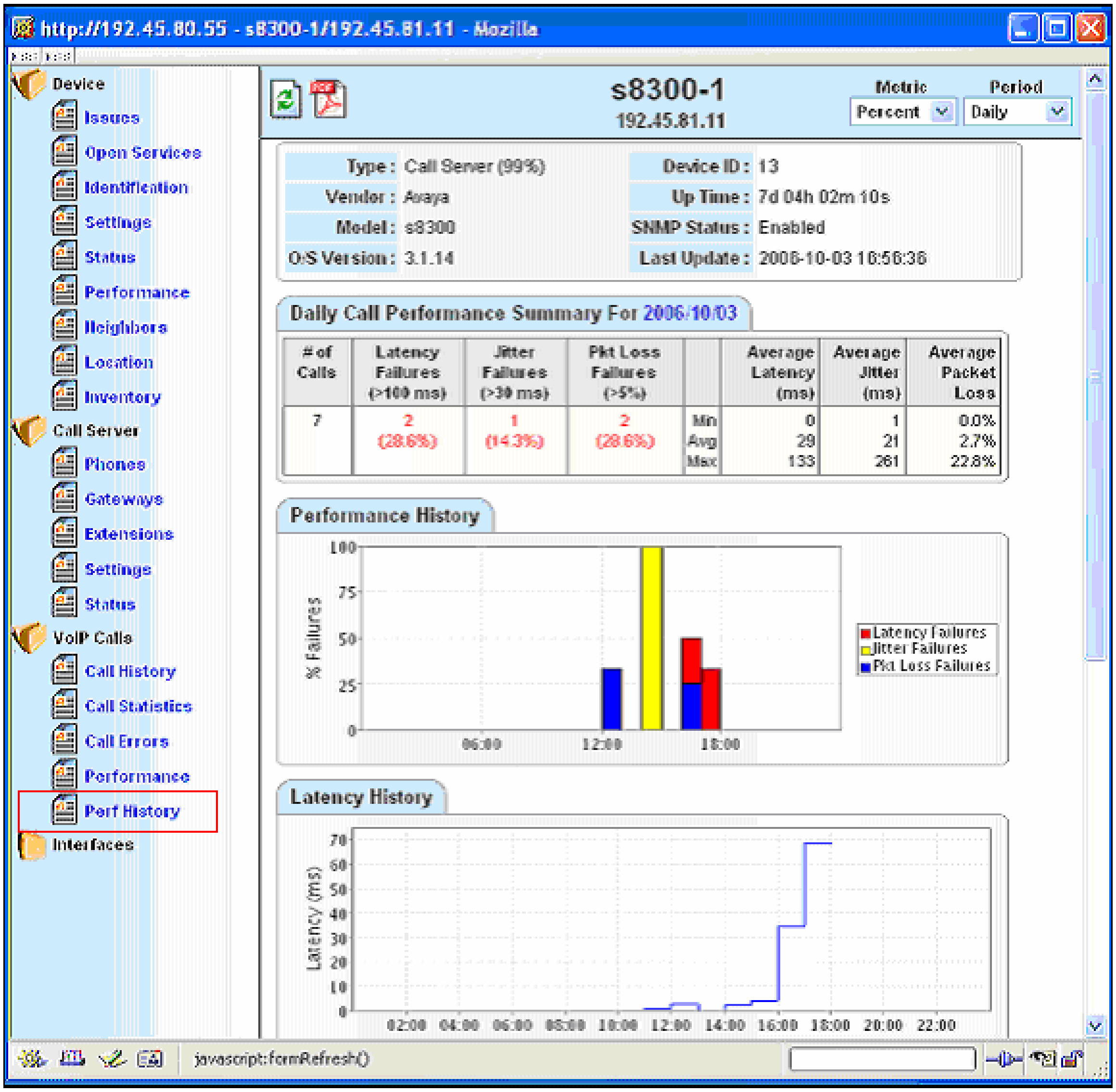
Model: S8300 SNMP Status: Enabled

O/S Version: 3.1.14 Last Update: 2006-10-03 16:56:36

Daily Call Performance Summary For 2006/10/03

# of Calls	Latency Failures (>100 ms)	Jitter Failures (>30 ms)	Pkt Loss Failures (>5%)		Average Latency (ms)	Average Jitter (ms)	Average Packet Loss
7	2 (28.6%)	1 (14.3%)	2 (28.6%)	Min Avg Max	0 29 133	1 21 261	0.0% 2.7% 22.8%

The next screen shows the “Perf History” page, which displays similar data as the Performance page. Instead of showing distribution charts, as in the Performance page, it displays latency, jitter, and packet loss charts over the selected date and time period. It may be possible to isolate network-wide problems to a specific time period using these charts.



s8300-1
192.45.81.11

Metric: Percent
Period: Daily

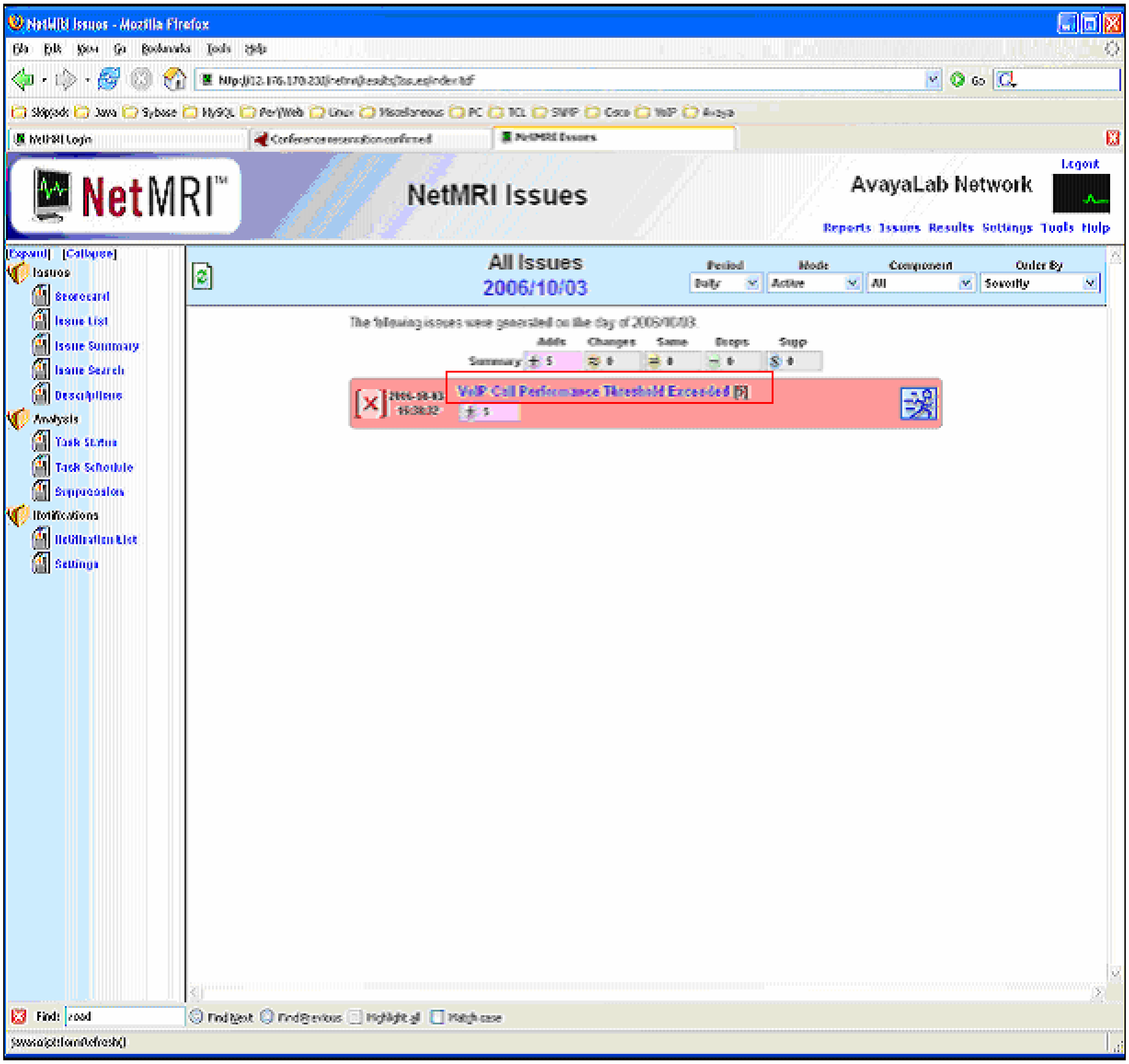
Type :	Call Server (99%)	Device ID :	13
Vendor :	Avaya	Up Time :	7d 04h 02m 10s
Model :	s8300	SNMP Status :	Enabled
O/S Version :	3.1.14	Last Update :	2006-10-03 16:56:36

Daily Call Performance Summary For 2006/10/03

# of Calls	Latency Failures (>100 ms)	Jitter Failures (>30 ms)	Pkt Loss Failures (>5%)		Average Latency (ms)	Average Jitter (ms)	Average Packet Loss
7	2 (28.6%)	1 (14.3%)	2 (28.6%)	Min Avg Max	0 29 133	1 21 261	0.0% 2.7% 22.8%

At the end of the testing, the NetMRI VoIP analysis task was executed. NetMRI automatically runs all analysis tasks once per day. To access the NetMRI Issues page, launch a web browser and connect to NetMRI by entering http://<NetMRI Lifecycle Manager IP address>. Supply a **Username** and **Password**, and click the **OK** button to access the NetMRI Issues page.

Click the **Issue List** link in the left pane of the window to view all issues. For the certification test, this specific task was executed at the end of the testing to show that the NetMRI Issue named VoIP Call Performance Threshold Exceeded issue was raised. This issue details all the endpoints that participated in a phone call with excessive latency, jitter, or packet loss during the analysis period. Click the issue, **VoIP Call Performance Threshold Exceeded**.



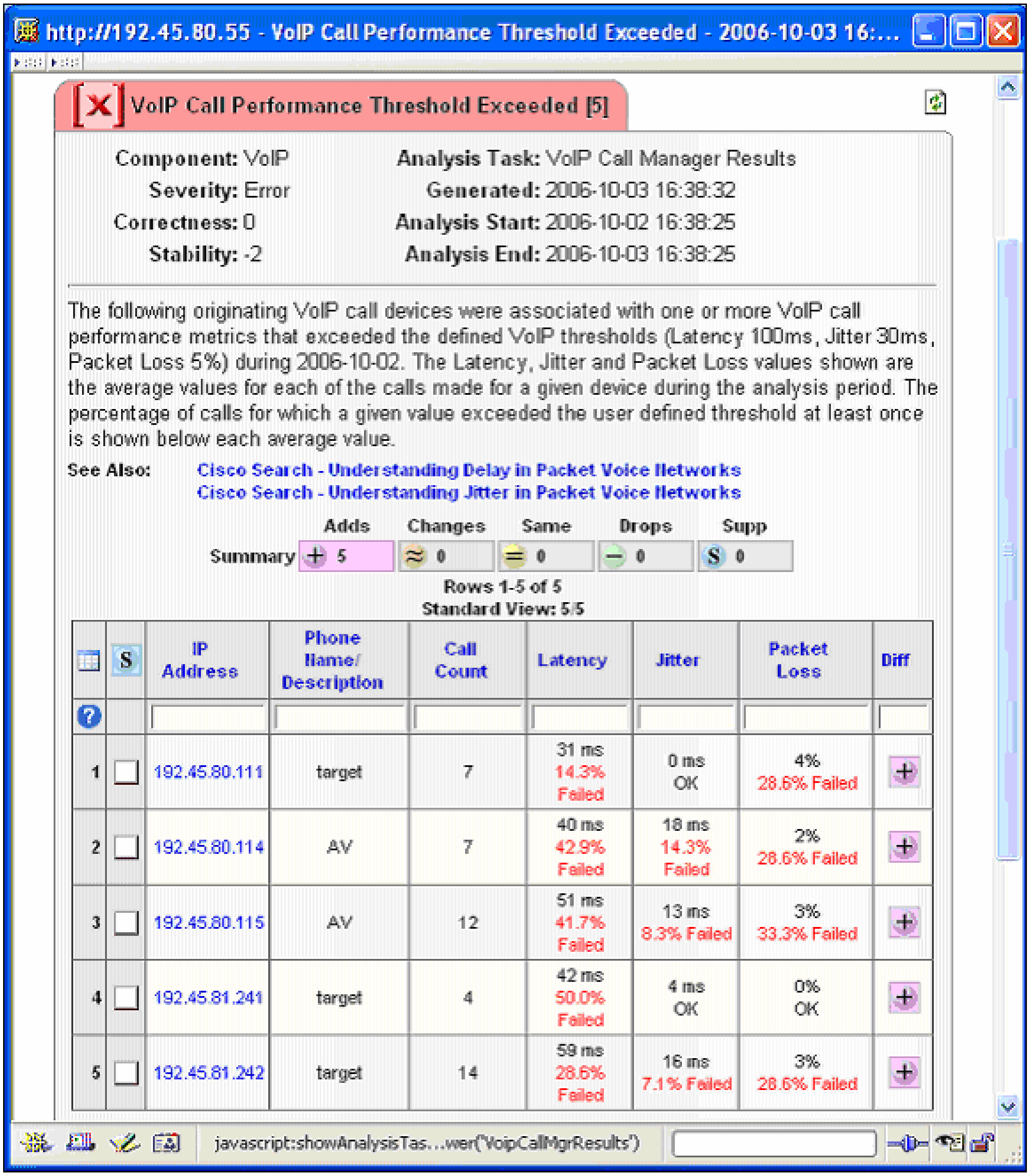
All Issues
2006/10/03

The following issues were generated on the day of 2006/10/03

	Adds	Changes	Same	Drops	Supp
Summary	5	0	0	0	0

2006-10-03 15:38:32 VoIP Call Performance Threshold Exceeded [5] + 5

The next screen shows the detailed information on the VoIP Call Performance Threshold Exceeded issue.



http://192.45.80.55 - VoIP Call Performance Threshold Exceeded - 2006-10-03 16:...

VoIP Call Performance Threshold Exceeded [5]

Component: VoIP
Severity: Error
Correctness: 0
Stability: -2

Analysis Task: VoIP Call Manager Results
Generated: 2006-10-03 16:38:32
Analysis Start: 2006-10-02 16:38:25
Analysis End: 2006-10-03 16:38:25

The following originating VoIP call devices were associated with one or more VoIP call performance metrics that exceeded the defined VoIP thresholds (Latency 100ms, Jitter 30ms, Packet Loss 5%) during 2006-10-02. The Latency, Jitter and Packet Loss values shown are the average values for each of the calls made for a given device during the analysis period. The percentage of calls for which a given value exceeded the user defined threshold at least once is shown below each average value.

See Also: Cisco Search - Understanding Delay in Packet Voice Networks
Cisco Search - Understanding Jitter in Packet Voice Networks

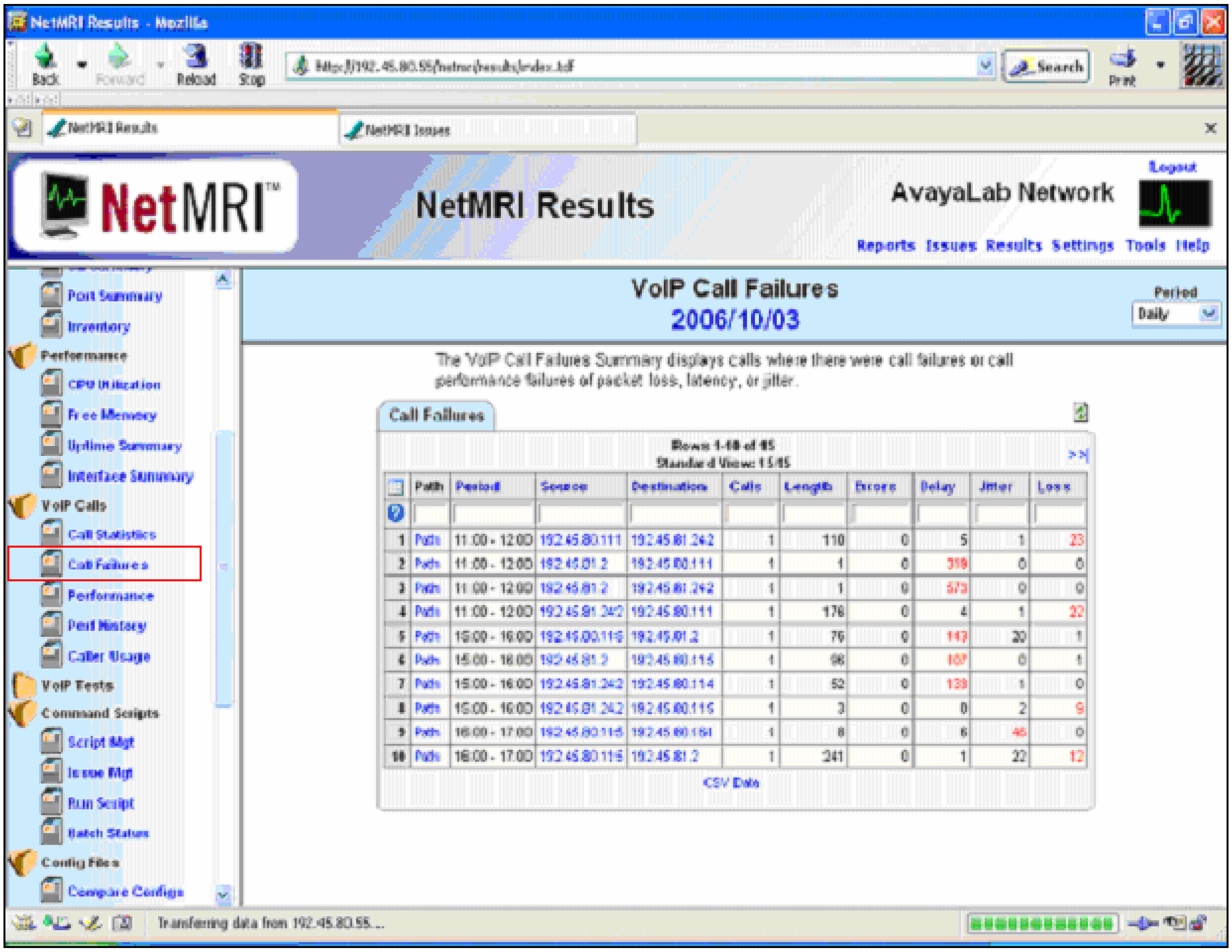
	Adds	Changes	Same	Drops	Supp
Summary	+ 5	≈ 0	= 0	− 0	S 0

Rows 1-5 of 5
Standard View: 5/5

	S	IP Address	Phone Name/ Description	Call Count	Latency	Jitter	Packet Loss	Diff
?								
1	□	192.45.80.111	target	7	31 ms 14.3% Failed	0 ms OK	4% 28.6% Failed	+
2	□	192.45.80.114	AV	7	40 ms 42.9% Failed	18 ms 14.3% Failed	2% 28.6% Failed	+
3	□	192.45.80.115	AV	12	51 ms 41.7% Failed	13 ms 8.3% Failed	3% 33.3% Failed	+
4	□	192.45.81.241	target	4	42 ms 50.0% Failed	4 ms OK	0% OK	+
5	□	192.45.81.242	target	14	59 ms 28.6% Failed	16 ms 7.1% Failed	3% 28.6% Failed	+

javascript:showAnalysisTas...wer('VoipCallMgrResults')

The following screen displays the “VoIP Call Failures” page, which shows all VoIP calls made across the entire network. This page can be accessed through navigating to the **Results → VoIP Calls → Call Failures** link. The Call Failures page displays any phone call made between two endpoints that resulted in some quality of service metric that exceeded the defined thresholds.



VoIP Call Failures

2006/10/03

The VoIP Call Failures Summary displays calls where there were call failures or call performance failures of packet loss, latency, or jitter.

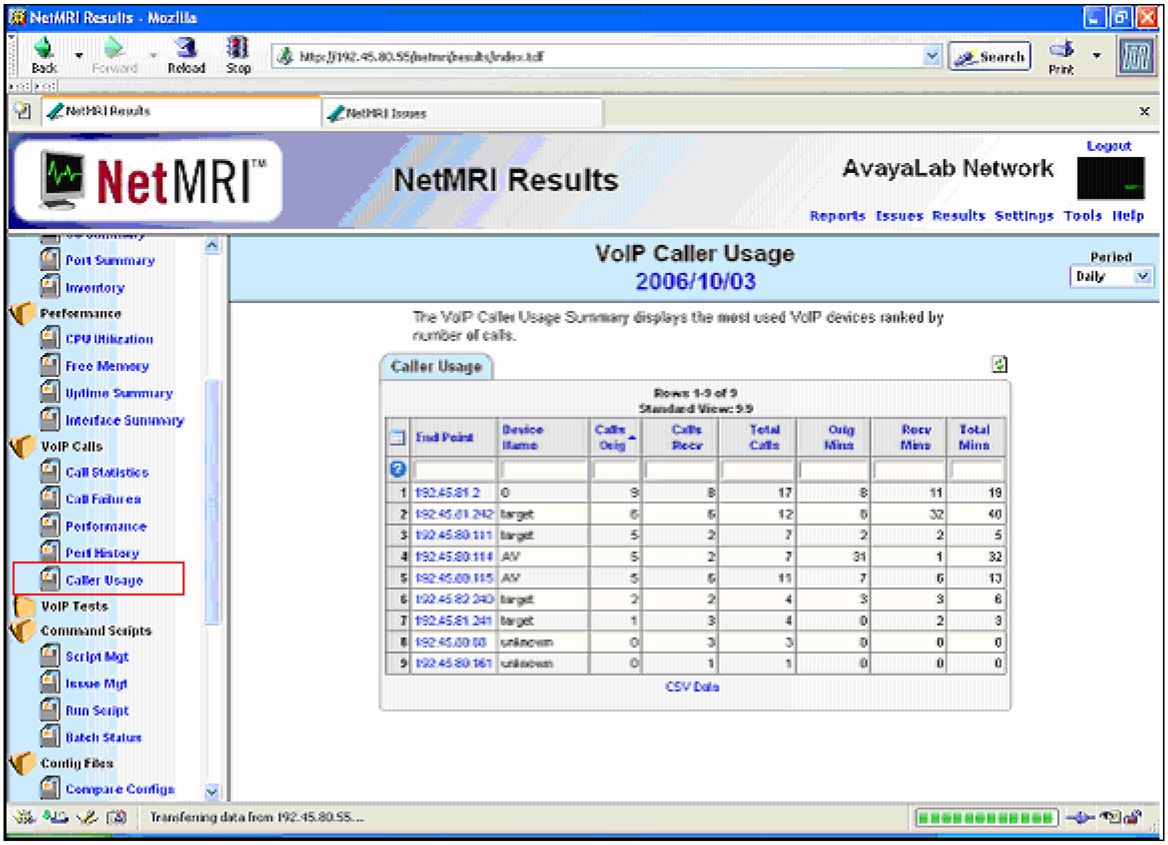
Call Failures

Rows 1-10 of 85
Standard View: 15/85

	Path	Period	Source	Destination	Calls	Length	Errors	Delay	Jitter	Loss
1	Path	11:00 - 12:00	192.45.80.111	192.45.81.242	1	110	0	5	1	23
2	Path	11:00 - 12:00	192.45.81.2	192.45.80.111	1	1	0	319	0	0
3	Path	11:00 - 12:00	192.45.81.2	192.45.81.242	1	1	0	573	0	0
4	Path	11:00 - 12:00	192.45.81.242	192.45.80.111	1	176	0	4	1	22
5	Path	15:00 - 16:00	192.45.80.115	192.45.81.2	1	76	0	147	20	1
6	Path	15:00 - 16:00	192.45.81.2	192.45.80.115	1	96	0	107	0	1
7	Path	15:00 - 16:00	192.45.81.242	192.45.80.114	1	52	0	133	1	0
8	Path	15:00 - 16:00	192.45.81.242	192.45.80.115	1	3	0	0	2	9
9	Path	16:00 - 17:00	192.45.80.115	192.45.80.161	1	8	0	6	46	0
10	Path	16:00 - 17:00	192.45.80.115	192.45.81.2	1	241	0	1	22	12

CSV Data

The “VoIP Caller Usage” page, shown below, displays similar information as the Call History page. This table displays, for each endpoint, the number of calls made and received, total calls, and the number of minutes of each.



VoIP Caller Usage

2006/10/03

The VoIP Caller Usage Summary displays the most used VoIP devices ranked by number of calls.

Rows 1-9 of 9
Standard View: 9.9

	End Point	Device Name	Calls Orig	Calls Recv	Total Calls	Orig Mins	Recv Mins	Total Mins
1	192.45.81.2	0	9	8	17	8	11	19
2	192.45.81.242	target	6	6	12	8	32	40
3	192.45.80.111	target	5	2	7	2	2	5
4	192.45.80.114	AV	5	2	7	31	1	32
5	192.45.80.115	AV	5	6	11	7	6	13
6	192.45.82.240	target	2	2	4	3	3	6
7	192.45.81.241	target	1	3	4	0	2	3
8	192.45.80.98	unknown	0	3	3	0	0	0
9	192.45.80.161	unknown	0	1	1	0	0	0

5. Interoperability Compliance Testing

The interoperability compliance testing included feature and serviceability testing. The feature testing evaluated the ability of NetMRI to provide quality of calls placed to and from stations. The serviceability testing introduced failure scenarios to see if NetMRI can resume monitoring and 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 NetMRI, 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, and conferenced calls. During the compliance test, a network impairment tool was utilized to simulate network delay and packet drop. For serviceability testing, failures such as cable pulls and resets were applied. Verification of each call was made by performing queries into the NetMRI data, and looking at the results recorded in NetMRI internal logs. At the end of the testing, a NetMRI analysis task was run to verify that NetMRI would report on phone calls, which exceeded one of the predefined quality of service metrics.

5.2. Test Results

NetMRI successfully provided VoIP call quality data on various types of calls discussed in Section 5.1. For serviceability testing, NetMRI was able to resume collecting VoIP call quality data after restoration of connectivity to the CLAN, and after resets of the NetMRI 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 NetMRI to all devices.
- Verify that calls can be successfully completed between the IP and Digital telephones.
- Compare VoIP quality data from the following sources:
    - Network impairment tool settings
    - The Avaya IP telephone's Network Audio Quality data
    - NetMRI

7. Support

Technical support for the NetMRI can be obtained by contacting NetCordia Support via the support link at http://www.netcordia.com/support/contact.shtml or by calling the support telephone number of 410-266-6161.

8. Conclusion

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

9. References

This section references the Avaya and NetCordia 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

NetCordia provided the following documentation. For additional product and company information, visit http://www.netcordia.com.

[3] NetMRI Users Guide: Release 1.5p4

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.