Avaya VoIP Monitoring Manager Reference

14-300614
Issue 1
June 2005

Table Of Contents

About VoIP Monitoring Manager

VoIP Monitoring Manager is a Voice over IP (VoIP) Quality of Service (QoS) monitoring tool. It enables you to monitor and review the quality of a call on an AVAYA™ VoIP network. Using the VoIP Monitoring Manager, you can view the Jitter, Round Trip Time (RTT) and Packet Loss experienced at the endpoints and during a session. The QoS data displays currently active endpoints or for endpoints active in the past. With this information, you can begin to troubleshoot and isolate problems.

If you are new to using the VoIP Monitoring Manager, the following information explains what you can do with this tool.

Search for Endpoints

You search endpoints active from some time in the past or within a date range. The Advanced Search options enable you to narrow your search to match phone numbers, SIP user names, network addresses, or QoS level.

View Reports

Once you have completed your search, you can view a summary or a detailed report. The reports display the QoS data for selected endpoints. This is particularly useful for monitoring Gateways or locating problems at a particular endpoint. You can also view a report for endpoints involved in a session. This will assist with determining problems that occur between two endpoints or in an isolated area of the network.

Generate Automatic Alarms

You can generate SNMP Traps/Alarms , which enables the VoIP Monitoring Manager to alert you when the Jitter, Round Trip Time or Packet Loss reaches certain levels. This assists you to routinely monitor the network, and troubleshoot problems.

See Also

Components of VoIP Monitoring Manager

Starting VoIP Monitoring Manager

How to Use VoIP Monitoring Manager Client

About Licenses

About VoIP Monitoring Manager Client

The VoIP Monitoring Manager (VMM) Client provides the graphical user interface (GUI) for VoIP Monitoring Manager. The VMM Client does not communicate with the VMM RTCP Monitor and does not use SNMP. The data that is displayed is gathered from the VoIP Monitoring Manager (VMM) Server.

The VMM Client may be installed on the same machine as the VMM Server, or it may be installed on another machine on the network. It is possible for the VMM Server and the VMM Client to communicate over a dial-up connection.

See Also

Components of VoIP Monitoring Manager

Starting the VoIP Monitoring Manager

How to Use VoIP Monitoring Manager Client

About VoIP Monitoring Manager Web Client

The VoIP Monitoring Manager (VMM) Client can run as a web application in a browser. This is useful if you only have the VMM Server installed.

The VMM Server needs to be running a web server. If you purchased Avaya Integrated Management, the Apache web server will already be installed and running. If you choose to run the Apache web server, the VMM installation will assist with configuration. The machine running the VMM Web Client needs to have the Sun Java Plug-in installed to run the Web Client.

Configure the web server to publish the file to the following default install path:

C:\Program Files\Avaya\VoIP Monitoring Manager\jars\ClientApplet.htm

If you run the web client you will not have access to all the functionality available in the application. This includes features such as copy and connect to a new server. For more information see Starting VoIP Monitoring Manager Web Client.

See Also

Components of VoIP Monitoring Manager

Starting the VoIP Monitoring Manager Web Client

Web Client Displaying Incorrect Time

About VoIP Monitoring Manager Server

The VoIP Monitoring Manager Server acts as a proxy between the VoIP Monitoring Manager Client and the VoIP Monitoring Manager RTCP Monitor. The main purpose of the VoIP Monitoring Manager Server is to reduce the amount of traffic to the VoIP Monitoring Manager Client by performing large data downloads and extensive processing of the MIB data stored on the RTCP Monitor. The VoIP Monitoring Manager Server can reside on the same PC as the RTCP Monitor.

See Also

Components of VoIP Monitoring Manager

Starting the VoIP Monitoring Manager

Components of VoIP Monitoring Manager

The VoIP Monitoring Manager (VMM) application comprises the VMM RTCP Monitor and the VMM Server, which accepts connections from the VMM Client. If you only have the VMM Server installed, you can run VMM Client as a web client.

To ensure it will run correctly, you will need to have configured the Switch Administration Forms, have a Windows SNMP Agent installed on the Server and the Monitoring Manager Server needs to be installed onto the network.

The components and their relationship are described in more detail in the following links:

- VoIP Monitoring Manager Server
- VoIP Monitoring Manager RTCP Monitor
- VoIP Monitoring Manager Client
- VoIP Monitoring Manager Web Client
- Database

See Also

About VoIP Monitoring Manager

Starting VoIP Monitoring Manager

How to Use VoIP Monitoring Manager Client

Configure the Avaya Communication Manager IP-Network Region Form

Configure the Avaya Communication Manager System-Parameters IP-Options Form

About Licenses

VoIP Monitoring Manager requires licenses that you must purchase from Avaya. You can purchase these licenses in sets of 2000 phone endpoints and 40 media gateways. The Avaya licenses are managed by the WebLM server, which is provided with VoIP Monitoring Manager.

By selecting **Help>About** in the VMM Server or the VMM Client, you can view the following information:

- the number of licenses purchased
- the number of phones at the local server. This number represents the phones that reported to VMM in the last 28 days. This number will increase if you move phones (for example, change extensions or IP addresses). In this case, these phones appear to be new endpoints to VMM. Since there is a 30-day grace period, this will not be a problem.
- the number of phones at the local server that exceed the license (that is, the number of phones that are unlicensed). If greater than zero, this number is displayed in red. This can occur if you have only one monitor connected to the WebLM License Server, and you have more phones stored in the database than licenses purchased.
- the number of media gateways at the local server. This number represents the media gateways that reported to VMM in the last 28 days.
- the number of media gateways at the local server that exceed the license (that is, the number of media gateways that are unlicensed). If greater than zero, this number is displayed in red. This can occur if you have only one monitor connected to the WebLM License Server, and you have more media gateways stored in the database than licenses purchased.

Each VMM RTCP monitor periodically checks the number of endpoints it knows about and requests/renews the licenses for them. If there is more than one RTCP monitor and the total number of endpoints known exceeds the number of licenses, the RTCP monitor that requests licenses first will get its licenses. The RTCP monitor that requests licenses last will be denied licenses. If you enter the 30-day grace period because license limits were exceeded, the About dialog box will appear every time the VMM Server and VMM Client are started. If you exceed the 30-day grace period, VoIP Monitoring Manager stops collecting RTCP data.

Avaya provides a 90-day trial version of VoIP Monitoring Manager. After 90 days, VoIP Monitoring Manager stops collecting RTCP data. You have the option of purchasing the VoIP Monitoring Manager license key from Avaya to fully activate the VoIP Monitoring Manager beyond the 90-day trial period. When a license key is purchased, an instance of WebLM License Server is required to manage the license key.

Contact your authorized Avaya Sales Representative to purchase additional VMM licenses.

Help

Most screens and tasks in VoIP Monitoring Manager have matching topics in this help. You can go directly to the matching topic by clicking the Help button shown on the screen or dialog.

If the topic displayed does not show the required information, you can open the entire help at any time.

To open the Help Contents, select **Help** > **Contents**.

To open the Help File, click on this icon on the **Tool Bar** or **Help** > **Contents**.

What's this help

The What's this? button located on the Tool Bar enables you find out what a **Tool Bar** or button is in the application. You click on the **What's this?** button as shown above and then click the object. The help will open explaining that particular object.

Context-sensitive help

If you click the help button on a form, help about that form (or its uses) is displayed.

About menu

You access the About menu from **Help > About**. The About dialog shows the version number for the VoIP Monitoring Manager (VMM) Client. This is useful to ensure that you are using the same version number for the VMM Client as the VMM Server.

Send us feedback!

To send us feedback or to suggest any improvements about this Online Help, send an email to performance@avaya.com

Support Details

If you require further support details check the Avaya web site located at www.avaya.com for the most recent information. From the main page, navigate to the support page and search for VoIP Monitoring Manager.

Installation Checklist

Installation Checklist

The VoIP Monitoring Manager Server (VMM Server) needs to be installed on the VoIP network. Before you install the software, you need to configure the Switch Administration Forms.

1. Configure Switch Administrator forms

   You need to configure the System-Parameters IP-Options Form and the IP-Network-Region Form to send RTCP reports to the RTCP Monitor.

2. Make one port 1099

   The VMM Client and Server communicate using Java Remote Method Invocation (RMI), and uses port 1099 as its default port on the machine running the VMM server. If port 1099 is not available, another port must be made available.

3. Check for Windows SNMP Agent

   The SNMP Agent must be installed for the VoIP Monitoring Manager Server to function. You can check if the Windows SNMP Agent has been configured to run at startup automatically. The installation also checks to see if the Windows SNMP Agent is installed.

   If the Windows SNMP Agent is not installed, the **Add/Remove Windows Components** starts automatically and you are be prompted for the Windows 2000 CD location to install the Windows SNMP Agent.

4. Check for a valid SNMP Community ID

   You must set an ID with the correct privileges.

5. Configure SNMP agent for sending traps

   Although SNMP is installed and running, it dies not send the required traps until you configure it.

6. Download VoIP Monitoring Manager or Install from CD

   If you are downloading the program from a web site, select to **Run this program from its current location** and the installation program starts automatically. Alternatively, you can select to save the file to disk, which may be the faster option. Once saved to your hard drive, double-click the saved program's name to start the install. If you are installing the program from a CD-ROM, insert the CD into your drive and follow the instructions.

7. Connect to a database

   When you first install VoIP Monitoring Manager, you need to connect Server to a database.

> Solving Installations Problems: If you are experiencing difficulties running the application after installation the following checks may assist you:
>
> - Check Windows SNMP Agent is Running
> - Check for a Valid Community ID

See Also

About VoIP Monitoring Manager

Components of VoIP Monitoring Manager

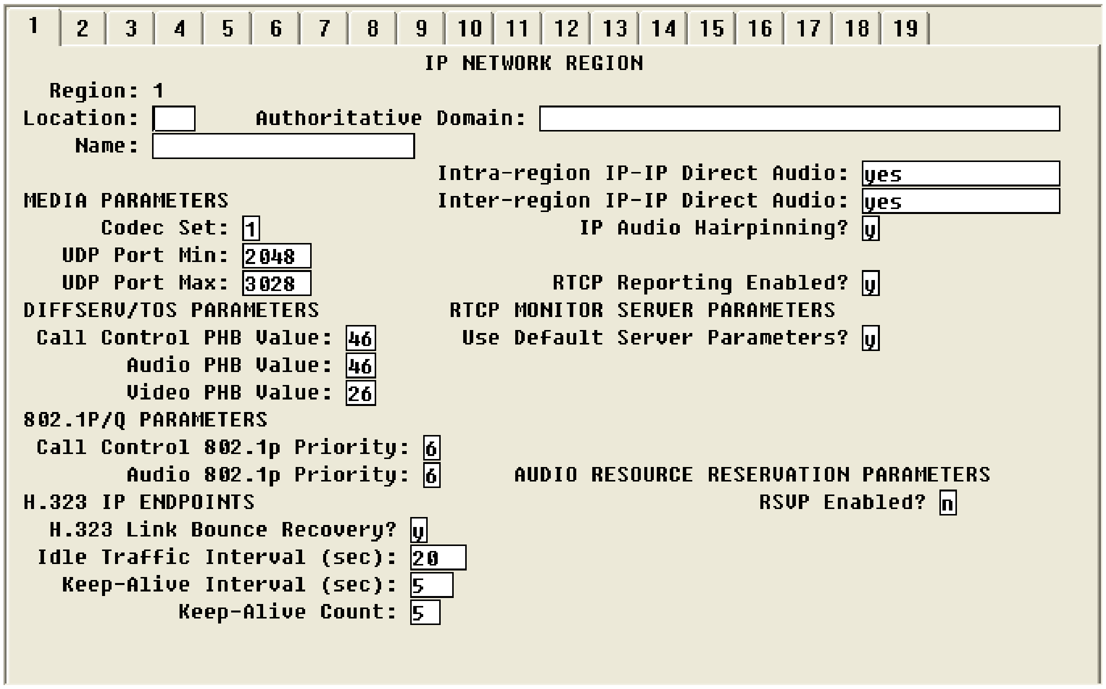
VoIP Monitoring Manager Server Error Messages

Configure IP-Network-Region form

There are two Switch Administration Forms (SAT) that need to be configured to send RTCP reports to the RTCP Monitor. These forms are called the ip-network-region form and the system-parameters ip-options form.

Configuration for the ip-network-region form

- Set the **RTCP Reporting Enabled?** field to **y** (yes).
- Set **Use Default Server Parameters?** field to **y** (yes). This indicates that this network region uses the default values specified previously on the system-parameters-ip-options form as well.



```
                                     IP NETWORK REGION
   Region: 1
 Location:          Authoritative Domain:
     Name:
                                   Intra-region IP-IP Direct Audio: yes
MEDIA PARAMETERS                   Inter-region IP-IP Direct Audio: yes
      Codec Set: 1                            IP Audio Hairpinning? y
   UDP Port Min: 2048
   UDP Port Max: 3028                       RTCP Reporting Enabled? y
DIFFSERV/TOS PARAMETERS             RTCP MONITOR SERVER PARAMETERS
 Call Control PHB Value: 46          Use Default Server Parameters? y
        Audio PHB Value: 46
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                       RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
           Keep-Alive Count: 5
```

Why you might not want to use the default parameters?

Multiple VoIP Monitoring Manager Servers might be installed on a large system in order to reduce the network traffic between a set of endpoints and the RTCP Monitor (e.g. low bandwidth link between endpoints in one network region and a remote RTCP Monitor). The network traffic due to RTCP reports being sent from the endpoints to the RTCP Monitor is usually low, less than 40 bytes per second per currently active VoIP call (RTP session). Therefore, it is usually unnecessary to have multiple RTCP Monitors.

If multiple VoIP Monitoring Manager Servers are installed on the system then the endpoints in each network region can be configured to send their RTCP reports to different RTCP Monitors.

To achieve this set the **Use Default Server Parameters?** field to **n (no)** and specify the IP address of the Windows 2000 PC running the VoIP Monitoring Manager Server for that network region.

See Also

Troubleshooting

No Endpoints Matched the Search

Components of VoIP Monitoring Manager

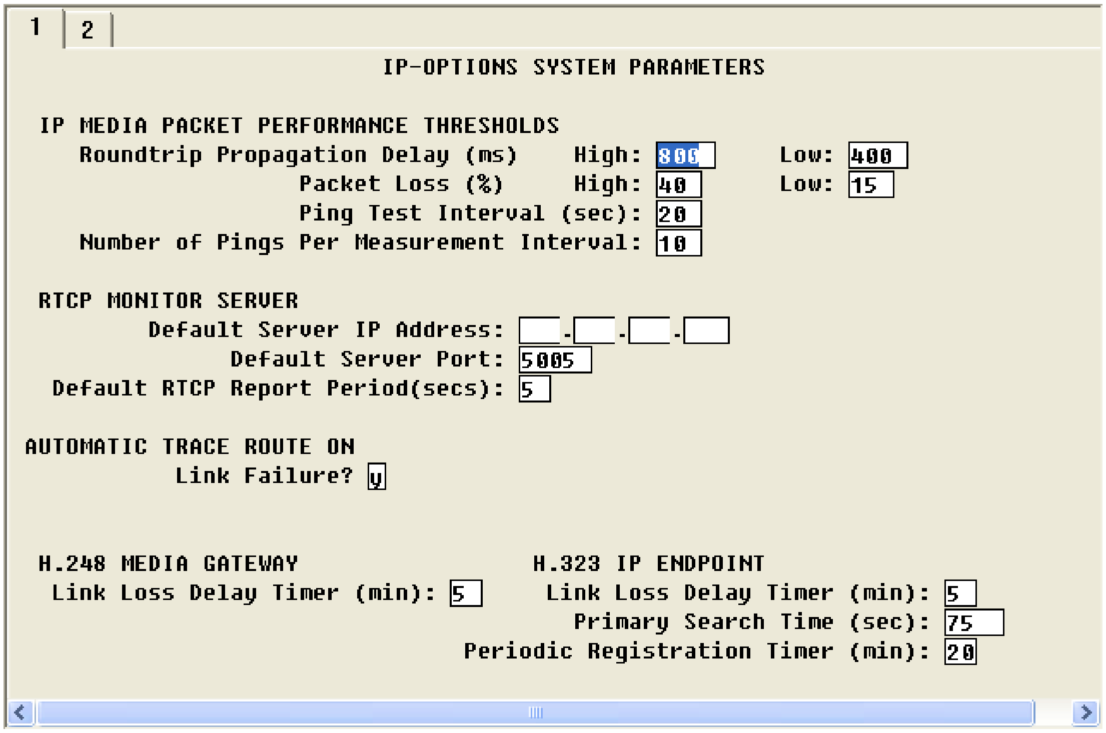
Configure System Parameters IP Options Forms

Configure System-Parameters IP-Options Form

There are two Switch Administration Forms (SAT) that need to be configured to send RTCP reports to the RTCP Monitor. These forms are called the system-parameters ip-options form (as shown below) and the ip-network-region form.

Configuration for the system-parameters ip-options form

- Set the RTCP MONITOR SERVER, Default Server IP Address to the address of the Windows 2000 PC running the VoIP Monitoring Manager Server.



```
                             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:    .   .   .
               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
```

See Also

Troubleshooting

No Endpoints Matched the Search

Components of VoIP Monitoring Manager

Configure IP-Network-Region Form

Make one port available

The VMM client and server communicate using Java Remote Method Invocation (RMI), and uses the port 1099 on the machine on which the VMM server is running.

If this port is not available, the VMM server will attempt to use the following ports: 49177, 51173, or 63006. Although it is unlikely that all of these ports will be in use on a single machine, please ensure that at least one of these ports is available.

Check Windows SNMP Agent is Installed and Running

The Windows SNMP Agent must be installed before you install the VoIP Monitoring Manager Server. You are prompted during the VoIP Monitoring Manager install to install it from the Windows 2000 CD. If the Windows SNMP Agent is not installed or not running, you will experience problems receiving data.

Check if Windows SNMP Agent is Installed and Running

1. Select **Start > Settings > Control Panel > Administrative Tools > Services**.
2. Scroll down until you see the words **SNMP Service.** It should have a status as **Started** and Startup Type as **Automatic**. If it is not included in the list you will need to install it from the Windows 2000 CD.
3. If it is listed but not set to run automatically, you will need to change its properties as follows:
4. Right-click on SNMP and select **Properties** from the context menu. The SNMP Service Properties dialog opens.
5. Select **Automatic** from the **Startup Type** drop down list.
6. Click **OK**.

See Also

Check for a Valid Community ID

Troubleshooting

Components of VoIP Monitoring Manager

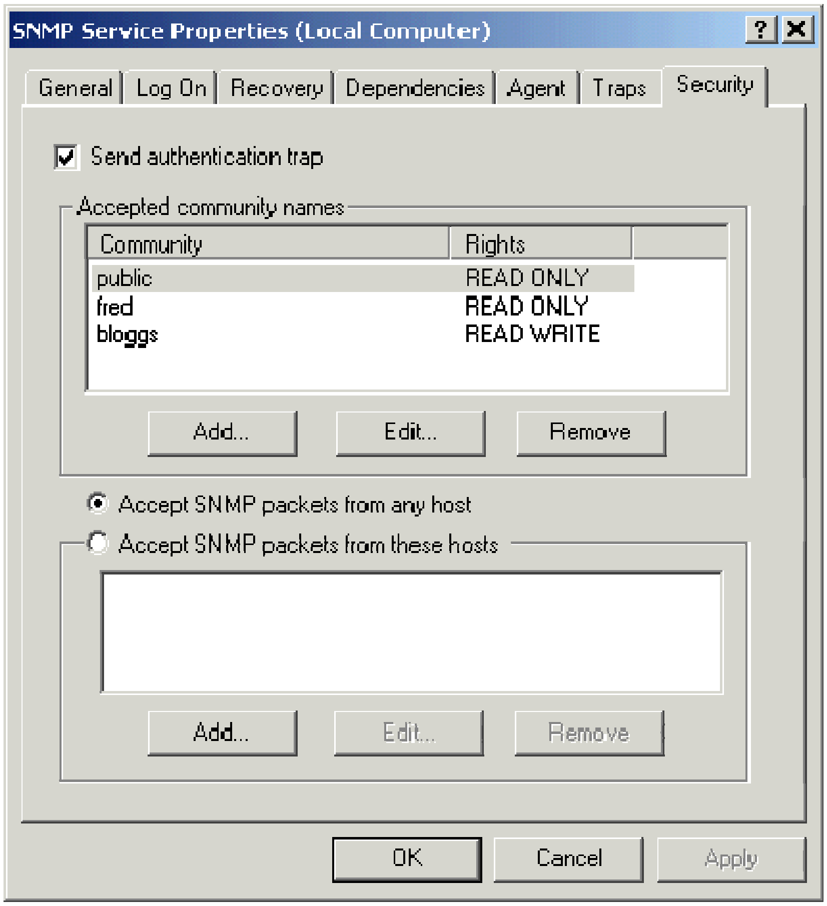
Check for a Valid SNMP Community ID

The Community ID for your Windows SNMP Agent must match the Community ID defined in the VoIP Monitoring Manager Options. By default it is public but it may have been changed.

You cannot complete this procedure unless you have already checked that Windows SNMP is installed and running.

To Check for a Valid Community ID

1. Click **Start > Settings > Control Panel > Administrative Tools > Services**.
2. Scroll down and select the **SNMP Service**.
3. Right-click on SNMP Service and select **Properties** from the context menu.
4. Select the **Security** tab. The VoIP Monitoring Manager Options must have a Community ID from the list of Community Names.



☑ Send authentication trap

Community	Rights
public	READ ONLY
fred	READ ONLY
bloggs	READ WRITE

● Accept SNMP packets from any host

○ Accept SNMP packets from these hosts

5. Add a public ID with Read and Write privileges (if one does not already exist), or is not available for use by VoIP Monitoring Manager

6. Click **OK**.

See Also

VoIP Monitoring Manager Options

Components of VoIP Monitoring Manager

Configure SNMP Service For Sending Traps

To send Traps you need to configure the SNMP Service.

To Configure Windows SNMP Agent for Sending Traps

1. Click **Start > Settings > Control Panel > Administrative Tools > Services**.
2. Scroll down and select the SNMP Service.
3. Right-click on SNMP Service and select **Properties** from the context menu.
4. Select the **Traps** tab.
5. Type the community name that is configured on the network management system where trap messages will be sent and click **Add** to list.
6. In the Trap destinations area, click **Add**. The SNMP Service Configuration dialog displays.
7. In the **SNMP Service Configuration** dialog, type the IP Address of the network management system you want the traps to be sent and click **Add**. The dialog closes.
8. From the SNMP Service Properties dialog, click **OK**.

If the changes do not take effect immediately, you may have to restart the SNMP Service. To restart either Service, right-click on it and select **Restart** from the context menu.

See Also

Generating Traps & Alarms

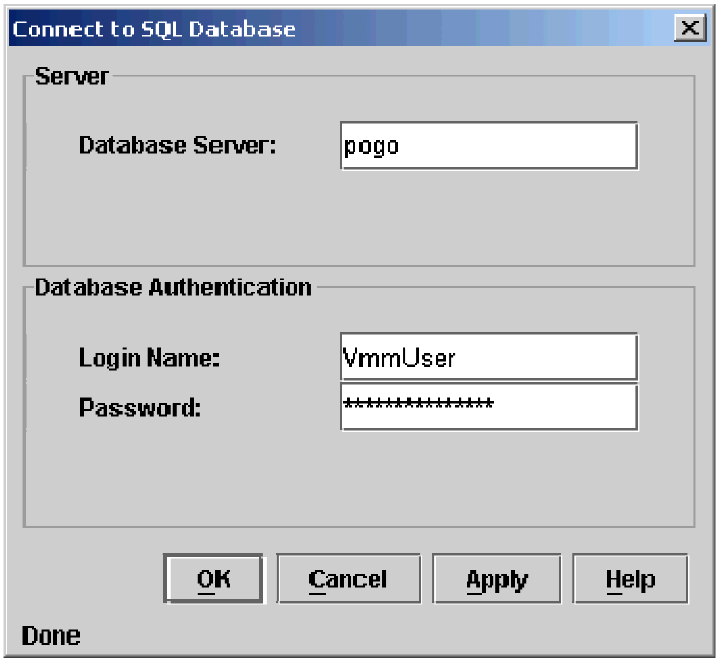
Connect to Database

When VoIP Monitoring Manager is first installed, you need to connect it to the database. You also need to perform this task if you decide to change to a different database (for example you upgrade to a SQL Server database from the standard MSDE database). This is explained in Migrate Data.

> This setting is for both reading of monitor data, and writing of RTCP data.

To connect to a database:

1. From the VoIP Monitoring Manager server interface, select **File > Connect to Database**.



Database Server: pogo

Login Name: VmmUser

Password: ***************

Done

2. Enter the Database Server name, Logon Name, and Password.

   The database server name can be either a name or an IP address. In either case, it must be accessible on your network.

3. Click **OK**.

See Also

Unable to establish database connection (error message)

Manage your licenses

You must log into the WebLM server that manages your Avaya licenses. The license server is required to activate VoIP Monitoring Manager beyond the 90-trial period. If you do not have a license to use VoIP Monitoring Manager, you can use the software for a 90-day trial period.

See Also

About Licenses

Connecting to the License Server

Customized Setup

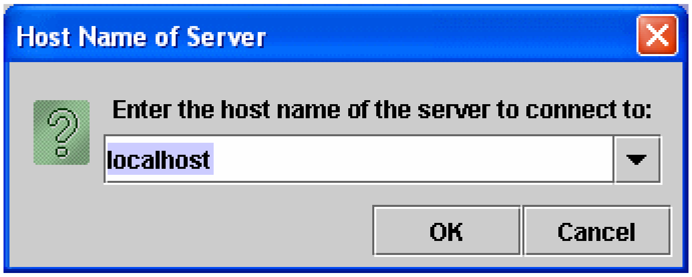
Customized Setup

You only need to use these procedures if you are changing the default installation such as creating your own database.

Change Monitoring Manager Server

To change the VoIP Monitoring Manager Server that the VoIP Monitoring Manager Client is communicating with:

1. Select **File > Connect to New Server.** The Host Name Server dialog box appears.
2. Enter the name of the new VoIP Monitoring Manager Server and click **OK**.


Host Name of Server

Enter the host name of the server to connect to:

localhost

If you are using the VoIP Monitoring Manager Client from a browser, you will be unable to change the server that the Client is receiving information from. The monitor that is displaying the Client must be directly connected to the Server that is running the VoIP Monitoring Manager Server.

See Also

Connect to New Server

Configure Database Tables

You do not need to configure the database tables as part of a normal installation—this happens automatically. You only need to configure the database tables if you initially use the default MSDE database, but then decide to migrate to an SQL Server database.

See also

Migrate data

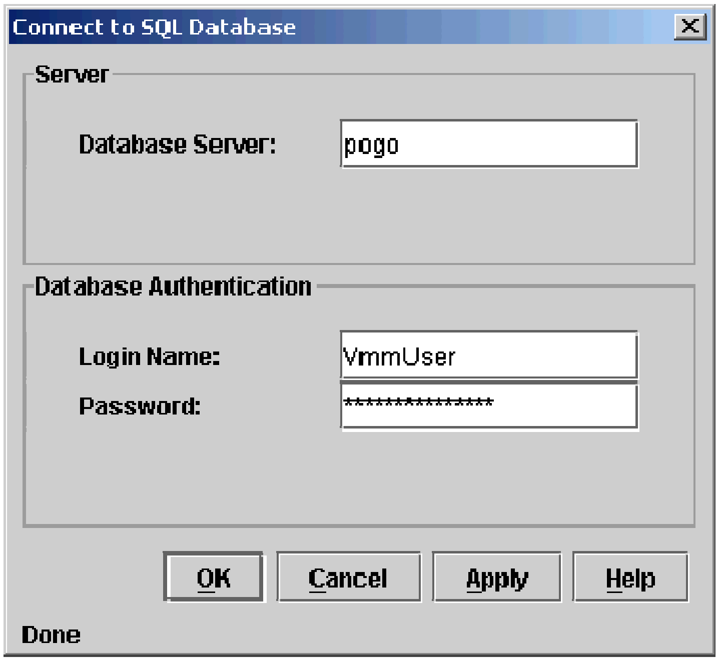
Migrate Data

Use this procedure if you want to migrate VoIP Monitoring Data from the standard MSDE database to a SQL Server database. Reasons for performing this migration include:

- Database content needs to exceed 2GB.
- You want access to improved management and reporting tools available in SQL Server.
- You want the remote administration capabilities of SQL Server.
- You regularly need a connection pool of more than five connections.

To migrate data:

1. Install SQL Server.
2. Set up the VMM database:
    - Copy *SetupNewVmmDatabase.zip* to the MS SQL Server machine. (This zip can be found in the VMM installation\SQL folder.)
    - Extract the zip file and follow the instructions in the extracted *readme.txt* file.
3. Create a backup of the existing MSDE database.
4. Using the standard SQL Server tools, restore the backed-up database as a new SQL Server database. (Alternatively, use the script provided: <*VMM installation directory*>*sql**RestoreVmmDatabase.bat*.)
5. Start Avaya VoIP Monitoring Manager Server.
6. Select **File > Connect to Database**.



Connect to SQL Database

Server

Database Server: pogo

Database Authentication

Login Name: VmmUser

Password: ***************

7. Enter the Database Server name, Logon Name, and Password. (Note the default VMM login/password created by the setup scripts is **VmmUser/VmmUserPassword**.)

8. Click **OK**.

The AVAYA VoIP Monitoring Manager Server shows progress of the connection. When both Server Status and SNMP Agent Status bars at 100%, the connection has been successful.

For security reasons, you must change the VmmUser password. Run the batch file *ChangeVmmUserPassword.bat*, which is included in the zip, to change the password associated with the VmmUser SQL login. Then, reconfigure the VMM Server with the new password.

See Also

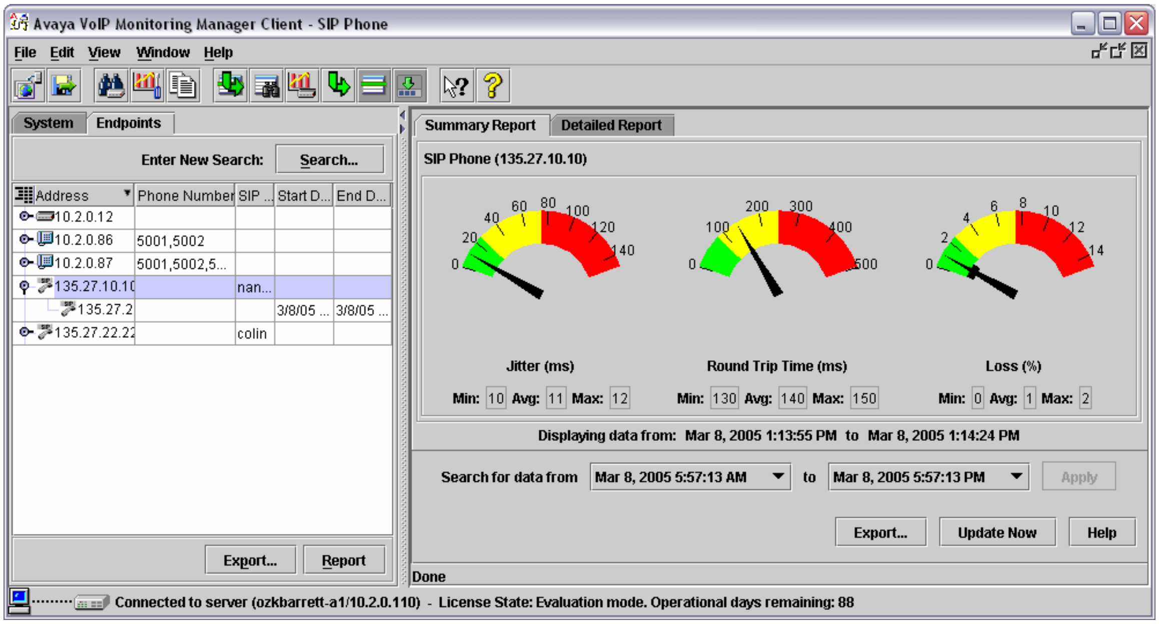
Database Schema

Entity Relationship Diagram

Overview of VoIP Monitoring Manager Client

VoIP Monitoring Manager Client

The following image displays an example of the VoIP Monitoring Manager Client in use. A search has been completed and a Summary Report is displaying ready for analysis. To familiarize yourself with the environment such as its tools and menus, click on it in the image below.



Enter New Search:

Address	Phone Number	SIP ...	Start D...	End D...
10.2.0.12				
10.2.0.86	5001,5002			
10.2.0.87	5001,5002,5...			
135.27.10.10		nan...		
135.27.2			3/8/05 ...	3/8/05 ...
135.27.22.22		colin		

SIP Phone (135.27.10.10)

Jitter (ms)	Round Trip Time (ms)	Loss (%)
Min: 10 Avg: 11 Max: 12	Min: 130 Avg: 140 Max: 150	Min: 0 Avg: 1 Max: 2

Displaying data from: Mar 8, 2005 1:13:55 PM to Mar 8, 2005 1:14:24 PM

Search for data from Mar 8, 2005 5:57:13 AM to Mar 8, 2005 5:57:13 PM

Done

Connected to server (ozkbarrett-a1/10.2.0.110) - License State: Evaluation mode. Operational days remaining: 88

See Also

How to Use VoIP Monitoring Manager Client

About the System Pane

About the Endpoints Pane

About Summary Reports

About Detailed Reports

System Pane

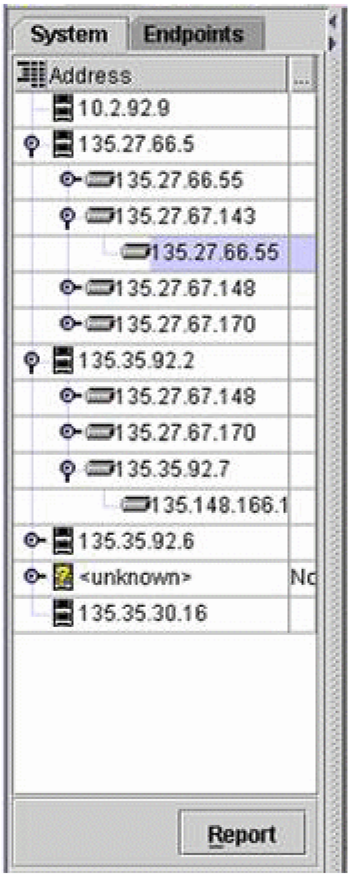
The System pane is populated based on the media gateways that have reported to the VMM server in the last hour (or specified time period).

> Data for the System Pane is only obtained over the last hour because this uses an expensive query if the database is large. If your system has a small database, you may want to increase this "look back" time. To increase the "look back" time, you must change the value of the **SystemViewSearchInterval** attribute in the ***VoIPMonMgrClient.ini*** file. The ***VoIPMonMgrClient.ini*** file is located in the VMM installation directory. Note that the value of the **SystemViewSearchInterval** attribute is in hours.

For each object, the System displays the following information (if available):

- Name (if you configured friendly names for gateways)
- IP address

The following image shows a sample System pane.



```
Address
  10.2.92.9
  135.27.66.5
    135.27.66.55
    135.27.67.143
      135.27.66.55
    135.27.67.148
    135.27.67.170
  135.35.92.2
    135.27.67.148
    135.27.67.170
    135.35.92.7
      135.148.166.1
  135.35.92.6
  <unknown>                 Nc
  135.35.30.16
```

The System pane may contain the following icons:

Gatekeeper

Unknown Gatekeeper

Gateway

From the System pane, you can select a gateway and click the **Report** button to view an aggregated report of all the VoIP sessions over the selected link.

See Also

Summary Media Gateway Link Report

Detailed Media Gateway Link Report

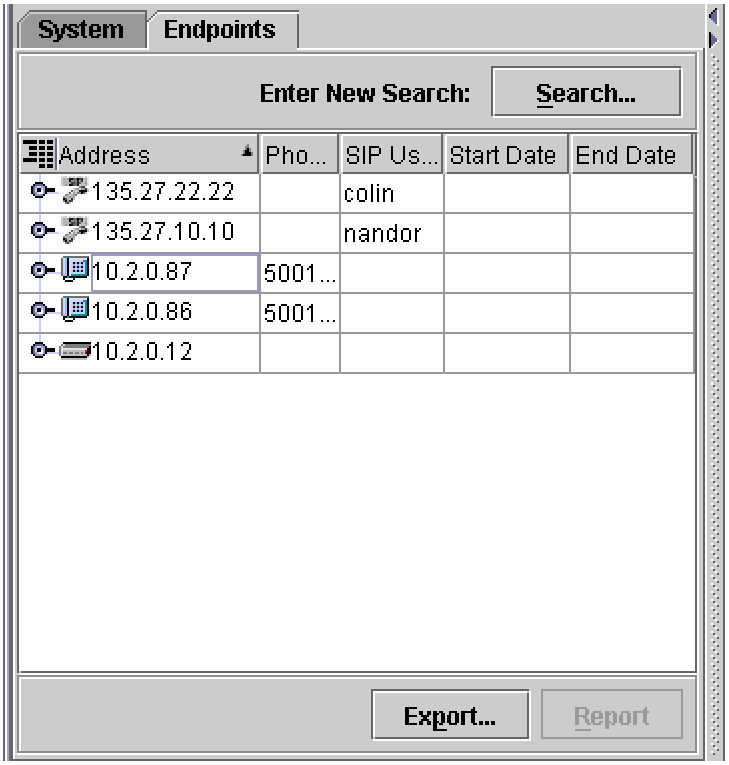
Trace Routes Media Gateway Link Report

Endpoints Pane

The Endpoints pane displays:

- the list of active endpoints
- the list of endpoints that are the result of a **Search** you performed

The following image shows a sample Endpoints pane.



Address	Pho...	SIP Us...	Start Date	End Date
135.27.22.22		colin		
135.27.10.10		nandor		
10.2.0.87	5001...			
10.2.0.86	5001...			
10.2.0.12				

The Endpoints pane may contain the following icons:

Gateway

IP Phone

Avaya IP Softphone

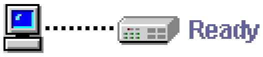
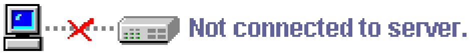
SIP Phone

See Also

VoIP Monitoring Manager Client

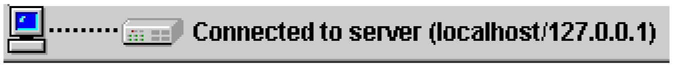
Connection Status

When you start the VoIP Monitoring Manager Client, it attempts to connect to the VoIP Monitoring Manager Server. The results of this connection are displayed in the Status Bar. Some of the possible connection icons are as follows:

 Ready	The VoIP Monitoring Manager Client is connected to the VoIP Monitoring Manager Server.
 Not connected to server.	The VoIP Monitoring Manager Client is not connected to the VoIP Monitoring Manager Server.

Display in Status Bar

When you connect to a new VoIP Monitoring Manager Server, a message displays in the status bar as shown below.



Connected to server (localhost/127.0.0.1)

See Also

How to Use VoIP Monitoring Manager Client

Components of VoIP Monitoring Manager

Status Bar

The Status Bar is the area of space at the bottom of the VoIP Monitoring Manager Client showing the Connection Status. You toggle the display of the Status bar either by clicking on its icon on the Tool Bar or select/deselect the checkbox in the **View** menu.

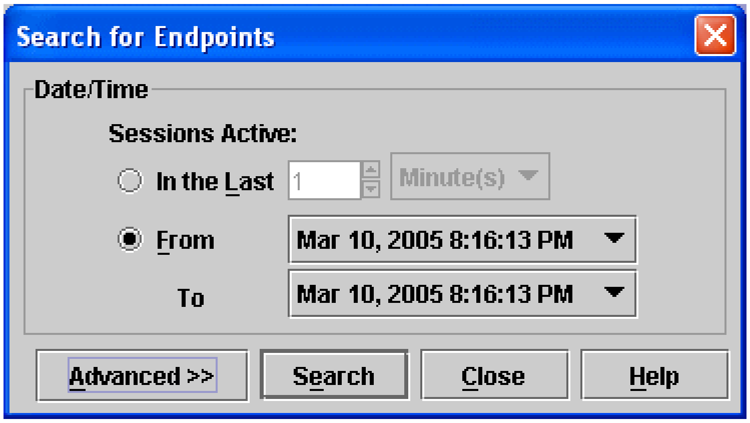
See Also

VoIP Monitoring Manager Client

Search Dialog

The Search dialog is where you set your search criteria for gathering endpoints. You access the dialog from the Search button on the Endpoints tab or **Edit > Search**. A search is based on the time period for the active endpoints. This could be endpoints that were active in the last minute, hour, day or month or were active between a date range.

You can use the **Advanced Search** to run a search for a specific phone number, SIP username, network address, or based on a QoS value. Once you have entered the details, you click the **Search** button. A Search updates the Results List with the endpoints. Then you can select an endpoint and view the report.



Search for Endpoints

Date/Time

Sessions Active:

○ In the Last 1 Minute(s)

● From Mar 10, 2005 8:16:13 PM

To Mar 10, 2005 8:16:13 PM

See Also

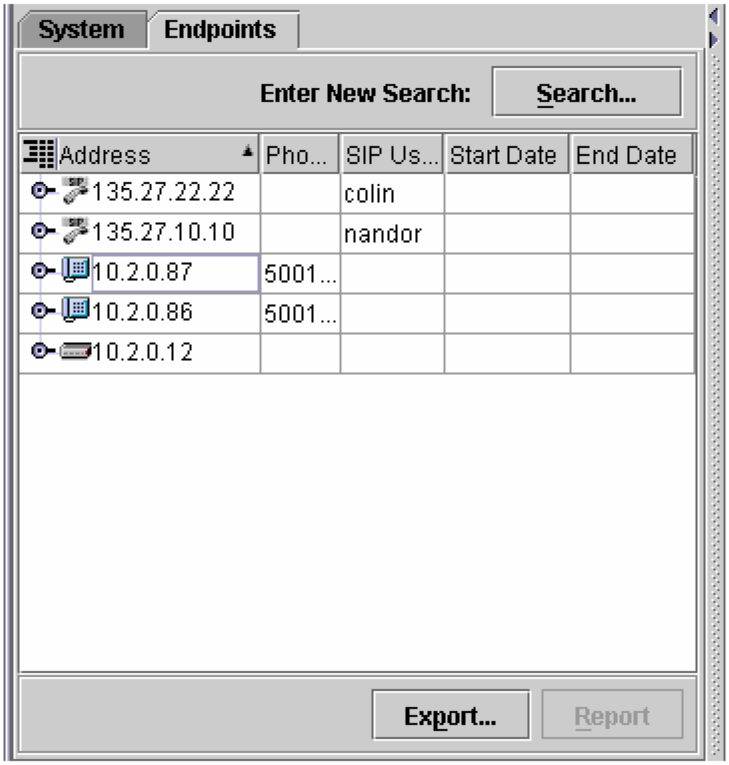
Advanced Search

Run a Search

View a Report

Results List

The Results List shown in this image displays a list of endpoints that are a result of the **Search**. You can toggle the display of the Results List by unchecking the option from **View > Results**. You can also use shrink and expand the pane, by pointing your mouse at the right side edge and drag the edge to the desired size.



Address	Pho...	SIP Us...	Start Date	End Date
135.27.22.22		colin		
135.27.10.10		nandor		
10.2.0.87	5001...			
10.2.0.86	5001...			
10.2.0.12				

The Results window may contain the following icons:

Gateway

IP phone

Avaya IP Softphone

Avaya SIP Softphone

See Also

VoIP Monitoring Manager Client

View Tool Bar

You can toggle the display of the **Tool Bar** in the VoIP Monitoring Manager Client. Hiding the Tool Bar provides you with more screen space. Toggle this option by de/selecting the **Tool Bar** option from the **View Menu**.

See Also

VoIP Monitoring Manager Client

Search Button

To access the **Search** dialog, click on the **Search button** on the Results List or the **Search** icon on the **Tool Bar**. Alternatively, select **Edit > Search.** This opens the Search dialog so that you can run a search for endpoints based on a time period. You can also use the Advanced Search options to narrow your search to match phone number, SIP username, network address and/ or QoS level.

See Also

Run a Search

Getting Started Guide (Client)

Starting VoIP Monitoring Manager

You need to ensure that the VoIP Monitoring Manager (VMM) Server is installed and running on the network before you start the VMM Client. If you only have the VMM Server installed, you can also start the VMM Client as a Web Client.

VoIP Monitoring Manager Server cannot be run unless a database is installed and configured properly.

To Start VoIP Monitoring Manager as an Application

1. From the machine with the VoIP Monitoring Manager Server, select **Start > Programs > Avaya > VoIP Monitoring Manager > Server**. The VoIP Monitoring Manager Server starts.

2. From the machine with the VoIP Monitoring Manager Client, select **Start > Programs > Avaya > VoIP Monitoring Manager > Client**. The VoIP Monitoring Manager Client starts.

Now you can search for endpoints and then view the QoS data in a report format.

> ℹ If the VoIP Monitoring Manager Server has difficulty connecting to the Windows SNMP Agent, check the Windows SNMP Agent is installed and running.

See Also

Connect to Database

Run a Search

View a Report

How to Use VoIP Monitoring Manager Client

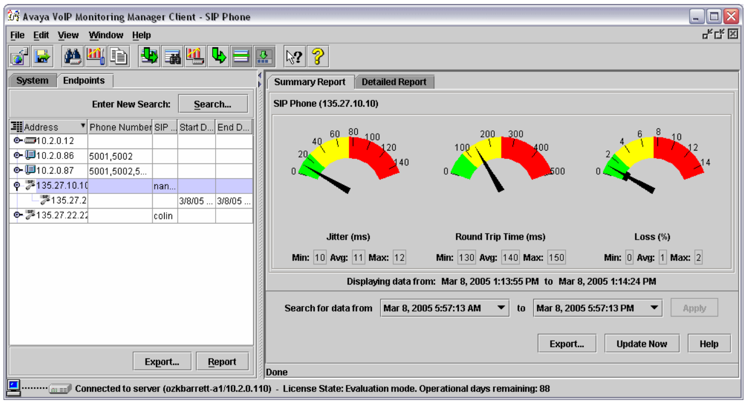
About Detailed Reports and Summary Reports

Interpreting the Values Using Detailed Reports and Summary Reports

How to Use VoIP Monitoring Manager Client

To use the VoIP Monitoring Manager, you must start the VoIP Monitoring Manager Server, before you start the Client. Then you can begin to search for endpoints, view reports and begin your analysis.

If you want to become familiar with the application's tools and menus, click on the image below. If you are new to VoIP Monitoring Manager but have a specific task in mind, these links will help you get started:



Address	Phone Number	SIP ...	Start D...	End D...
10.2.0.12				
10.2.0.86	5001,5002			
10.2.0.87	5001,5002,5...			
135.27.10.10		nan...		
135.27.2			3/8/05 ...	3/8/05 ...
135.27.22.22		colin		

SIP Phone (135.27.10.10)

Jitter (ms) Min: 10 Avg: 11 Max: 12

Round Trip Time (ms) Min: 130 Avg: 140 Max: 150

Loss (%) Min: 0 Avg: 1 Max: 2

Displaying data from: Mar 8, 2005 1:13:55 PM to Mar 8, 2005 1:14:24 PM

Search for data from Mar 8, 2005 5:57:13 AM to Mar 8, 2005 5:57:13 PM

Done

Connected to server (ozkbarrett-a1/10.2.0.110) - License State: Evaluation mode. Operational days remaining: 88

- Run a Search
- View a Report
- Interpreting the Values Using Summary Reports
- Interpreting the Values Using Detailed Reports

See Also

About VoIP Monitoring Manager

Components of VoIP Monitoring Manager

About Detailed Reports and Summary Reports

Interpreting the Values Using Detailed Reports

Starting VoIP Monitoring Manager Web Client

The Avaya VoIP Monitoring Manager Client can run as a Web application in a browser. This is useful if you only have the server installed. To run the Avaya VoIP Monitoring Manager Client as a Web application, the following requirements must be met:

- The PC on which the Avaya VoIP Monitoring Manager Server software is installed must be running a Web server. The Apache Web server is automatically installed on the server when the Avaya VoIP Monitoring Manager Server software is installed.
- The Web server must be configured to publish the file to the following VoIP Monitoring Manager installation path:
  C:\Program Files\Avaya\VoIP Monitoring Manager\jars\ClientApplet.htm
- The PC you will use to access the Avaya VoIP Montoring Manager Server must be able to connect to the VMM server via a Web browser and have the following software installed:
  - Microsoft Internet Explorer 6 or later
  - SUN Java 2 Runtime Environment, SE v1.4.2_06

For more information see the topic About the VoIP Monitoring Manager Web Client

To Start Web Client

- From your browser, type in the following url:

  ```
  Http://VMMServerMachineName/VoIPMonMgr/ClientApplet.html
  ```

  VMMServerMachineName = the machine running the VMM Server. This url points to the machine running the VMM Server.

  If you do not have the Sun Java Plug-in installed, you are prompted to install it.

  To exit the Web Client, just close the browser.

> There are limitations in using the VMM Web Client. These are imposed by the security restrictions associated with running unsigned applets. The limitations are:
>
> - You can only access one monitor that is directly connected to the server running the VMM Server.
> - You cannot connect to a new server or use the Copy functionality.

See Also

Components of VoIP Monitoring Manager

Web Client Displays an Incorrect Time

Run a Search

The first action required when using the VoIP Monitoring Manager Client is to search for endpoints. You can search endpoints active from a point in time into the past or between a date range. You can also use the Advanced Search options to narrow the search based on phone number, SIP username, network addresses, or QoS value. Once you have completed your search, the Results List updates with a list of endpoints where you select the endpoint from to view a report.

To Run a Search

1. Perform one of the following steps:

   - Select **Edit > Search**.
   - Click **Search** on the Endpoints pane.

   The Search dialog appears.

2. From the **Search** dialog, click the drop down arrow to select the time period for active endpoints. The default is 1 minute but you can select hours, days weeks or months.

3. If you want to select a date range of active endpoints, click **From** and click the calendar(s) drop down arrow to open the calendar.

4. From the calendars, select the **start** (from) and **end date** (to) of the range. You can select hours, minutes, seconds and AM/PM. You can also use the arrow buttons to scroll through the months and years.

5. Click **Search**. The Results List updates with a list of endpoints. Now, you can select an endpoint and view its report.

See Also

Advanced Search

How to Use VoIP Monitoring Manager Client

About Detailed Reports and Summary Reports

Interpreting the Values Using Detailed Reports and Summary Reports

View a Report

You can generate reports for endpoints and media gateways.

Endpoint Reports

After you run a search, you can view the report on selected endpoints and endpoints involved in a session. There are two types of reports: Summary Reports and Detailed Reports.

To View the QoS Data for an Endpoint

1. From the **Results List,** select an **endpoint** or click the expanding icon and select a child endpoint that was in a session with the parent endpoint. The Report button become available.

2. Click **Report**. The Report dialog opens.

Media Gateway Link Reports

From the System pane, you can select a media gateway and click the **Report** button to view an aggregated report of all the VoIP sessions over the selected link. There are three types of reports: Summary Media Gateway Link Report, Detailed Media Gateway Link Report, and Trace Routes Media Gateway Link Report.

See Also

How to Use VoIP Monitoring Manager Client

About Detailed Reports and Summary Reports

Interpreting the Values Using Detailed Reports and Summary Reports

How to... (Client)

Connect to New Server

The Connect to New Server option enables you to change the server that the VoIP Monitoring Manager Client is connecting to, so that you can analyze endpoints that are reporting to a different server. This option is not available when using the VoIP Monitoring Manager Web Client.

To Change the VoIP Monitoring Manager Server

1. Select **File > Connect to a New Server.** The Host Name Server dialog opens.
2. From the Host Name Server dialog, type in the VoIP Monitoring Manager Server's name.
3. Click **OK** to save the changes. The Connection in Progress dialog displays. The VoIP Monitoring Manager Client starts connecting to the VoIP Monitoring Manager Server.

When the connection is made the Connection Status will display the network as being **Ready**. If the connection to the VoIP Monitoring Manager Server is unsuccessful, you will be prompted to check if the VoIP Monitoring Manager Server is available and to try again.

See Also

Components of VoIP Monitoring Manager

Troubleshooting

Error Messages

Run a Search

The first action required when using the VoIP Monitoring Manager Client is to search for endpoints. You can search endpoints active from a point in time into the past or between a date range. You can also use the Advanced Search options to narrow the search based on phone number, SIP username, network addresses, or QoS value. Once you have completed your search, the Results List updates with a list of endpoints where you select the endpoint from to view a report.

To Run a Search

1. Perform one of the following steps:
   - Select **Edit > Search**.
   - Click **Search** on the Endpoints pane.

   The Search dialog appears.
2. From the **Search** dialog, click the drop down arrow to select the time period for active endpoints. The default is 1 minute but you can select hours, days weeks or months.
3. If you want to select a date range of active endpoints, click **From** and click the calendar(s) drop down arrow to open the calendar.
4. From the calendars, select the **start** (from) and **end date** (to) of the range. You can select hours, minutes, seconds and AM/PM. You can also use the arrow buttons to scroll through the months and years.
5. Click **Search**. The Results List updates with a list of endpoints. Now, you can select an endpoint and view its report.

See Also

Advanced Search

How to Use VoIP Monitoring Manager Client

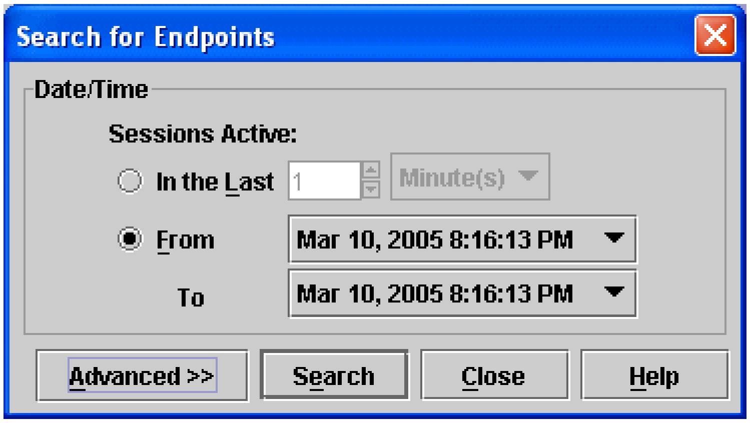
About Detailed Reports and Summary Reports

Interpreting the Values Using Detailed Reports and Summary Reports

Search Dialog

The Search dialog is where you set your search criteria for gathering endpoints. You access the dialog from the Search button on the Endpoints tab or **Edit > Search**. A search is based on the time period for the active endpoints. This could be endpoints that were active in the last minute, hour, day or month or were active between a date range.

You can use the **Advanced Search** to run a search for a specific phone number, SIP username, network address, or based on a QoS value. Once you have entered the details, you click the **Search** button. A Search updates the Results List with the endpoints. Then you can select an endpoint and view the report.


Search for Endpoints
Date/Time
Sessions Active:
○ In the Last 1 Minute(s)
● From Mar 10, 2005 8:16:13 PM
To Mar 10, 2005 8:16:13 PM
Advanced >>
Search
Close
Help

See Also

Advanced Search

Run a Search

View a Report

Advanced Search

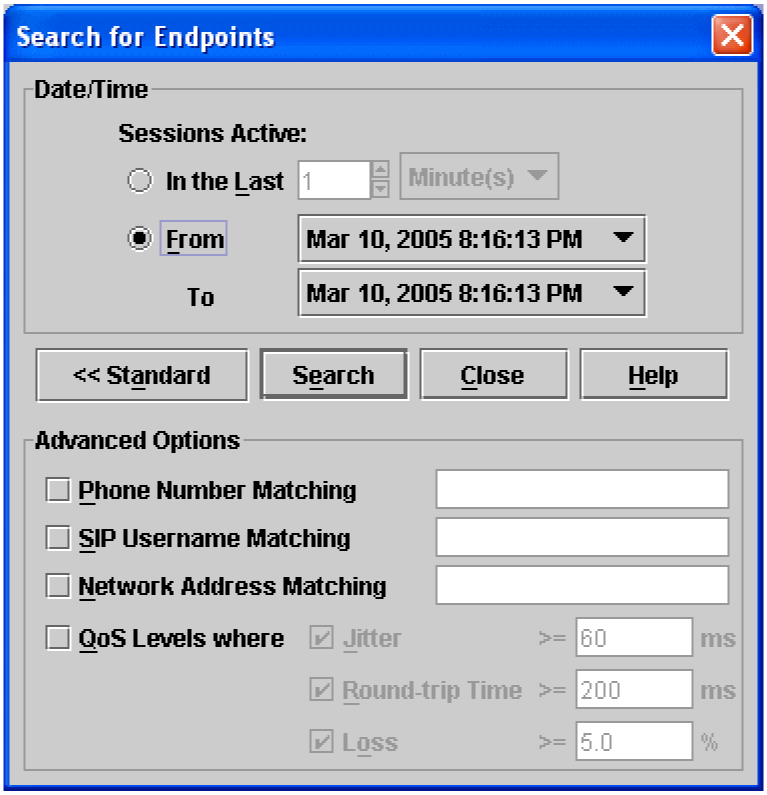
The Advanced Search enables you to search for endpoints matching a phone number, SIP username, network address, or QoS value. You can select one or more of the options and you can enter in more than one phone number or network address.

To Run an Advanced Search

1. From the **Search dialog**, click **Advanced Search**. If the Search dialog is not visible on the screen, click **Search** to display the Search dialog.

2. Check one or more of the checkboxes and/or type a value in the fields. If more than one item is selected the results returned will match all the parameters set. (E.g. Jitter > 300 and RTT > 350 for a specified phone number)

3. Click the **Search** button. The Results List updates.



Search for Endpoints

Date/Time

Sessions Active:

○ In the Last 1 Minute(s)

● From Mar 10, 2005 8:16:13 PM

To Mar 10, 2005 8:16:13 PM

Advanced Options

□ Phone Number Matching

□ SIP Username Matching

□ Network Address Matching

□ QoS Levels where ☑ Jitter >= 60 ms

☑ Round-trip Time >= 200 ms

☑ Loss >= 5.0 %

See Also

Search for a Specific Phone Number

Search for a Specific SIP Username

Search for a Specific Network Address

Search Using QoS Values

Search for a Specific Network Address

You can specify in your search to display endpoints that match an IP Address or hostname by entering the address or hostname in the Advanced Search options. This is useful for narrowing your search to a limited number of results displaying in the Results List.

You can enter:

- A range of IP addresses such as 123.4.122.122 – 123.4.122.225.
- A list of addresses that are separated by commas such as 123.4.102.120, 223.4.122.122, belibot.mycomputer.com.
- A part of the IP address, you can use an asterisk (*) as a substitution. For example; if you enter 123.*.*.225, it will find all addresses that start with 123 and end with 225 such as 123.4.122.225 and 123.4.190.225.
- A part of the name such as *belibot* for *belibot.mycomputer.com*. However, in this situation the search will only find hostnames in the same domain.

See Also

Advanced Search

Search for a Specific Phone Number

Search for a Specific SIP Username

Search Using Quality of Service (QoS) Values

Search for a Specific Phone Number

You can specify in your search to display endpoints that match a specific phone number by entering in the phone number in the Advanced Search options. This is useful for narrowing your search to a limited number of results displaying in the Results List.

You can:

- Enter commas to separate numbers e.g. **9835, 9872**. If you include spaces between numbers, VoIP Monitoring Manager will remove them. So, if you enter **9835, 9822 9872**, VoIP Monitoring Manager will remove the space between **9822** and **9872** and then search for **9835** and **98229872**.
- Use dashes to specify a range of phone numbers e.g. **2000 – 8000**.
- Enter a question mark (?) or asterisk (*) as a wild card. It is useful for substituting numbers in your search. The question mark can be used multiple times. However, each ? substitutes for exactly one character. An asterisk (*) substitutes for 0 or more characters. Wild cards cannot be used in ranges.

Example Wild Card Searches

- ?345 = Finds all extensions that are four digits long and end with 345. (? substitutes for exactly one character.)
- 9??? = Finds all the extensions from 9000 – 9999.
- 9* = Finds all the extensions that start with 9.

See Also

Advanced Search

Search for a Specific Network Address

Search for a Specific SIP Username

Search Using Quality of Service (QoS) Values

Search for a Specific SIP Username

You can specify in your search to display endpoints that match a specific SIP username by entering the SIP username in the Advanced Search options. This is useful for narrowing your search to a limited number of results displaying in the Results List.

You can:

- Enter a question mark (?) or asterisk (*) as a wild card. It is useful for substituting characters in your search. The question mark can be used multiple times. However, each ? substitutes for exactly one character. An asterisk (*) substitutes for 0 or more characters. Wild cards cannot be used in ranges.

Example Wild Card Search

- B??? = Finds all the SIP usernames that consist of four characters and begin with the letter B.
- B* = Finds all the SIP usernames that start with the letter B.

See Also

Advanced Search

Search for a Specific Network Address

Search for a Specific Phone Number

Search Using Quality of Service (QoS) Values

Search Using Quality of Service (QoS) Values

You can specify in your search to display endpoints that have QoS values greater than a given threshold by using the Advanced Search options. The Results List will only display those endpoints that contain the QoS data you have specified. This is useful for narrowing your search to a limited number of results that you will need to analyze.

The default ranges are as follows:

•□□□Jitter	Greater than 60 ms
•□□□Round Trip Time	Greater than 200 ms
•□□□Packet Loss	Greater than 5%

See Also

Advanced Search

Search for a Specific Phone Number

Search for a Specific Network Address

View Results List

The Results List displays the results of your search. You can toggle the display of the Results List. Hiding the Results List creates more space so that it is easier to see the reports. You toggle the display of the Results List either by clicking on this icon on the **Tool Bar** or select/deselect the checkbox in the **View** menu.

See Also

VoIP Monitoring Manager Client

Search Dialog

Export Result List

You can export the data in the results list to a comma separated value (csv) file.

The exported data contains records for every endpoint and every session that is displayed in VoIP Monitoring Manager. Opening or closing session folders (to show or hide the endpoints) does not affect the data that is exported.

You can open this file in most database and spreadsheet programs such as Microsoft Excel. Exporting the data to a spreadsheet enables you to manipulate the data so you can create your own reports. Click this link to see an example (Adobe Acrobat 5 or later required – the page has been split into three because of its width). You can use the sorting, counting and calculation features of Microsoft Excel to create your own reports from this raw data.

The data exported is divided into 3 tables:

- Session Table
- Time-varying Data Table
- Trace Route Table

To Export Data from the Result List

1. **File** > **Export Result List** or click the **Export** button located at the bottom of the **Result List**. A Save dialog opens.

   > **Tip:** If you want to limit the data that is exported, narrow down your search so that less data displays in the Result List.

2. Navigate to a folder.
3. In the **File name:** field, type a name for the file.
4. Click **Save as**. The file saves with the CSV extension.
5. From Microsoft Excel, open the file. From here you can build your own report.

> Microsoft Excel can only handle 65,536 rows of data. If your exported data file contains more rows, you will need to write a script that splits the data into smaller files before you import the data into Excel.

See Also

Export Report Data

Creating Reports with Export Data

Some Fields Are Blank in the Exported Data

Creating Reports with Exported Data

You can export the data from the Result List and/or Report dialogs to Microsoft Excel. Using Microsoft Excel you can create your own reports as shown in the linked example. This report was created by using Microsoft Excel's calculation features. It includes averaging results, counting the number of sessions, and unique participants and setting filters to determine the longest sessions, creating a line graph to visually demonstrate the information. You can create your own reports from the exported data—click this link to see and example (Adobe Acrobat reader is required).

See Also

Export Results List

Export Report Data

Some Fields Are Blank in the Exported Data

View Active Endpoints

You can view all active endpoints by clicking on this icon on the **Tool Bar** or selecting this option from the **View Menu**. The **Results List** is updated with all currently active endpoints.

See Also

VoIP Monitoring Manager Client

View Status Bar

The Status Bar is the gray bar at the bottom of the VoIP Monitoring Manager Client. It provides information on the current status such as the connection status to the VoIP Monitoring Manager Server. You toggle the display of the Status bar by clicking on this icon on the **Tool Bar** or select/deselect the checkbox on the **View** menu.

See Also

Connection Status

Update System View

To update information displayed on the System pane, click **Update System View** icon as shown above. This icon is located on the Tool Bar and the menu option can be accessed from **View > Refresh System View**.

See Also

System Pane

Summary Media Gateway Link Report

Detailed Media Gateway Link Report

Trace Routes Media Gateway Link Report

About Summary Reports or Detailed Reports

Interpreting the Values Using Summary Reports or Detailed Reports

Configure Friendly Names for Gateways

By default, VMM provides an IP address (when available) for each gateway. To make it easier to identify gateways, you can assign an alias (a "friendly" name) for each gateway. When assigned, the alias for a gateway will be displayed in the Label column on the System pane.

You can assign aliases on

- **a per-server basis**
  If you configure aliases on a per-server basis, the aliases will be displayed on all VMM clients that access that VMM server.
- **a per-client basis**
  If you configure aliases on a per-client basis, each VMM client will use its own aliases for the gateways. Even though each VMM client will view the same gateways, each VMM client will have its own alias for each gateway.
- **both a per-server basis and a per-client basis**
  If you configure aliases on both a per-server basis and a per-client basis, the VMM client will use the alias from the VMM server if that VMM client does not have an alias specified for the gateway. If both the VMM server and the VMM client have specified an alias for the same gateway, VMM client will use its alias. In this configuration, the alias specified in the VMM client will always take precedence over the alias specified in the VMM server.

To configure aliases for gateways, you must create a gateway alias configuration file and assign an alias to the IP address of each gateway you want. In the configuration file, you define an alias for a gateway by entering the IP address of the gateway, followed by the alias you want to use. Be sure to enter one IP address and alias per line in this file.

For example, suppose you have gateways at IP addresses 192.168.33.50, 192.168.37.89, and 192.168.56.22, and you want to assign an alias to each gateway. In the gateway alias configuration file, you would enter the following information:

```
192.168.33.50 Bob
192.168.37.89 Alice
192.168.56.22 Jane
```

One you create and save the gateway alias configuration file, you must specify the name of this file as the value of the **FriendlyPath** attribute in the server and/or client initialization files. By default, in both the VMM server initialization file and the VMM client initialization file, the **FriendlyPath** attribute is set to **FriendlyLabelsServer.ini** (FriendlyPath=FriendlyLabelsServer.ini).

VMM server uses the initialization file ***VoIPMonMgrServer.ini***. VMM client uses the initialization file ***VoIPMonMgrClient.ini***. These initialization files are located in the VMM installation directory.

NOTE:
The gateway alias configuration file must be located in the same folder as the VMM initialization file (that is, VoIPMonMgrServer.ini or VoIPMonMgrClient.ini).

About Dialog

This dialog box shows

- the version of VMM
- the current license state (that is, whether you are using a valid license or you are running VMM in evaluation mode)
- the number of licenses purchased
- the number of phones at the local server. This number represents the phones that reported to VMM in the last 28 days. This number will increase if you move phones (for example, change extensions or IP addresses). In this case, these phones appear to be new endpoints to VMM. Since there is a 30-day grace period, this will not be a problem.
- the number of phones at the local server that exceed the license (that is, the number of phones that are unlicensed). If greater than zero, this number is displayed in red. This can occur if you have only one monitor connected to the WebLM License Server, and you have more phones stored in the database than licenses purchased.
- the number of media gateways at the local server. This number represents the media gateways that reported to VMM in the last 28 days.
- the number of media gateways at the local server that exceed the license (that is, the number of media gateways that are unlicensed). If greater than zero, this number is displayed in red. This can occur if you have only one monitor connected to the WebLM License Server, and you have more media gateways stored in the database than licenses purchased.

Avaya provides a 90-day trial version of VoIP Monitoring Manager. After 90 days, VoIP Monitoring Manager stops collecting RTCP data. You have the option of purchasing the VoIP Monitoring Manager license key. This key is required to fully activate the VoIP Monitoring Manager beyond the 90-day trial period. When a license key is purchased, an instance of WebLM License Server is required to manage the license key. If you do not have a license to use VoIP Monitoring Manager, you can use the software for a 90-day trial period.

See Also

About Licenses

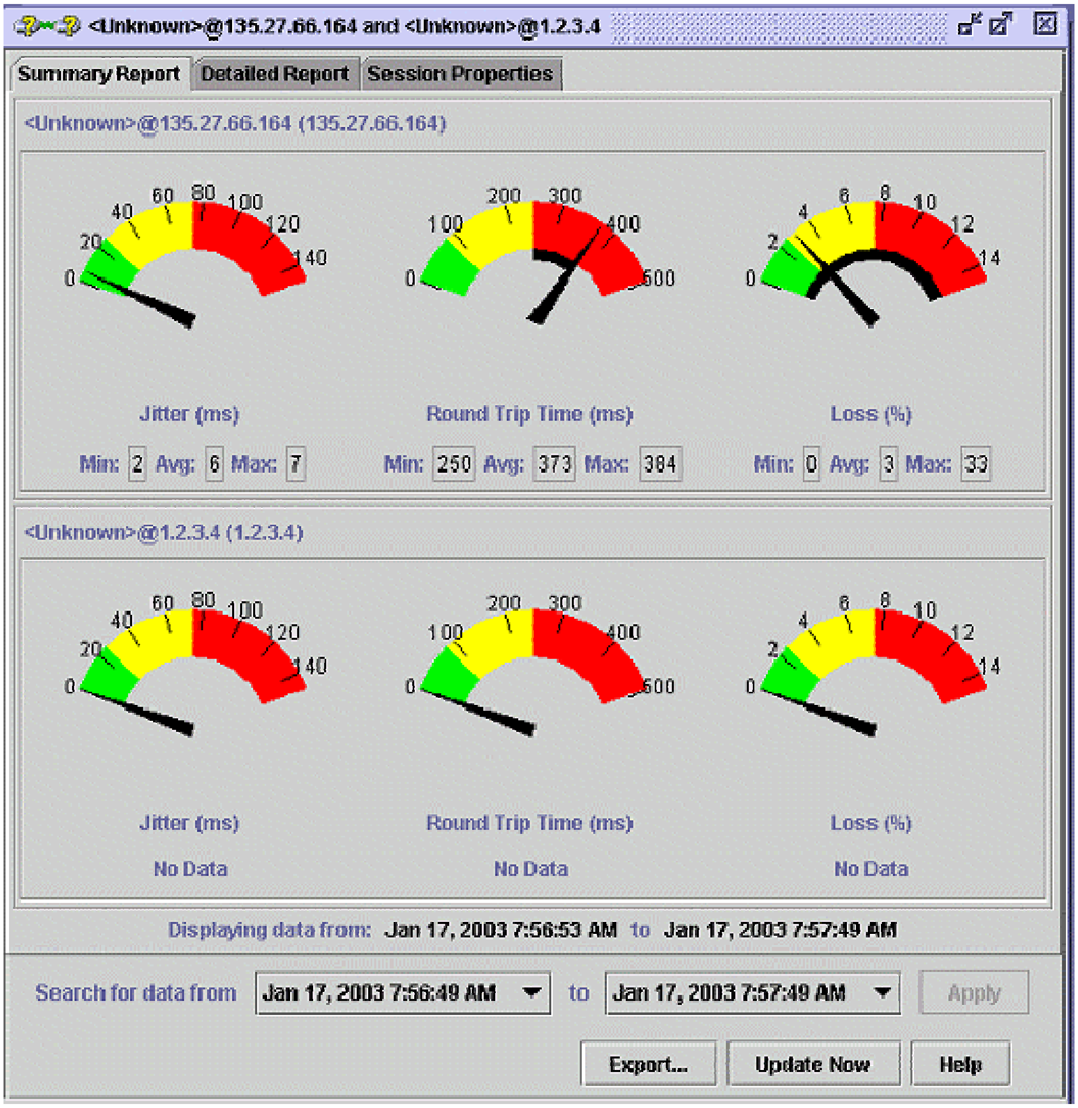
Working with Reports (Client)

About Summary Reports

The Summary Reports display the QoS data as a reading on a gauge. The green segment of the gauge indicates values that reflect acceptable voice quality measured. The amber segment warns you of degraded voice quality levels and the red segment indicates unacceptable voice quality levels measured. The needle on the gauge shows the average values measured and the black inner arc shows the range of values measured. To edit the default range displayed on the gauges, use the Report Properties dialog.

The Summary Report Features:

- **Displays information** such as the type of endpoint and the phone number.
- **Displays start and end dates** at the bottom of the report. These dates can be altered to narrow or lengthen the date range. This will cause the data to show more or less detail in the report.



<Unknown>@135.27.66.164 and <Unknown>@1.2.3.4

<Unknown>@135.27.66.164 (135.27.66.164)

Jitter (ms) Min: 2 Avg: 6 Max: 7

Round Trip Time (ms) Min: 250 Avg: 373 Max: 384

Loss (%) Min: 0 Avg: 3 Max: 33

<Unknown>@1.2.3.4 (1.2.3.4)

Jitter (ms) No Data

Round Trip Time (ms) No Data

Loss (%) No Data

Displaying data from: Jan 17, 2003 7:56:53 AM to Jan 17, 2003 7:57:49 AM

Search for data from Jan 17, 2003 7:56:49 AM to Jan 17, 2003 7:57:49 AM

See Also

About Detailed Reports

About Session Properties

Data Stored for 100 Days

Interpreting the Values Using Summary Reports or Detailed Reports

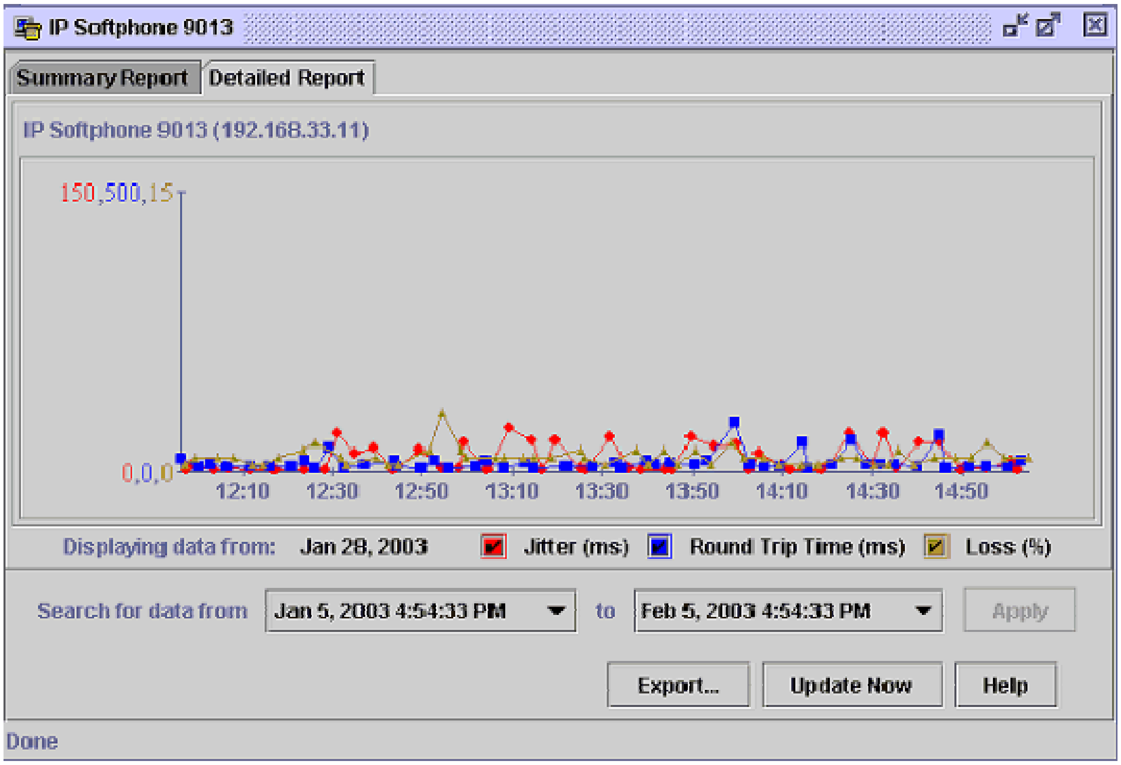
Search for a Specific Phone Number, SIP Username, QoS Values or Network Address

About Detailed Reports

A Detailed Report enables you to see more detailed information than a Summary Report provides. The Detailed Reports show how the QoS values change during the call and when this occurred. This is displayed on a line graph. The X-axis shows the time range and the Y-axis shows the value for each of the QoS parameters. The upper values on the Y-axis indicate unacceptable limits. Each point on the line graph represents the maximum value since the last point displayed.

The Detailed Report Features:

- **A tool tip** enables you to point your mouse at the samples on the line report to see the exact data measured.
- **Color-coded QoS data** is represented on the report by a different color. You can uncheck the display of one or more of the QoS data.
- Show more or less detail by altering the date range. These dates can be altered to narrow or lengthen the date range. This causes the data to show respectively more or less detail in the report.



Displaying data from: Jan 28, 2003 ☑ Jitter (ms) ☑ Round Trip Time (ms) ☑ Loss (%)

Search for data from Jan 5, 2003 4:54:33 PM to Feb 5, 2003 4:54:33 PM

See Also

About Summary Reports

About Session Properties

Interpreting the Values Using Detailed Reports and Summary Reports

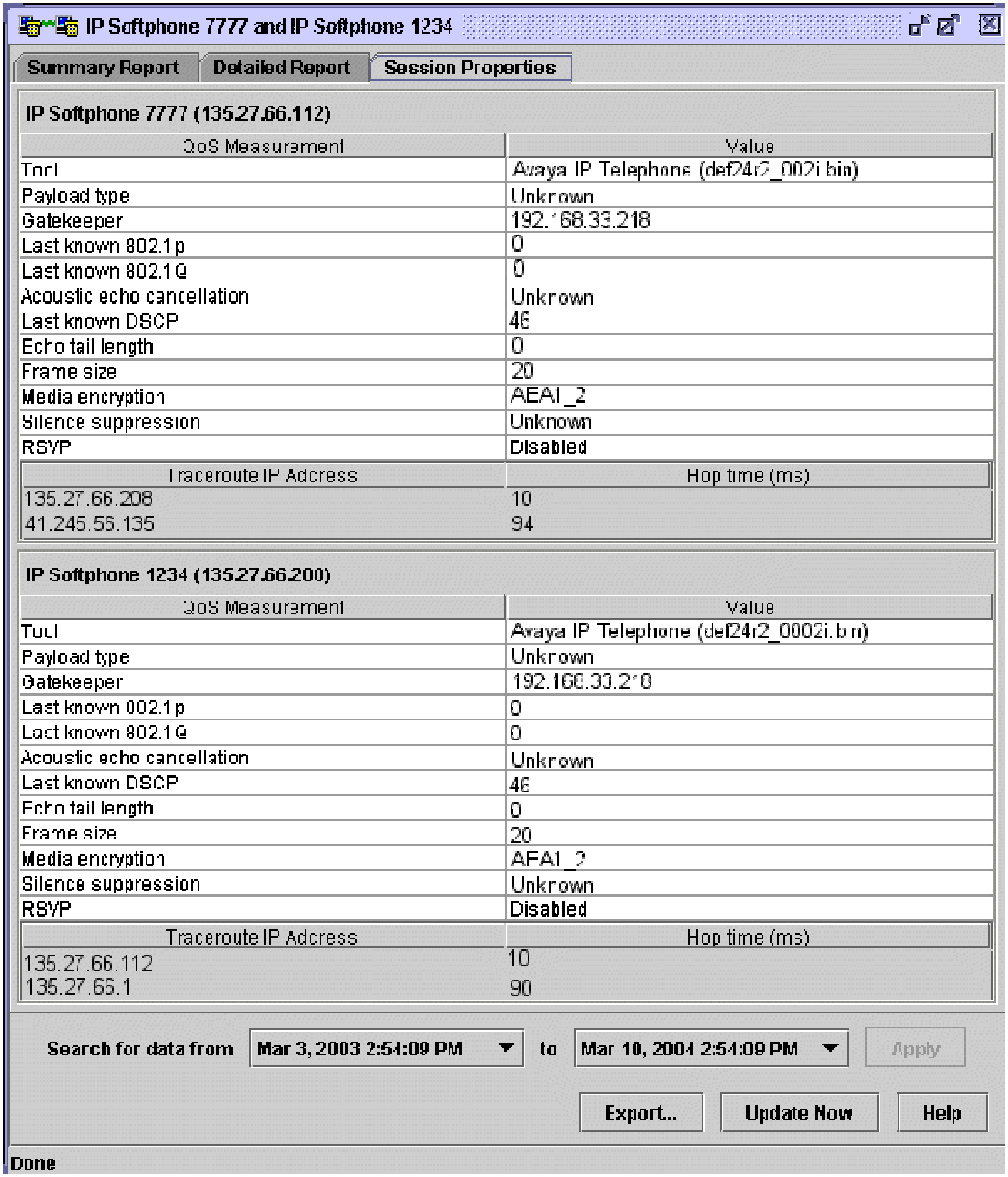
Search for a Specific Phone Number, SIP Username, QoS Values,or Network Address

About Session Properties

The report dialog displays the following static properties of the current session in the Session Properties tab:

To Display the Session Properties

1. From the Result List, expand a call and select a **session** from the list.
2. Click **Report**. The Report dialog displays.
3. From the Report dialog, click the **Session Properties** tab. The Session Properties displays.
4. Click on an option in the image for more information.



IP Softphone 7777 (135.27.66.112)

QoS Measurement	Value
Tool	Avaya IP Telephone (def24r2_002i.bin)
Payload type	Unknown
Gatekeeper	192.168.33.218
Last known 802.1p	0
Last known 802.1Q	0
Acoustic echo cancellation	Unknown
Last known DSCP	46
Echo tail length	0
Frame size	20
Media encryption	AEAI_2
Silence suppression	Unknown
RSVP	Disabled

Traceroute IP Address	Hop time (ms)
135.27.66.208	10
41.245.55.135	94

IP Softphone 1234 (135.27.66.200)

QoS Measurement	Value
Tool	Avaya IP Telephone (def24r2_0002i.bin)
Payload type	Unknown
Gatekeeper	192.168.33.218
Last known 802.1p	0
Last known 802.1Q	0
Acoustic echo cancellation	Unknown
Last known DSCP	46
Echo tail length	0
Frame size	20
Media encryption	AEA1_2
Silence suppression	Unknown
RSVP	Disabled

Traceroute IP Address	Hop time (ms)
135.27.66.112	10
135.27.65.1	90

Search for data from Mar 3, 2003 2:54:09 PM to Mar 10, 2004 2:54:09 PM

See Also

Components of VoIP Monitoring Manager

Starting the VoIP Monitoring Manager Web Client

Difference Between Endpoint and Session Reports

The QoS data that displays on an endpoint report is an aggregation of all the sessions that are active at this endpoint.

Single Endpoint Reports Show Multiple Sessions

Some endpoints (such as media gateways) can participate in multiple concurrent sessions, so a high value on a single endpoint report indicates that one or more of the sessions is/was experiencing degradation of quality. It does not indicate which session.

Session Reports Display Endpoints for Only that Session

In contrast, a report showing both endpoints involved in the session displays the QoS data as experienced by both endpoints for that session only. To isolate problems, you need to narrow your search by either searching for a specific QoS value or altering the date of the report.

See Also

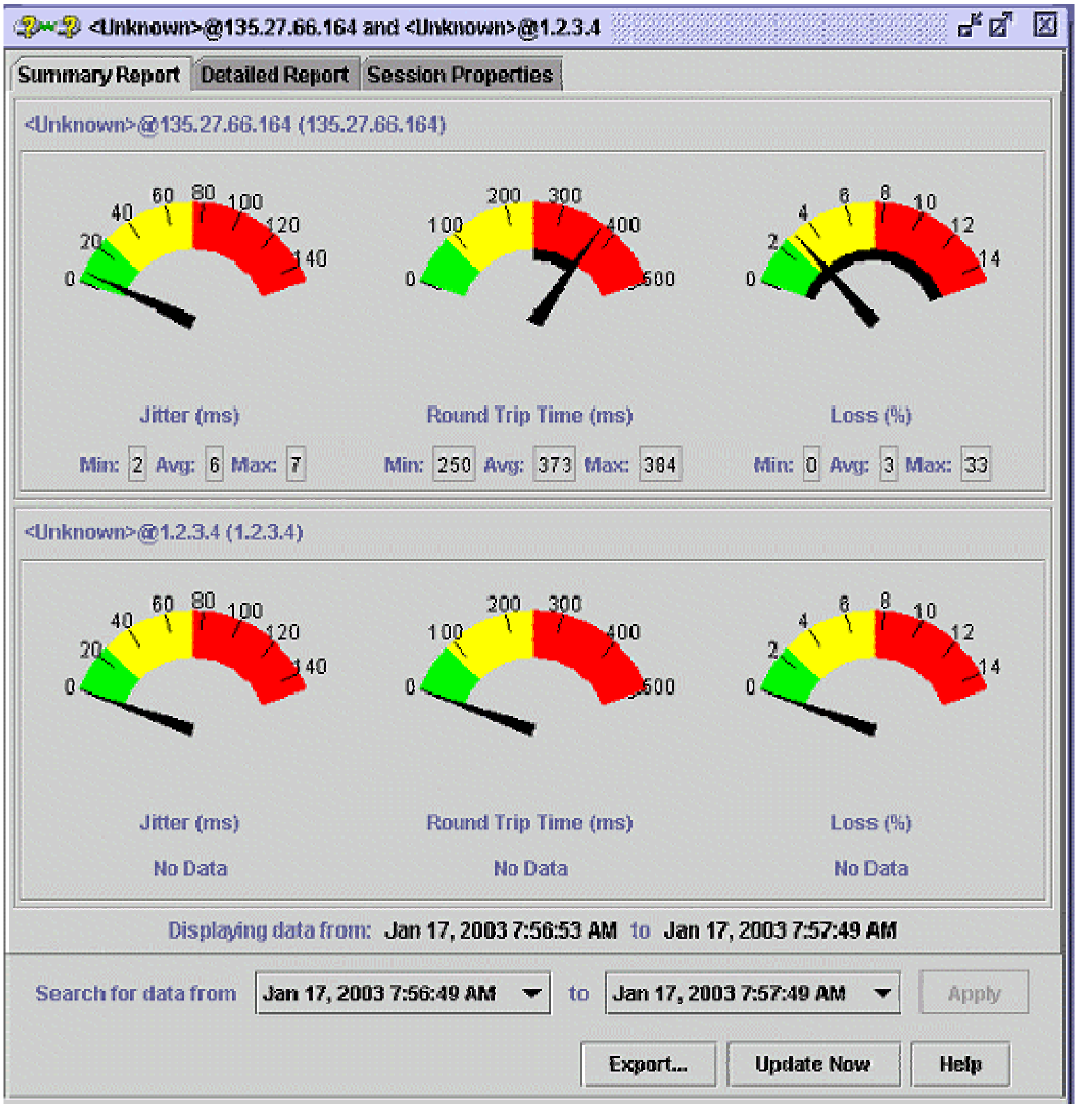
View Sessions in a Report

About Detailed and Summary Reports

Interpreting the Values Using Detailed Reports and Summary Reports

Summary Session Report

A session displays in a Summary Report as shown in the image. The parent endpoint involved in the session displays in the top report with the child endpoint below.



<Unknown>@135.27.66.164 and <Unknown>@1.2.3.4

<Unknown>@135.27.66.164 (135.27.66.164)

Min: 2 Avg: 6 Max: 7

Min: 250 Avg: 373 Max: 384

Min: 0 Avg: 3 Max: 33

<Unknown>@1.2.3.4 (1.2.3.4)

No Data

No Data

No Data

Displaying data from: Jan 17, 2003 7:56:53 AM to Jan 17, 2003 7:57:49 AM

Search for data from Jan 17, 2003 7:56:49 AM to Jan 17, 2003 7:57:49 AM

See Also

How to Use VoIP Monitoring Manager Client

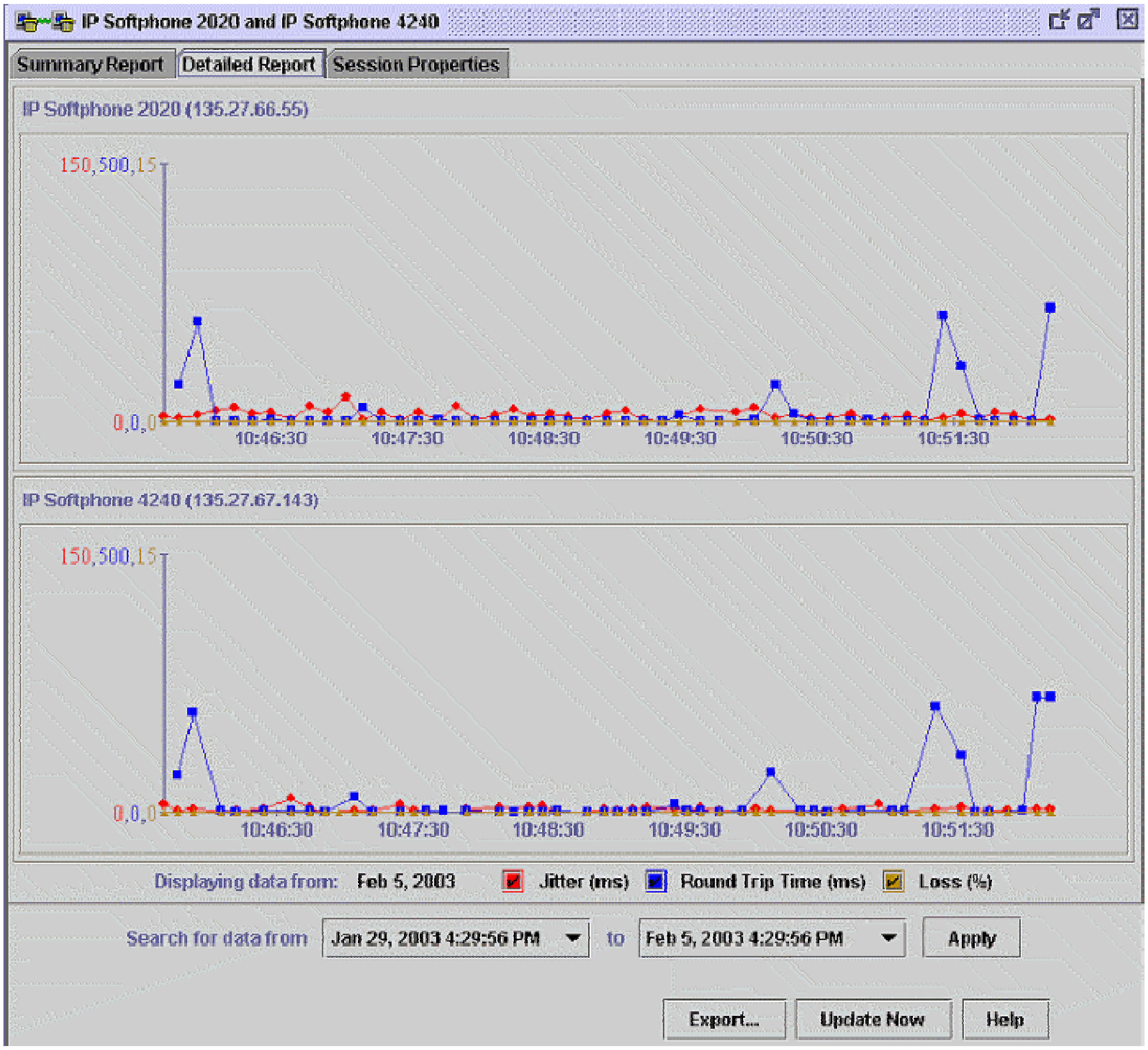
About Summary Reports and Detailed Reports

Interpreting the Values Using Summary Reports and Detailed Reports

Detailed Session Report

A session displays in a Detailed Report as shown in the image. The parent endpoint involved in the session displays in the top report with the child endpoint below.

To view a Detailed Session Report, click the **Detailed Report** tab located at the top of the report dialog.



Displaying data from: Feb 5, 2003 ☑ Jitter (ms) ☑ Round Trip Time (ms) ☑ Loss (%)

Search for data from Jan 29, 2003 4:29:56 PM to Feb 5, 2003 4:29:56 PM Apply

See Also

How to Use VoIP Monitoring Manager Client

About Summary Reports and Detailed Reports

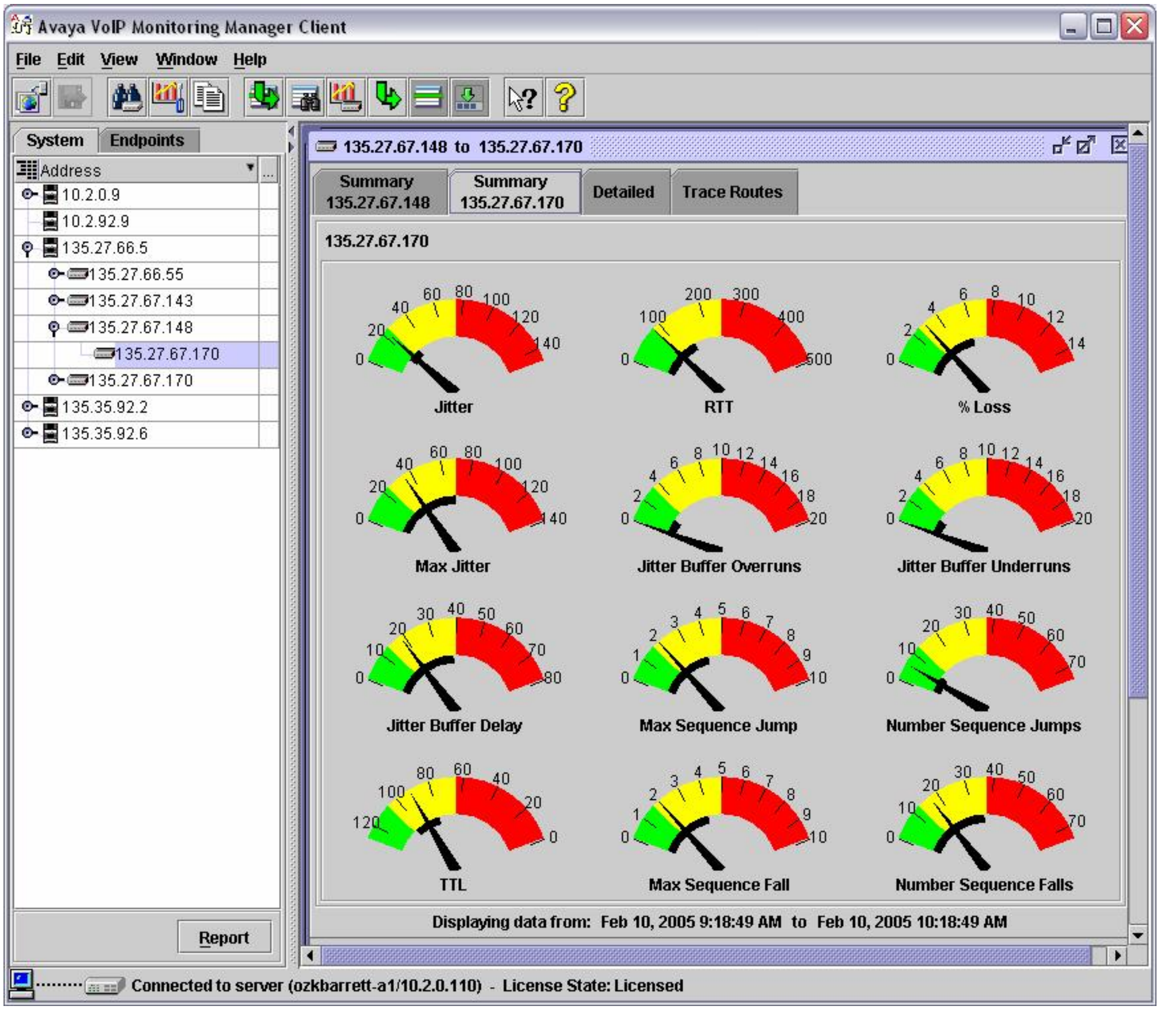
Interpreting the Values Using Summary Reports and Detailed Reports

Summary Media Gateway Link Report

Displays the following aggregate information of all the VoIP sessions for the selected media gateway:

- Jitter
- RTT
- % Loss
- Max Jitter
- Jitter Buffer Overruns
- Jitter Buffer Underruns
- Jitter Buffer Delay
- Max Sequence Jump
- Number Sequence Jumps
- TTL
- Max Sequence Fail
- Number Sequence Fails

The following image is a sample Summary Media Gateway Link report.



Displaying data from: Feb 10, 2005 9:18:49 AM to Feb 10, 2005 10:18:49 AM

Connected to server (ozkbarrett-a1/10.2.0.110) - License State: Licensed

To view a Summary Media Gateway Link Report

1. From the System pane, select an object or click the expanding icon and select a child endpoint that was in a session with the parent endpoint. The Report button becomes available.
2. Click **Report**. The Media Gateway Link reports appear.
3. Click the **Summary** tab.

See Also

How to Use VoIP Monitoring Manager Client

Detailed Media Gateway Link Report

Trace Routes Media Gateway Link Report

About Summary Reports and Detailed Reports

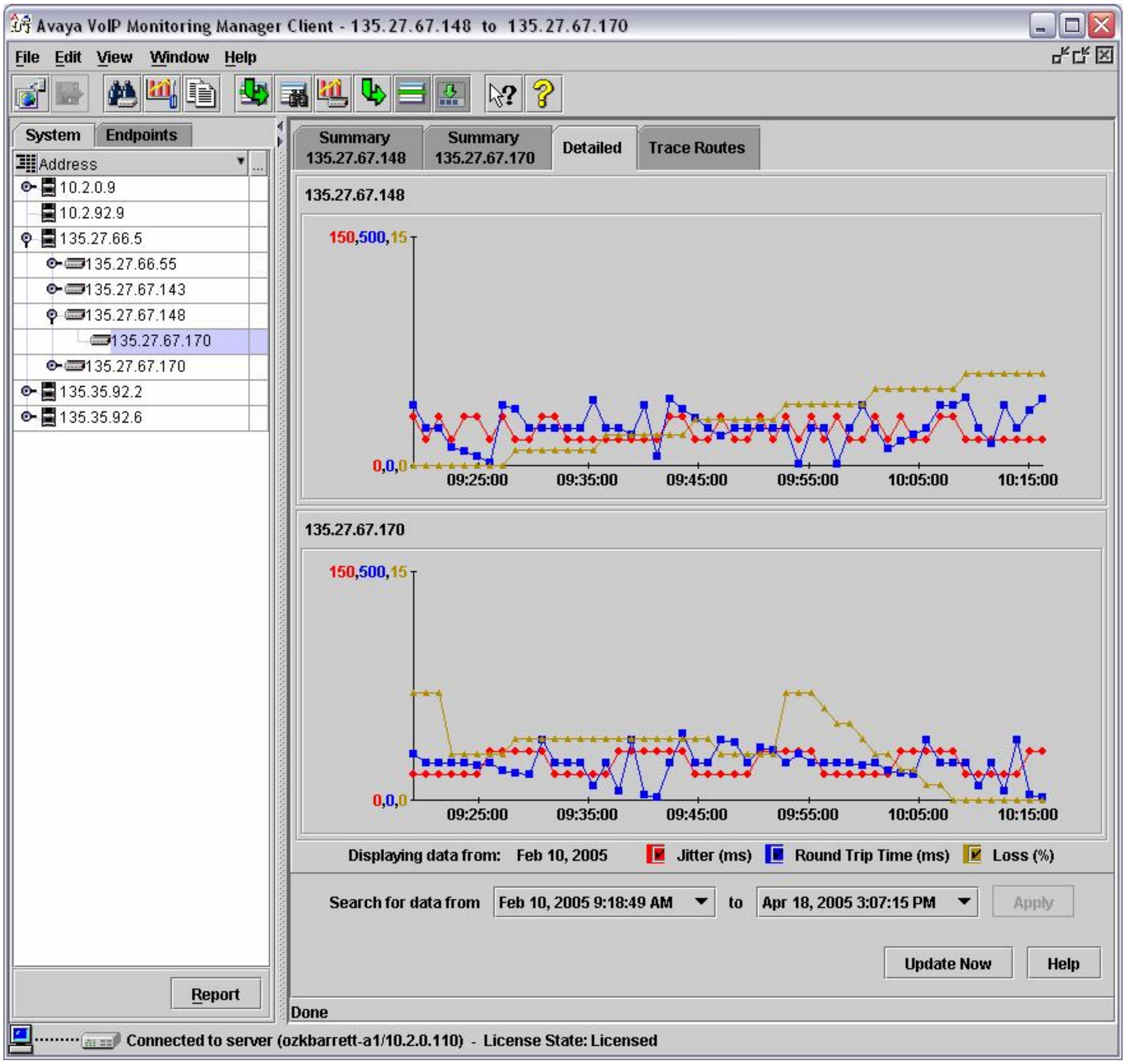
Interpreting the Values Using Summary Reports and Detailed Reports

Detailed Media Gateway Link Report

Shows the aggregate jitter, RTT, and percent loss on a graph for VoIP sessions going between the two selected media gateways. This report excludes VoIP sessions at the media gateways that are with phones.

The parent endpoint involved in the session displays in the top report with the child endpoint below.

The following image shows a sample Detailed Media Gateway Link report.



To view a Detailed Media Gateway Link Report

1. From the System pane, select an object or click the expanding icon and select a child endpoint that was in a session with the parent endpoint. The Report button becomes available.

2. Click **Report**. The Media Gateway Link reports appear.

3. Click the **Detailed Report** tab.

See Also

How to Use VoIP Monitoring Manager Client

Summary Media Gateway Link Report

Trace Routes Media Gateway Link Report

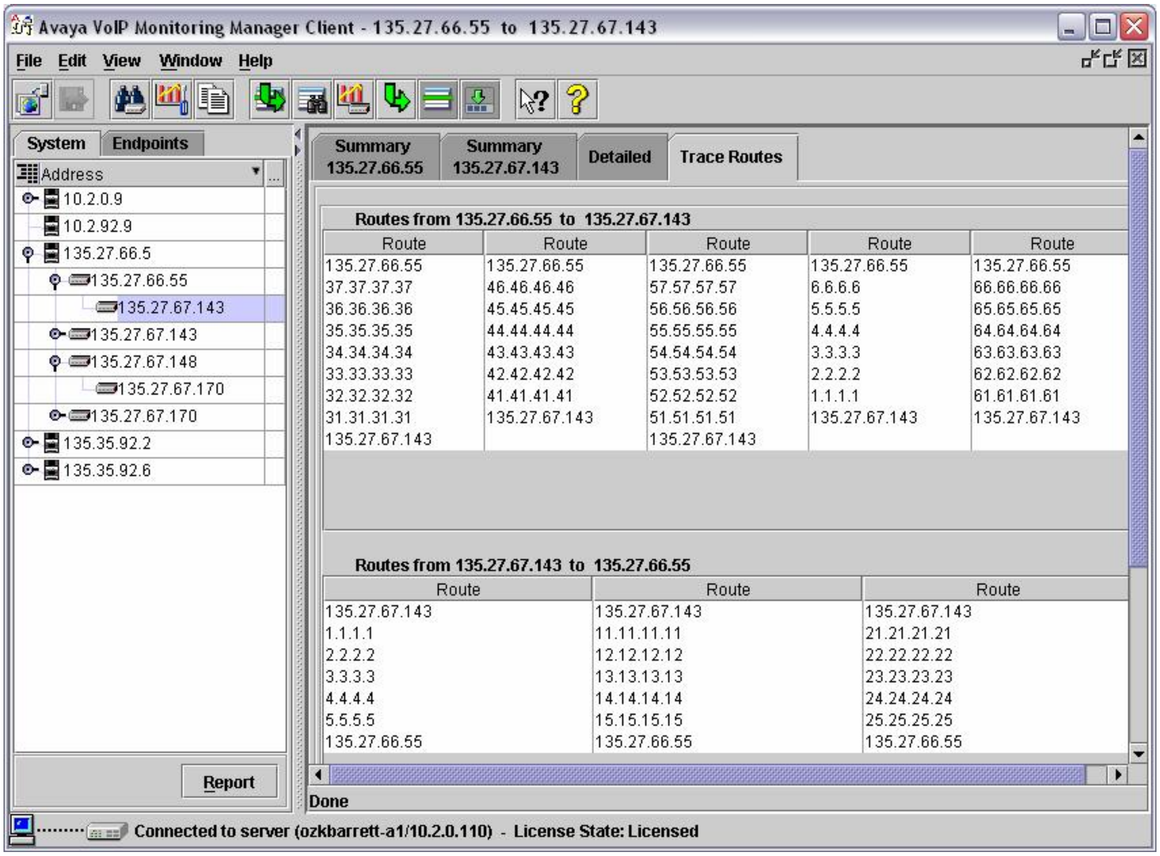
About Summary Reports and Detailed Reports

Interpreting the Values Using Summary Reports and Detailed Reports

Trace Routes Media Gateway Link Report

Shows the probable routes used between the two selected media gateways.

The following image shows a sample Trace Routes Media Gateway Link report.



Routes from 135.27.66.55 to 135.27.67.143

Route	Route	Route	Route	Route
135.27.66.55	135.27.66.55	135.27.66.55	135.27.66.55	135.27.66.55
37.37.37.37	46.46.46.46	57.57.57.57	6.6.6.6	66.66.66.66
36.36.36.36	45.45.45.45	56.56.56.56	5.5.5.5	65.65.65.65
35.35.35.35	44.44.44.44	55.55.55.55	4.4.4.4	64.64.64.64
34.34.34.34	43.43.43.43	54.54.54.54	3.3.3.3	63.63.63.63
33.33.33.33	42.42.42.42	53.53.53.53	2.2.2.2	62.62.62.62
32.32.32.32	41.41.41.41	52.52.52.52	1.1.1.1	61.61.61.61
31.31.31.31	135.27.67.143	51.51.51.51	135.27.67.143	135.27.67.143
135.27.67.143		135.27.67.143		

Routes from 135.27.67.143 to 135.27.66.55

Route	Route	Route
135.27.67.143	135.27.67.143	135.27.67.143
1.1.1.1	11.11.11.11	21.21.21.21
2.2.2.2	12.12.12.12	22.22.22.22
3.3.3.3	13.13.13.13	23.23.23.23
4.4.4.4	14.14.14.14	24.24.24.24
5.5.5.5	15.15.15.15	25.25.25.25
135.27.66.55	135.27.66.55	135.27.66.55

Done

Connected to server (ozkbarrett-a1/10.2.0.110) - License State: Licensed

To view a Trace Routes Media Gateway Link Report

1. From the System pane, select an object or click the expanding icon and select a child endpoint that was in a session with the parent endpoint. The Report button becomes available.

2. Click **Report**. The Media Gateway Link reports appear.

3. Click the **Trace Routes** tab.

See Also

How to Use VoIP Monitoring Manager Client

Summary Media Gateway Link Report

Detailed Media Gateway Link Report

View a Report

You can generate reports for endpoints and media gateways.

Endpoint Reports

After you run a search, you can view the report on selected endpoints and endpoints involved in a session. There are two types of reports: Summary Reports and Detailed Reports.

To View the QoS Data for an Endpoint

1. From the **Results List,** select an **endpoint** or click the expanding icon and select a child endpoint that was in a session with the parent endpoint. The Report button become available.

2. Click **Report**. The Report dialog opens.

Media Gateway Link Reports

From the System pane, you can select a media gateway and click the **Report** button to view an aggregated report of all the VoIP sessions over the selected link. There are three types of reports: Summary Media Gateway Link Report, Detailed Media Gateway Link Report, and Trace Routes Media Gateway Link Report.

See Also

How to Use VoIP Monitoring Manager Client

About Detailed Reports and Summary Reports

Interpreting the Values Using Detailed Reports and Summary Reports

Close Report

You can close the report by either clicking on the **Close** button on the Title Bar of the report or select the **Close** option from the **Window** menu. The Close button is the last button on the right hand side of the report. The icon has an X in the middle of it as shown above.

- Select **Window > Close** (Ctrl + w, then e).

See Also

Arrange the Reports on the Screen

Close All Reports

You can close all the reports simultaneously by selecting the **Close All** option from the **Window** menu. If you only want to close one report, click on the **Close button** on the report.

- Select **Window > Close** (Ctrl + w, then l).

See Also

Arrange the Reports on the Screen

Copy Report

You can copy the reports to the computer's clipboard. This enables you to paste the report as an image into other applications.

To Copy

1. Click on the title bar of the report you want to copy.
2. Select **Edit > Copy Report** (Ctrl + C).
3. Open the application you want to paste the report into such as Word or Excel.
4. Press **Ctrl + v** on your keyboard to paste the report.

> If you are using the VoIP Monitoring Manager Web Client then you will be unable to copy the reports to another program.

Move the Reports

You can drag and drop the reports around the display area to assist with viewing. To move the report, click on the Title Bar with your left mouse button, and by holding the button down, drag the Title Bar across the screen. If you cannot see the Title Bar, you may need to expand the viewing area or use the scroll bars to bring the Title Bar into view.

Expand and Shrink the Reports

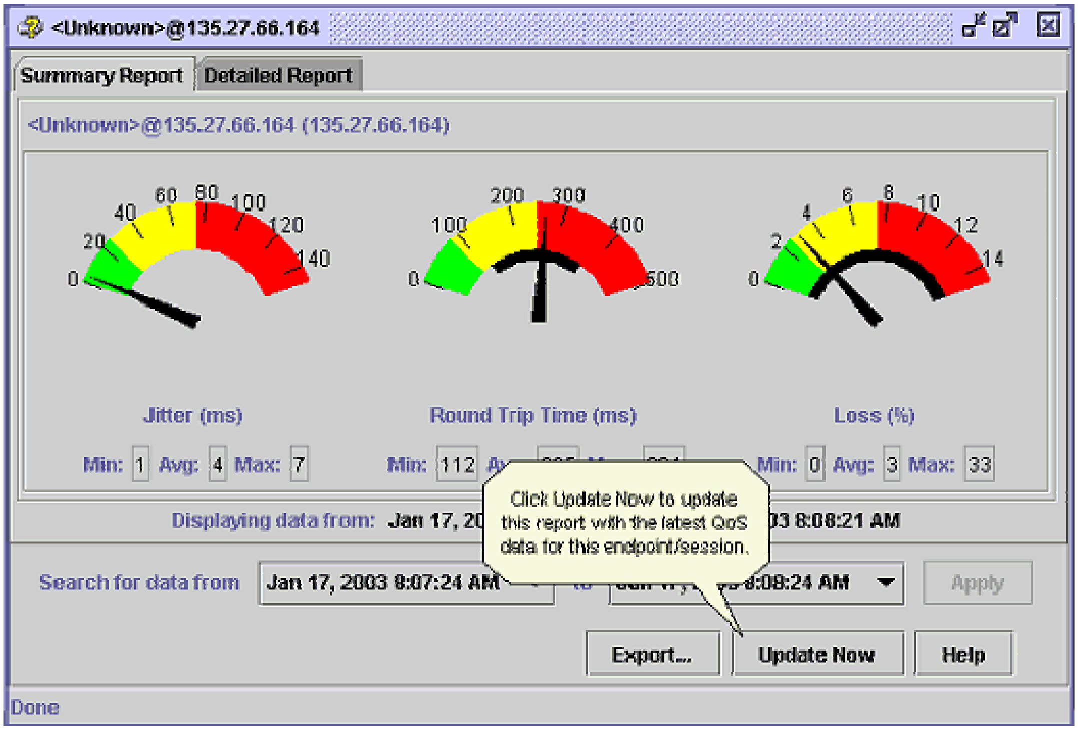
You can also expand and shrink a report, by pointing your mouse at the report's borders, when the cursor changes into a bi-directional arrow, hold down your left mouse button and drag the report's borders to the size you want. You can also apply this action to the whole application to make it bigger or smaller.

See Also

Arrange the Reports on the Screen

Update Report

To update an individual report click on the **Update Now** button located on the report dialog. The report will update with the QoS data for the endpoint/session.



Jitter (ms) Min: 1 Avg: 4 Max: 7

Round Trip Time (ms) Min: 112

Loss (%) Min: 0 Avg: 3 Max: 33

Displaying data from: Jan 17, 20 03 8:08:21 AM

Search for data from Jan 17, 2003 8:07:24 AM 8:08:24 AM

Click Update Now to update this report with the latest QoS data for this endpoint/session.

See Also

View a Report

About Summary Reports or Detailed Reports

Interpreting the Values Using Summary Reports or Detailed Reports

Update All Reports

To update all reports that are displaying, click **Update All Reports** icon as shown above. This icon is located on the Tool Bar and the menu option can be accessed from **View > Update All Reports**.

See Also

Search

About Summary Reports or Detailed Reports

Interpreting the Values Using Summary Reports or Detailed Reports

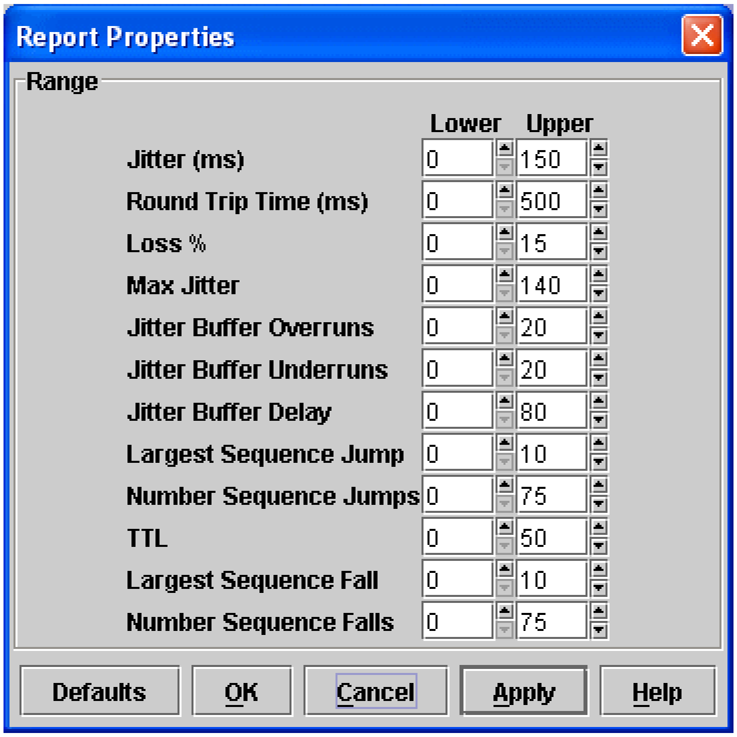
Edit Report Properties

The Report Properties dialog is accessed from the **Edit** menu. It enables you to edit the range of the scale for each of the QoS parameters displayed on the reports.

To alter the range, type in a number in the fields or use the arrow buttons and click **Apply** or **OK** to save your changes.

To reset the parameters to the default settings, click **Defaults**.

To close the dialog without saving any changes, click **Cancel**.



	Lower	Upper
Jitter (ms)	0	150
Round Trip Time (ms)	0	500
Loss %	0	15
Max Jitter	0	140
Jitter Buffer Overruns	0	20
Jitter Buffer Underruns	0	20
Jitter Buffer Delay	0	80
Largest Sequence Jump	0	10
Number Sequence Jumps	0	75
TTL	0	50
Largest Sequence Fall	0	10
Number Sequence Falls	0	75

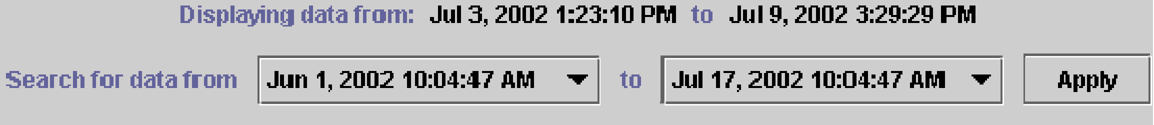
See Also

About Summary Reports or Detailed Reports

Interpreting the Values Using Summary Reports or Detailed Reports

Altering Date Range of Reports

You can edit the date range that displays on an individual report. This enables you to zoom in or out on a time period and see more or less of the detail. If you select a smaller date range, then you will see more data on the graph. If you select a longer date range then you will see less detail.



Displaying data from: Jul 3, 2002 1:23:10 PM to Jul 9, 2002 3:29:29 PM

Search for data from Jun 1, 2002 10:04:47 AM ▼ to Jul 17, 2002 10:04:47 AM ▼ Apply

To Alter the Date Range

1. From the report, click the **Search data from** and the **to** drop down arrows to access the calendars. You can click on the day and use the arrow buttons to scroll through AM/PM, seconds, minutes, hours, months and years.

2. Click **Apply.** The Report updates with the QoS data for the adjusted date range.

See Also

About Detailed Reports and Summary Reports

Interpreting the Values Using Detailed Reports and Summary Reports

Interpreting Reports

Interpreting the Values Using Detailed Reports

You interpret the Detailed Reports by noting where the sampled QoS data displays on the line graph and noting when this may have occurred. The upper values on the Y-Axis indicate unacceptable limits. The X-Axis shows the date.

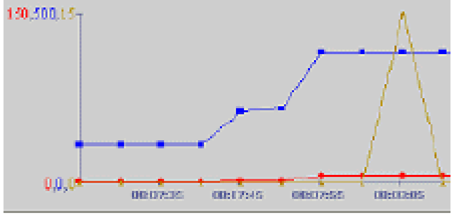


Table of Values for Detailed Reports

Jitter (ms) Displayed Red ☑	**Round Trip Time (ms)** Displayed Blue ☑	**Loss (%)** Displayed Brown ☑
> 150ms **Not Acceptable**	**> 500ms** **Not Acceptable**	**> 30%** **Not Acceptable**
50 to 150ms **Warning** Crackling, static or intermittent delay could be reported.	**150 to 500ms** **Warning** Slight pause in the conversation at the lower end of the range to more lengthy delays at the top end of the range could be reported.	**10 to 30%** **Warning** Drop out and missing parts of the conversation could be reported.

0 to 50ms **Acceptable** Conversation was smooth.	**0 to 180ms** **Acceptable** No delay between each endpoint.	**0 to 10%** **Acceptable** No drop out in conversation.

See Also

About Detailed Reports

About Summary Reports

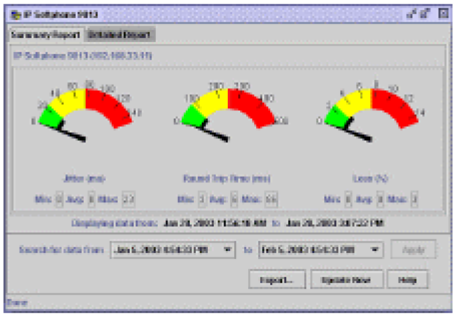
About Session Properties

Interpreting the Values Using Summary Reports

Search for a Specific Phone Number, QoS Values or Network Address

Interpreting the Values Using Summary Reports

You interpret the Summary Reports by noting where the needle on the gauges is positioned for each of the QoS gauges. When the needle is positioned in either the yellow or red ranges, it is indicating degradation in the QoS. The needle on the gauge shows the average values measured and the black inner arc shows the range of values measured. These values also display below each gauge.



Displaying data from: Jan 28, 2003 11:56:18 AM to Jan 28, 2003 3:07:22 PM

Table of Values for Summary Reports

	Jitter (ms)	Round Trip Time (ms)	Loss (%)
🟩	**0 to 50ms**	**0 to 180ms**	**0 to 10%**
🟩	**Acceptable** Conversation was smooth.	**Acceptable** No delay between each endpoint.	**Acceptable** No drop out in conversation.
🟨	**50 to 150ms**	**180 to 500ms**	**10 to 30%**
🟨	**Warning** Crackling, static or intermittent delay could be reported.	**Warning** Slight pause in the conversation at the lower end of the range to more lengthy delays at the top end of the range could be reported.	**Warning** Drop out and missing parts of the conversation could be reported.
🟧	**> 150ms**	**> 500ms**	**> 30%**
🟧	**Not Acceptable**	**Not Acceptable**	**Not Acceptable**

See Also

About Detailed Reports

About Summary Reports

About Session Properties

Interpreting the Values Using Detailed Reports

Search for a Specific Phone Number, QoS Values or Network Address

Y-axis

The Y-axis on the Detailed Reports line graph is the vertical area of the report, covering the top to the bottom of the graph. The top of the Y-axis represents the upper levels for each of the QoS parameters and the bottom of the Y-axis represents the lower levels. You can point your mouse at the samples on the line graph and the exact time and QoS value will display. For more detailed information see the topic on About Detailed Reports and/or Interpreting Detailed Reports.

Different Scales for Each QoS Parameter

The QoS parameters have different values. To represent each parameter on the same report the Y-axis has a different scale that suits each QoS parameter. These scales are shown on the Y-axis in their respective colors.

See Also

Edit Report Properties

X-axis

X-axis

The X-axis on the Detailed Reports represents the date range. It is the horizontal area of the line graph, from the left to the right of the report. The start of the date range begins from the left of the horizontal axis and continues until the end of the date range on the far right side.

Alter the Date Range to Show More Detail

You can alter the date range to a shorter date or longer date period to see more or less detail.

See Also

Y-axis

About Detailed Reports

Interpreting Detailed Reports

Gateway

The Results List will display one or more phone numbers next to the Gateway endpoint type. These phone numbers are the phone numbers that the Gateway is acting as an intermediary for. Therefore, the phone number of the Gateway can change and can be multiple phone numbers. The Results List will separate endpoints involved in a session with a comma (,). Conferenced calls are separated by a colon (:).

For example, if the following phone number **8616,1111:1222, 8904** displays in the Results List, then the Gateway has three active sessions as explained:

- Telephone 8616 is a Non-IP telephone which is in a session with a Softphone.
- Telephones 1111 and 1222 are conferenced (e.g. IP phone 8888 is in a Session with these two phones).
- Telephone 8904 is a Non-IP telephone in a session with an IP telephone.

Arranging Reports

Maximize Reports

You can expand the report to fill the whole viewing area by clicking on the **Maximize button** on the report or from the **Window** menu. The Maximize button is the second button on the report's Title Bar. It is next to the **Close** button. If you select to maximize a report, you can undo maximize from the Window menu.

- Select **Window > Maximize** (Alt + w then, m)

See Also

Arrange the Reports on the Screen

Arrange Icons

The Arrange Icons option on the Window menu enables you to line reports up along the bottom of the application. For this option to be available, you must have a report minimized.

- Select **Window > Arrange Icons** (Alt + w, then a)

See Also

Arrange the Reports on the Screen

Arrange the Reports on the Screen

You can organize the reports in the VoIP Monitoring Manager display area using the following options from the Window menu. Multiple reports. For more information, click on any of the following options:

- Cascade
- Maximize
- Tile Horizontally
- Tile Vertically
- Arrange Icons
- Close
- Close All

You can also hold your mouse down on the Title Bar of each report and drag the report across the screen or click on the Minimize, Maximize or Close buttons. To re-open a window that you have minimized, double-click on the minimized Title Bar.

See Also

How to Use VoIP Monitoring Manager Client

About Detailed Reports or Summary Reports

Interpreting the Values Using Detailed or Summary Reports

Tile Vertically

You can tile all reports vertically so that each report is lined up, one next to the other showing the Title Bar and the QoS data. If you still have difficulty viewing the reports, try maximizing the application or closing either the **Tool Bar** or **Results List**.

- Select **Window > Tile Vertically** (Alt + w, then v)

See Also

Arrange the Reports on the Screen

Tile Horizontally

You can tile all reports horizontally so that each report is lined up, one above the other showing the Title Bar and the QoS data. If you still have difficulty viewing the reports, try maximizing the application or close either the **Tool Bar** or Results List (**View** > **Tool Bar** or **Results List**)

- Select **Window > Tile Horizontally** (Alt + w, then h)

See Also

Arrange the Reports on the Screen

Cascade Reports

You can cascade all the reports so that each report overlaps the other showing the title bar for ease of access. To cascade the reports;

- Select **Window > Cascade** (Alt + w then c)

See Also

Arrange the Reports on the Screen

Minimize the Reports

You can minimize the report so that only the Title Bar is visible in the viewing area by clicking on the **Minimize** button on the report. The Minimize button is the first button on the report's Title Bar. It is next to the **Maximize** button. To return the report to its normal state, double click on the Title Bar.

See Also

Arrange the Reports on the Screen

View Multiple Reports

You can view multiple reports at one time by repeatedly selecting endpoints and clicking on the **Report** button. You may need to arrange the reports on the screen so that you can see them easily. You can minimize and maximize the reports. If you have minimized a report, you can easily maximize it by double-clicking on its title bar.

See Also

View a Report

About Summary and Detailed Reports

View Sessions in a Report

As a single phone call could include several sessions (e.g. if the call was shuffled, conferenced, transferred and for the initial dial tone) you can view both endpoints involved in the session in a single report. The reports display the parent endpoint involved in the session in the top part with the child endpoint in the bottom part of the report. By displaying in this manner you can view both endpoints at the same time and compare the QoS information.

To View Sessions in a Report

1. Run a Search. The Results List updates.
2. In the Results List, expand the **parent endpoint** by clicking the icon positioned in the far left column. The child endpoints display in a sub list.
3. Select a **child endpoint**. The Report button becomes available.
4. Click **Report.** A Summary Session Report displays showing the parent endpoint with another report below showing the child endpoint involved in the session. To view the Detailed Session Report, click the **Detailed Report** tab or click the Session Properties tab.

See Also

About Session Properties

About Detailed Reports and Summary Reports

Interpreting the Values Using Detailed Reports and Summary Reports

Export Data (Client)

Export Result List

You can export the data in the results list to a comma separated value (csv) file.

The exported data contains records for every endpoint and every session that is displayed in VoIP Monitoring Manager. Opening or closing session folders (to show or hide the endpoints) does not affect the data that is exported.

You can open this file in most database and spreadsheet programs such as Microsoft Excel. Exporting the data to a spreadsheet enables you to manipulate the data so you can create your own reports. Click this link to see an example (Adobe Acrobat 5 or later required – the page has been split into three because of its width). You can use the sorting, counting and calculation features of Microsoft Excel to create your own reports from this raw data.

The data exported is divided into 3 tables:

- Session Table
- Time-varying Data Table
- Trace Route Table

To Export Data from the Result List

1. **File** > **Export Result List** or click the **Export** button located at the bottom of the **Result List**. A Save dialog opens.

   Tip: If you want to limit the data that is exported, narrow down your search so that less data displays in the Result List.

2. Navigate to a folder.
3. In the **File name:** field, type a name for the file.
4. Click **Save as**. The file saves with the CSV extension.
5. From Microsoft Excel, open the file. From here you can build your own report.

   Microsoft Excel can only handle 65,536 rows of data. If your exported data file contains more rows, you will need to write a script that splits the data into smaller files before you import the data into Excel.

See Also

Export Report Data

Creating Reports with Export Data

Some Fields Are Blank in the Exported Data

Export Report Data (one session)

You can export the data from a single report to a comma separated value (csv) file by using the **Export** button located on the Report dialog.

Only the data from the selected report is exported, i.e. data that matches one session, rather than a summary for multiple session.

The recommended spreadsheet is Excel. Exporting the data to Excel enables you to manipulate the data so you can create your own statistical reports. Click this link to see an example (Adobe Acrobat 5 or later required – the page has been split into three because of its width). You can use the sorting, counting and calculation features of Microsoft Excel to create your own reports from this raw data.

The data exported is divided into 3 tables:

- Session Table
- Time-varying Data Table
- Trace Route Table

To Export Data from the Report Dialog

1. Click the **Report** button located on the **Report** dialog. A Save dialog opens.
2. Navigate to a folder.
3. In the **File name:** field, type a name for the file.
4. Click **Save as**. The file saves with the CSV extension.
5. From the spreadsheet program, open the file. From here you can build your own report.

> ℹ Microsoft Excel only handles 65,536 rows of data. If you need to export more data, you will need to write a script that allows you to export more data or you could try exporting it to a database program such as Access.

See Also

Export Results List

Creating Reports with Export Data

Some Fields Are Blank in the Exported Data

Creating Reports with Exported Data

You can export the data from the Result List and/or Report dialogs to Microsoft Excel. Using Microsoft Excel you can create your own reports as shown in the linked example. This report was created by using Microsoft Excel's calculation features. It includes averaging results, counting the number of sessions, and unique participants and setting filters to determine the longest sessions, creating a line graph to visually demonstrate the information. You can create your own reports from the exported data—click this link to see and example (Adobe Acrobat reader is required).

See Also

Export Results List

Export Report Data

Some Fields Are Blank in the Exported Data

Overview of VoIP Monitoring Manager (Server)

VoIP Monitoring Manager Options

The Options dialog allows you to define and change the Data Storage, RTCP, and Configuration Messaging settings.

The SNMP Configuration dialog allows you to define and change the SNMP settings.

based on the new properties

To Edit VoIP SNMP Settings

1. Select **Edit** > **SNMP Settings** from VoIP Monitoring Manager Server. The SNMP Configuration dialog displays.
2. Enter a value for SNMP Community ID.

To Edit VoIP Monitoring Manager Options

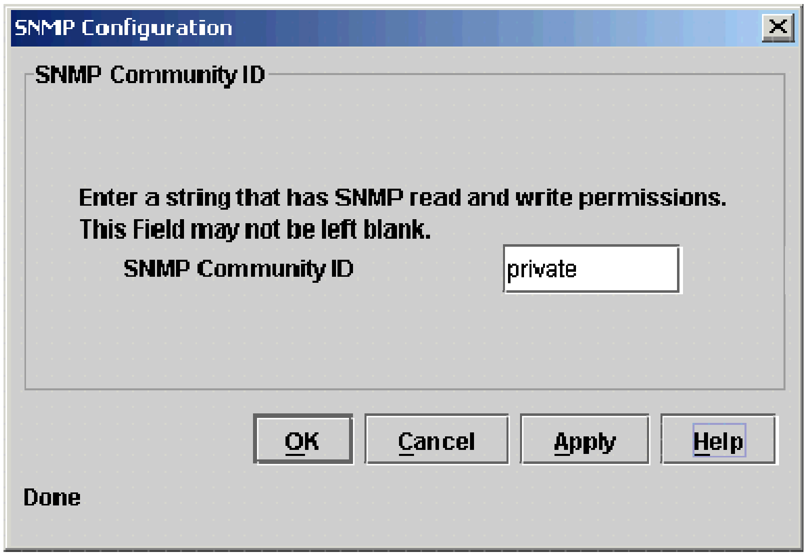
1. Select **Edit** > **Options** from VoIP Monitoring Manager Server. The Server Options dialog displays.
2. Click the Data Storage tab, RTCP tab, or Configuration Messaging tab to select settings and type values.

SNMP Settings Dialog

The SNMP dialog contains the Community ID field, which is an RTCP Monitor property as defined for your Windows SNMP Agent. The SNMP dialog allows you to configure the community IDs to be used so that the server can communicate with the SNMP agent.

The SNMP Community ID must have read and write privileges. To check this setting or create other IDs, refer to Check for Valid Community ID.

For more information about the SNMP dialog, click the Community ID field on the following image.



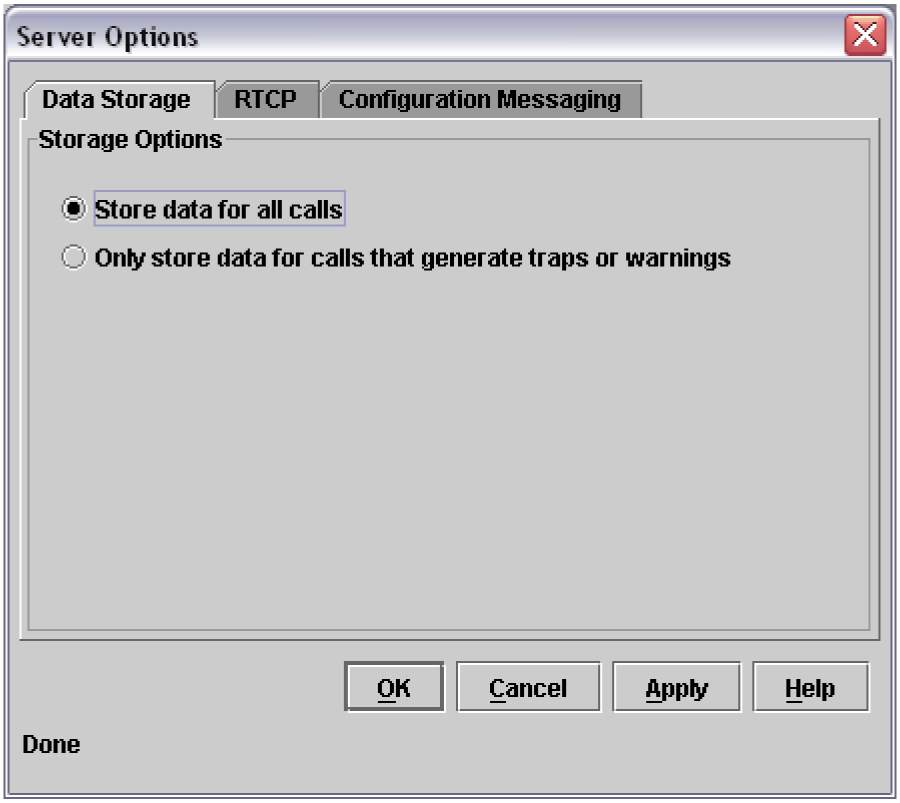
Enter a string that has SNMP read and write permissions.
This Field may not be left blank.

SNMP Community ID: private

Data Storage Tab

The Data Storage tab allows you to configure data storage options.

For more information about the Data Storage tab, click the Storage Options area on the following image.



Storage Options

● Store data for all calls

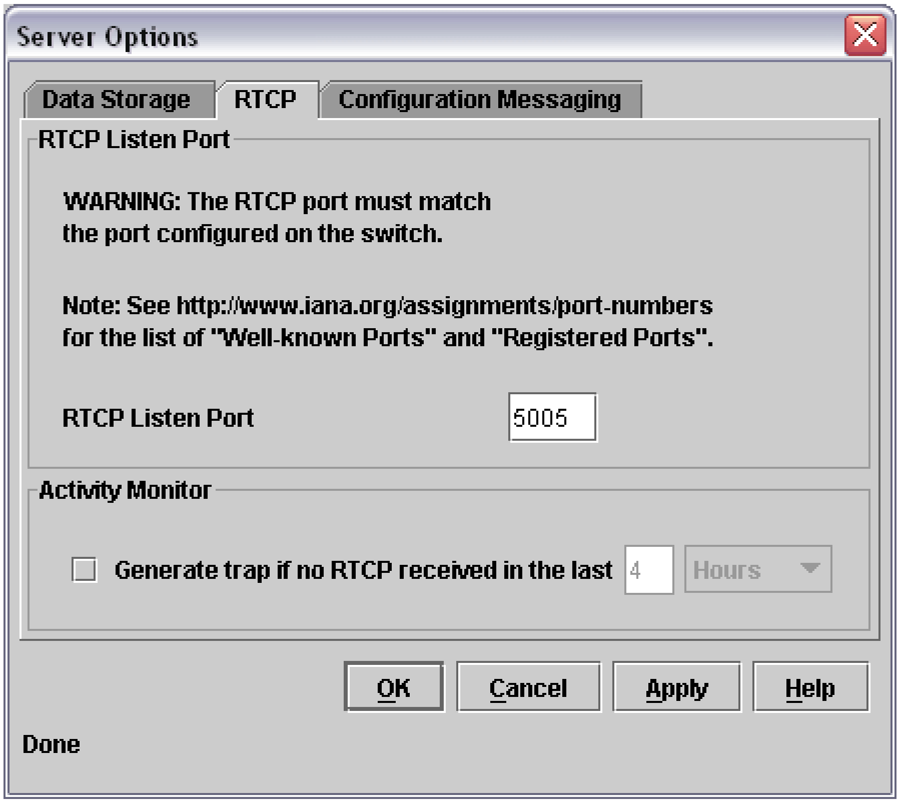
○ Only store data for calls that generate traps or warnings

Done

RTCP Tab

The RTCP tab contains the RTCP Listen Port field that matches the port configured in the telephony Switch Administration Forms (SAT). You can also configure the RTCP listen port and generate a trap based on inactivity.

For more information about the RTCP tab, click the Listen Port and Activity Monitor fields on the following image.



Server Options

RTCP Listen Port

WARNING: The RTCP port must match the port configured on the switch.

Note: See http://www.iana.org/assignments/port-numbers for the list of "Well-known Ports" and "Registered Ports".

RTCP Listen Port: 5005

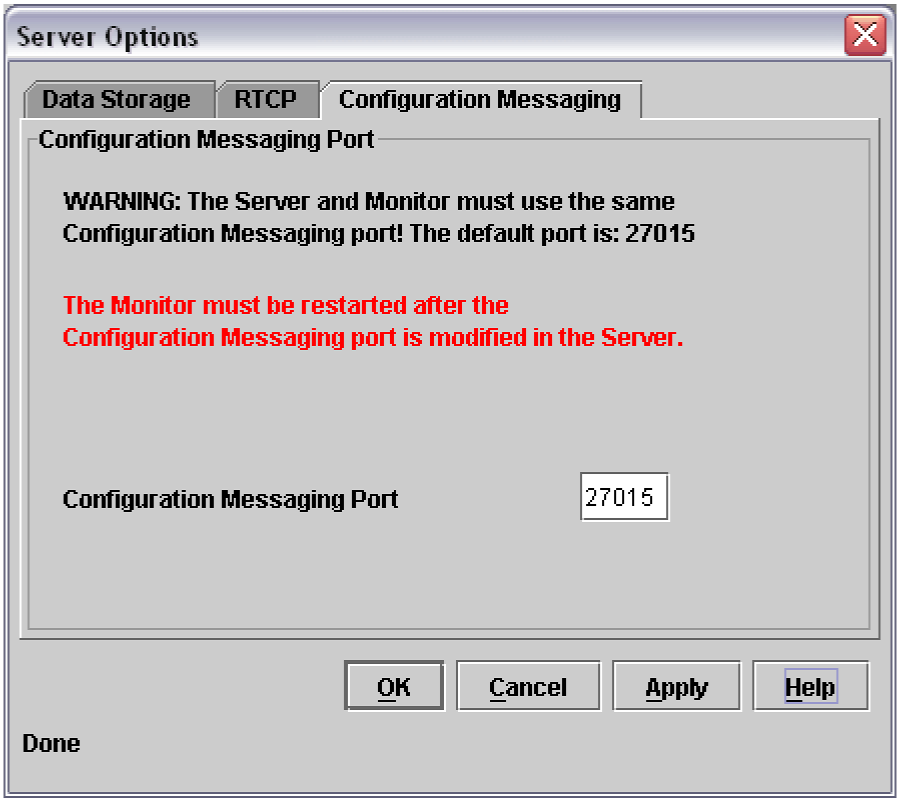
Activity Monitor

□ Generate trap if no RTCP received in the last 4 Hours

Done

Configuration Messaging Tab

The Configuration Messaging tab contain the Configuration Messaging Port field. The server and monitor must use the same Configuration Messaging port.



WARNING: The Server and Monitor must use the same Configuration Messaging port! The default port is: 27015

The Monitor must be restarted after the Configuration Messaging port is modified in the Server.

Configuration Messaging Port 27015

Done

See Also

Check for a Valid Community ID

Components of VoIP Monitoring Manager

VoIP Monitoring Manager Server Error Messages

About RTCP Monitor

The RTCP monitor collects the RTCP packets sent from the AVAYA™ endpoints and stores the information in a proprietary database. The RTCP monitor also runs as a sub-agent of the Windows SNMP agent. All the information contained in the database can be queried through SQL.

The specifications for querying the database are found in:

- The RTP MIB. The reference is located at http://www.ietf.org/rfc/rfc2959.txt
- The proprietary AVAYA-VMON-MIB (The ASN.1 definitions of this MIB and associated traps are included as text files in the installation)

See Also

VoIP Monitoring Manager Options

Components of VoIP Monitoring Manager

Starting the VoIP Monitoring Manager

Components of RTT

RTT can comprise the following four components:

- **Propagation delay:** The time it takes for a packet to travel across the network from sender to receiver. This variable is based on the speed of light and the distance the signal must travel. For example, the propagation delay between Singapore and Boston is much longer than the propagation delay between New York and Boston.
- **Transport delay:** The time it takes to traverse the network devices along a transmission path. Networks containing many routers, firewalls, congestion and low-speed WAN services, for example, introduce more delay than an overprovisioned LAN on a single floor of a building.
- **Packetization delay:** The time it takes for a compressor/decompressor (codec) to digitize an analog signal, build frames and then reverse the process at the other end. The G.729 codec has a higher packetization delay than the G.711 codec.
- **Jitter buffer delay:** The delay introduced by the receiver while it holds one or more packets to reduce variations in packet arrival times.

See Also

Troubleshooting

Interpreting the Values Using Summary Reports or Detailed Reports

Activity Monitor

Provides the ability to monitor RTCP activity for a set number of minutes, hours, or days. A trap is generated when no activity is received within the specified time period. The number must be from 1 through 99.

The check box is cleared with a setting of 4 hours, as a default setting.

About the Database

By default, all data sent to VoIP Monitoring Manager via RTCP from the endpoints is stored in the database. You can run reports against this data or export it for use in other programs, such as spreadsheets. Depending on the number of monitored terminals and the trap settings, the repository of data can become substantial.

VoIP Monitoring Manager is supplied by default with an MSDE database, which has a maximum size of 2 GB per database. You can migrate to an SQL Server database.

If you are using an MSDE database, the historical data is stored for 30 days in the database. After 30 days, the data will be deleted.

If you are using an SQL Server database, the historical data is stored for 100 days in the database. After 100 days, the data will be deleted .

If you need access to historical data, you must either backup the database or export reports that include the required data.

See Also

Database Schema

Entity Relationship Diagram

Data Storage Limits and Management

If you are using an MSDE database, the historical data is stored for 30 days in the database. After 30 days, the data will be deleted.

If you are using an SQL Server database, the historical data is stored for 100 days in the database. After 100 days, the data will be deleted .

See Also

About Summary Reports or Detailed Reports

Interpreting the Values Using Summary Reports or Detailed Reports

Storage Options

Store data for all calls

Records information for all calls identified by Avaya VoIP Monitoring Manager.

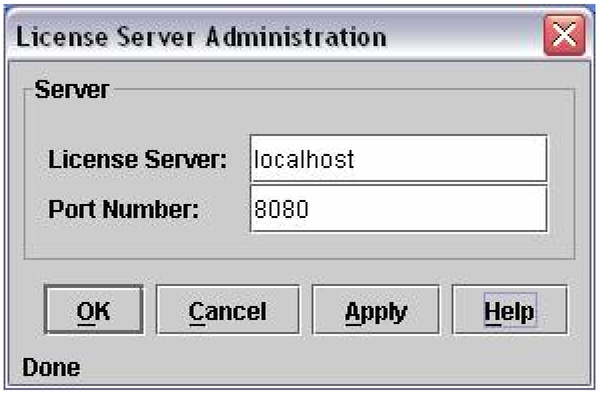
Only store data for calls that generate traps or warnings

Records information only for calls where the QoS levels result in a trap or warning as per the traps configurations. This is the default setting in the VoIP Monitoring Manager Server.

Data can still be viewed while a call is active.

License Server Administration Dialog

Enables you to log into the WebLM server that manages your Avaya licenses. The license server is required to activate VoIP Monitoring Manager beyond the 90-trial period. If you do not have a license to use VoIP Monitoring Manager, you can use the software for a 90-day trial period.



License Server Administration

Server

License Server: localhost

Port Number: 8080

Done

License Server

Enter the IP address of the WebLM server.

Port Number

Enter the port number.

Click the **OK** button to connect to the license server.

If you click the **Cancel** button, you will be able to start VMM, but you will only be able to use it for 90 days. The Status Bar area will indicate that VMM is operating in Evaluation mode and display the number of days remaining.

See Also

Connecting to the License Server

About Licenses

About Dialog

This dialog box shows

- the version of VMM
- the current license state (that is, whether you are using a valid license or you are running VMM in evaluation mode)
- the number of licenses purchased
- the number of phones at the local server. This number represents the phones that reported to VMM in the last 28 days. This number will increase if you move phones (for example, change extensions or IP addresses). In this case, these phones appear to be new endpoints to VMM. Since there is a 30-day grace period, this will not be a problem.
- the number of phones at the local server that exceed the license (that is, the number of phones that are unlicensed). If greater than zero, this number is displayed in red. This can occur if you have only one monitor connected to the WebLM License Server, and you have more phones stored in the database than licenses purchased.
- the number of media gateways at the local server. This number represents the media gateways that reported to VMM in the last 28 days.
- the number of media gateways at the local server that exceed the license (that is, the number of media gateways that are unlicensed). If greater than zero, this number is displayed in red. This can occur if you have only one monitor connected to the WebLM License Server, and you have more media gateways stored in the database than licenses purchased.

Avaya provides a 90-day trial version of VoIP Monitoring Manager. After 90 days, VoIP Monitoring Manager stops collecting RTCP data. You have the option of purchasing the VoIP Monitoring Manager license key. This key is required to fully activate the VoIP Monitoring Manager beyond the 90-day trial period. When a license key is purchased, an instance of WebLM License Server is required to manage the license key. If you do not have a license to use VoIP Monitoring Manager, you can use the software for a 90-day trial period.

See Also

About Licenses

Getting Started with VoIP Monitoring Manager (Server)

Starting VoIP Monitoring Manager

You need to ensure that the VoIP Monitoring Manager (VMM) Server is installed and running on the network before you start the VMM Client. If you only have the VMM Server installed, you can also start the VMM Client as a Web Client.

VoIP Monitoring Manager Server cannot be run unless a database is installed and configured properly.

To Start VoIP Monitoring Manager as an Application

1. From the machine with the VoIP Monitoring Manager Server, select **Start > Programs > Avaya > VoIP Monitoring Manager > Server**. The VoIP Monitoring Manager Server starts.

2. From the machine with the VoIP Monitoring Manager Client, select **Start > Programs > Avaya > VoIP Monitoring Manager > Client**. The VoIP Monitoring Manager Client starts.

Now you can search for endpoints and then view the QoS data in a report format.

> ℹ If the VoIP Monitoring Manager Server has difficulty connecting to the Windows SNMP Agent, check the Windows SNMP Agent is installed and running.

See Also

Connect to Database

Run a Search

View a Report

How to Use VoIP Monitoring Manager Client

About Detailed Reports and Summary Reports

Interpreting the Values Using Detailed Reports and Summary Reports

Starting VoIP Monitoring Manager Web Client

The Avaya VoIP Monitoring Manager Client can run as a Web application in a browser. This is useful if you only have the server installed. To run the Avaya VoIP Monitoring Manager Client as a Web application, the following requirements must be met:

- The PC on which the Avaya VoIP Monitoring Manager Server software is installed must be running a Web server. The Apache Web server is automatically installed on the server when the Avaya VoIP Monitoring Manager Server software is installed.
- The Web server must be configured to publish the file to the following VoIP Monitoring Manager installation path:
  C:\Program Files\Avaya\VoIP Monitoring Manager\jars\ClientApplet.htm
- The PC you will use to access the Avaya VoIP Montoring Manager Server must be able to connect to the VMM server via a Web browser and have the following software installed:
  - Microsoft Internet Explorer 6 or later
  - SUN Java 2 Runtime Environment, SE v1.4.2_06

For more information see the topic About the VoIP Monitoring Manager Web Client

To Start Web Client

- From your browser, type in the following url:

```
Http://VMMServerMachineName/VoIPMonMgr/ClientApplet.html
```

VMMServerMachineName = the machine running the VMM Server. This url points to the machine running the VMM Server.

If you do not have the Sun Java Plug-in installed, you are prompted to install it.

To exit the Web Client, just close the browser.

> There are limitations in using the VMM Web Client. These are imposed by the security restrictions associated with running unsigned applets. The limitations are:
>
> - You can only access one monitor that is directly connected to the server running the VMM Server.
> - You cannot connect to a new server or use the Copy functionality.

See Also

Components of VoIP Monitoring Manager

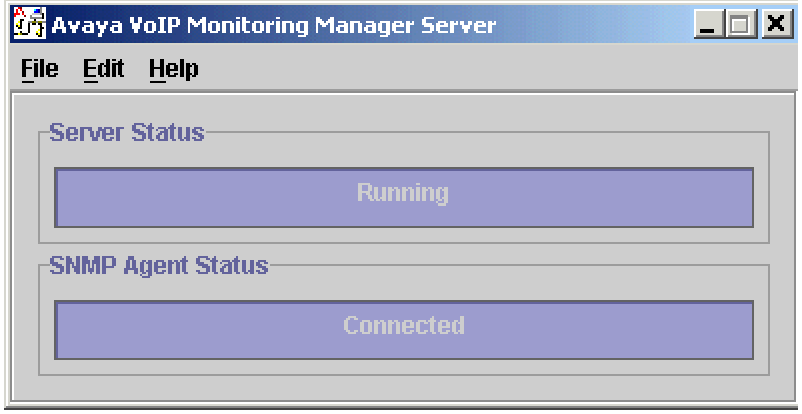
Web Client Displays an Incorrect Time

Monitoring Server Status

When you start the VoIP Monitoring Manager Server, you will see the Server status bar and Windows SNMP Agent status bar. When the Server is running, you will see the **Server Status** bar completely filled in. When the Windows **SNMP Agent** is connected you will also see the SNMP Agent Status bar completely filled in.

From the VoIP Monitoring Manager Server you can:

- Connect to RTCP Monitor
- Edit VoIP Monitoring Manager Options
- Generate Traps



See Also

Components of VoIP Monitoring Manager

Start the VoIP Monitoring Manager Server

VoIP Monitoring Manager Server Error Messages

Connect to RTCP Monitor

The Connect to RTCP Monitor enables you to (re)-establish the SNMP connection to the RTCP Monitor. When the VMM Server starts it automatically attempts to establish a connection with the RTCP monitor. If the SNMP connection is lost at any time, the Connect to RTCP Monitor menu enables to enable manually re-establishment of the connection.

See Also

About VoIP Monitoring Manager Server

VoIP Monitoring Manager Server Status

Changing the RTCP Listen Port

The RTCP Listen Port is the configurable port that is used to collect the AVAYA™ endpoints. The number must be from 1 through 65535. The default port is 5005.

> Changing the RTCP port will result in a warning that the RTCP port must match the port configured on the AVAYA™ voice system. For more information see http://www.iana.org/assignments/port-numbers and your AVAYA™ Call Processing or Switch Administration Forms (SAT).
>
> You will also need to enter a Windows SNMP Agent Community ID with write access (default: private). It is very unusual to change the listen port, as the default of 5005 should work in most situations.

Connecting to the License Server

The Connect to License Server option in the File menu enables you log into the WebLM server that manages your Avaya licenses. If the license server was not configured during installation, you are prompted to connect to the license server the first time you start the VMM Server.

To connect to the license server:

1. From the File menu, select **Connect to License Server**. The License Server Administration dialog box appears.
2. In the License Server box, enter the IP address of the WebLM server.
3. In the Port Number box, enter the port number.
4. Click the **OK** button.

If you click the **Cancel** button, you will be able to start VMM, but you will only be able to use it for 90 days. The Server Status area will indicate that VMM is operating in Evaluation mode and display the number of days remaining.

See Also

License Server Administration Dialog

About Licenses

Generating Traps & Alarms (Server)

Generating Traps & Alarms

You can set rules to generate Traps that notify you when the VoIP network QoS parameters have reached unacceptable levels. You define the rules in the Trap dialog, which has a tab for Call Traps and a Tab for System Traps. You open the Trap dialog from the VoIP Monitoring Manager Server **Edit > Trap Settings**.

You can set more than one rule for each type of trap, and each rule can be made up of more than one condition. When a rule has more than one condition, they have a logical AND relationship, i.e. they must all be satisfied before a trap is sent.

The RTCP Monitor generates a Trap to a pre-configured Trap Manager when the RTCP Monitor experiences the conditions defined. The Trap Manager is generally configured to be the Gateway Alarm Manager (GAM) or Network Alarm Manager (NAM) but any Trap Manager application can be used. Traps can be set for Calls (Sessions), Systems (Networks), and Terminals (endpoint).

VoIP Monitor Manager creates alarms (traps) based on two sets of rules:

- Call Alarms. If a specified condition occurs anywhere in the system, a trap is sent immediately.
- System Alarms. The specified condition must occur a specified number of times before a trap is sent. This is based on an accumulation of warnings from the entire system.

See Also

Configure SNMP Service for Sending Traps

Recommended Alarm Settings

Recommended Trap Settings

Values that you use to trigger alarms must be fine-tuned to suit your environment. Appropriate settings may vary greatly from one country to another.

The default settings that are in place when VoIP Monitoring Manager is installed are a useful starting point. These settings are based on an environment with high-quality telecommunications facilities. For example, it is reasonable to expect RTT of less than 300.

Severity	**Jitter**	**Delay**	**% loss**
MAJ	60	0	0
MAJ	0	500	0
MAJ	0	0	50
WRN	45	0	0
WRN	0	0	4.0

System warning interval: 100 warnings, 24 hours

Terminal warning interval: 50 warnings, 24 hours

A dialog with the recommended major alarm settings is shown in Call Traps.

A dialog with the recommended warning alarm settings is shown in System Traps.

Call Traps

A Call Trap (also referred to as a Call Alarm) is where a Trap has been triggered because a customer's Call (Session) has reached one of the pre-defined QoS parameter's thresholds.

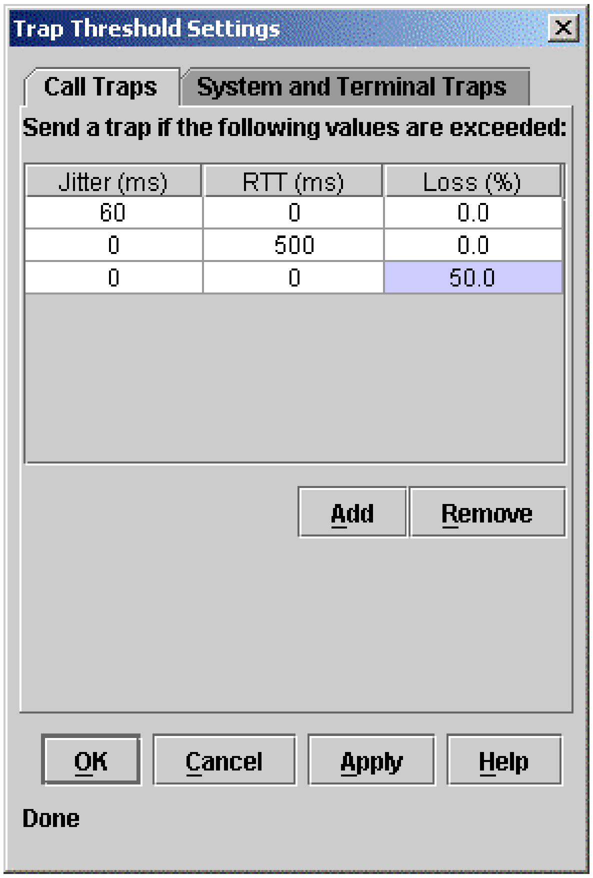
At the end of a call, the RTCP Monitor checks its Trap configurations and generates an alarm to a pre-configured Trap Manager. The conditions for the Trap are defined in the Trap dialog.

The system alarm can be based on any combination of jitter, delay (RTT) or packet loss.

Example

This example shows values entered into the Trap dialog. These values would result in a trap being sent at the end of the call, if at any time during the call the jitter >=60, or the delay >= 500 or the %loss >= 50. If the conditions in any one line are met then the following lines are not read. This is done to ensure that the number of traps sent for a given call is not greater than one.

Click the tabs and columns in the image for more information.



Send a trap if the following values are exceeded:

Jitter (ms)	RTT (ms)	Loss (%)
60	0	0.0
0	500	0.0
0	0	50.0

Also

Generating Traps & Alarms

System Alarms

Terminal Alarms

Configure SNMP Service for Sending Traps

System Traps

A System Trap (also called a System Alarm) is where a Trap/Alarm has been triggered because the number of Warnings has exceeded the defined threshold. The Trap is defined in the Trap dialog.

A trap can be defined for the total number of warnings detected on the system, or the total number of warnings detected on an individual terminal. Each trap has a specified interval during which the number of warnings must be accumulated.

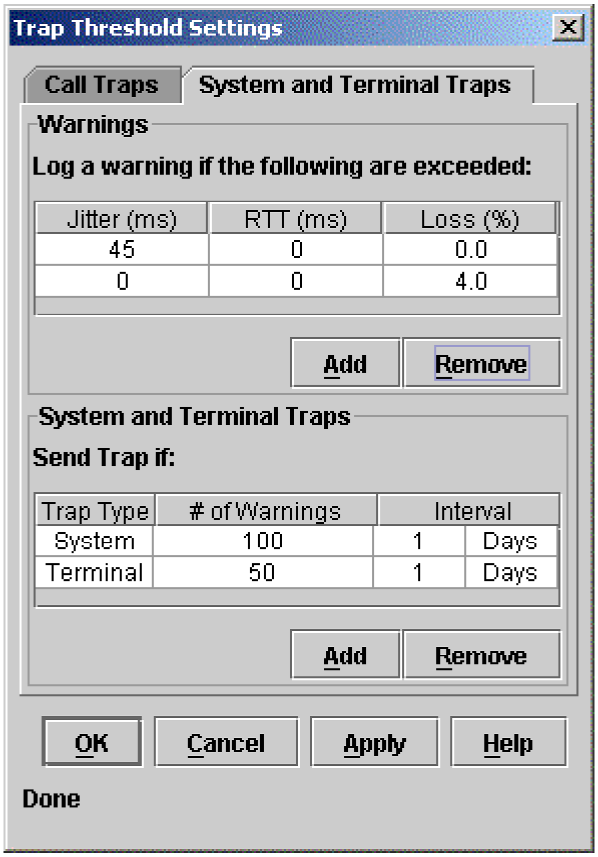
The RTCP Monitor periodically checks to see if the defined interval has expired. It counts the number of warnings recorded during this interval. If it has reached the defined threshold then a System Alarm is generated. To generate an Alarm as soon as the thresholds are reached, use an interval of zero (0).

The system alarm can be based on any combination of jitter, delay (RTT) or packet loss.

Example

This example shows values entered into the Trap dialog. These values would result in a warning being logged at the end of the call, if at any time during the call the jitter >=45, or the %loss >= 4. If the number of warnings logged in any 24-hour period exceeds 100, as defined in the **System's No# of Warnings** column, then a system trap is sent.

Click the tabs in the image for more information.



Warnings

Log a warning if the following are exceeded:

Jitter (ms)	RTT (ms)	Loss (%)
45	0	0.0
0	0	4.0

System and Terminal Traps

Send Trap if:

Trap Type	# of Warnings	Interval	
System	100	1	Days
Terminal	50	1	Days

Done

See Also

Generating Traps & Alarms

Call Traps

Terminal Traps

Configure SNMP Service for Sending Traps

Terminal Traps

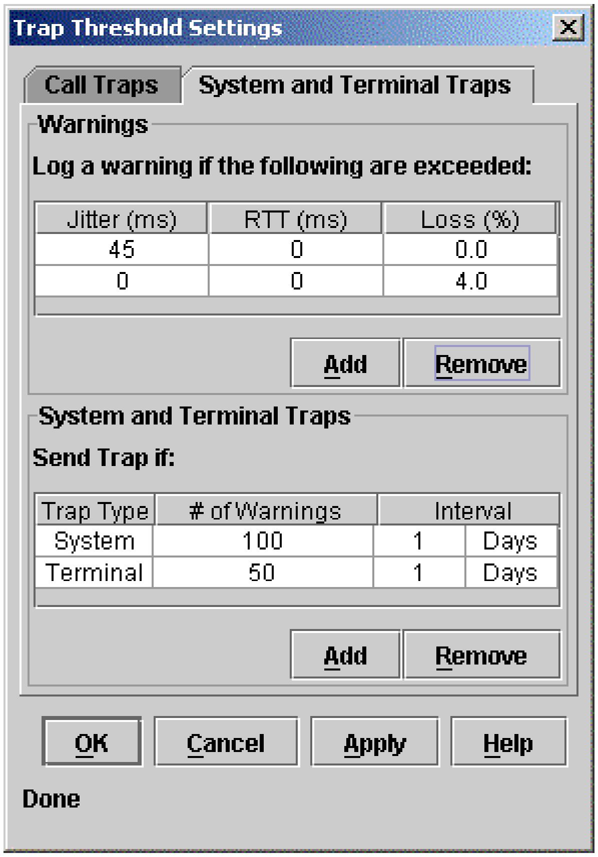
A Terminal Trap (also called a Terminal Alarm) is where a trap has been triggered because the number of Warnings for any one terminal (endpoint) has exceeded the defined threshold. The Trap is defined in the Trap Dialog. You can set Traps for each of the QoS parameters for Calls (Sessions), as well as thresholds for Systems (Networks), and Terminals (endpoint) in the Trap dialog.

The RTCP Monitor checks to see when the defined interval expires. It counts the number of warning traps for a specific IP endpoint. A terminal trap is sent when the number exceeds the specified number in the defined interval. To generate an Alarm as soon as the thresholds are reached, use an interval of zero (0).

Example

This example shows values entered into the Trap dialog. These values would result in a warning being logged at the end of the call, if at any time during the call the jitter >=45, or the %loss >= 4. If the number of warnings logged in any 24-hour interval, against a single endpoint (IP Address) exceeds 50, then a Terminal Trap is sent for that endpoint.

Click on the tabs or columns in this example to see more explanations.



Warnings

Log a warning if the following are exceeded:

Jitter (ms)	RTT (ms)	Loss (%)
45	0	0.0
0	0	4.0

System and Terminal Traps

Send Trap if:

Trap Type	# of Warnings	Interval	
System	100	1	Days
Terminal	50	1	Days

Done

See Also

Generating Traps & Alarms

Call Traps

System Alarms

Configure SNMP Service for Sending Traps

Troubleshooting

Troubleshooting

Use this section of help to look for solutions to common problems.

See Also

Error Messages

Components of VoIP Monitoring Manager

About Detailed Reports or Summary Reports

Interpreting the Values Using Detailed or Summary Report

License Problems

If the About dialog box indicates that you have exceeded the number of licenses, the following conditions may have occurred:

- You moved phones (for example, changed extensions or IP addresses). Moving phones will increase the number used licenses. In this case, these phones appear to be new endpoints to VMM. Since there is a 30-day grace period, and the endpoint count consists of the last 28 days, this will not be a problem.
- You need to purchase additional VMM licenses. Contact your authorized Avaya Sales Representative.

Each VMM RTCP monitor periodically checks the number of endpoints it knows about and requests/renews the licenses for them. If there is more than one RTCP monitor and the total number of endpoints known exceeds the number of licenses, the RTCP monitor that requests licenses first will get its licenses. The RTCP monitor that requests licenses last will be denied licenses. If you enter the 30-day grace period because license limits were exceeded, the About dialog box will appear every time the VMM Server and VMM Client are started. If you exceed the 30-day grace period, VoIP Monitoring Manager stops collecting RTCP data.

See Also

About Licenses

Client Error Messages

Client Error Messages

This part of help lists some common Client error messages that may occur as a result of mis-configuration or incorrect usage.

See Also

Components of VoIP Monitoring Manager

Troubleshooting

About Detailed Reports or Summary Reports

Interpreting the Values Using Detailed or Summary Reports

Access Error

If you receive the following error message you will need to change the java.policy file using the policy tool provided by SUN. The java.policy file is located in the directory where you installed AVAYA™ VoIP Monitoring Manager. Experienced Administrators should only make changes to this file.

This VoIP Monitoring Manager Client is not permitted to access hostname. Please update the java.policy file to give this client the necessary permission you will need to restart the client or select another host.

See Also

Troubleshooting

Graph Limit Reached

If you receive the following error message then the number of reports opened has reached the VoIP Monitoring Manager's limit. Only ten reports can be displayed at once. You will need to close some reports.

The reports for the selected endpoints could not be displayed, as the limit on the number of reports displayed would be exceeded. Please close some reports, or select fewer endpoints and try again.

See Also

Troubleshooting

Help Could Not Be Displayed

If you receive the following error message then there are problems displaying the help. You may need to check if the VoIP Monitoring Manager is installed correctly.

The help could not be displayed. Please check that the VoIP Monitoring Manager is installed correctly.

See Also

Troubleshooting

Invalid Bounds

If you receive any of the following error messages then the values entered in the Report Properties dialog is not a valid entry. Check that the value in the left field is less than the value in the right field or in the case for the packet loss field, the value must not be greater than or equal to 100.

> The upper/lower bound must be greater than the lower bound.
>
> The percentage loss upper bound must be greater than the lower bound and less than or equal to **100.**

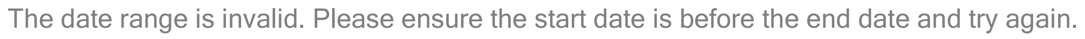
See Also

Troubleshooting

Search Using QoS Values

Invalid Date Range

If you receive this error message then the start date selected in the Search dialog is after the end date. You will need to change the start date or end date in the Search dialog so that the start date is before the end date.



The date range is invalid. Please ensure the start date is before the end date and try again.

See Also

Troubleshooting

About Summary Reports

Invalid Search Parameter

The **Invalid Search Parameter** error message displays if you have entered an incorrectly formatted entry in one or more of the fields in the Search dialog. Follow the suggested examples in the dialog or for more information on correct formatting consult the following topics:

- Search for a Specific Phone Number
- Search for a Specify SIP Username
- Search for a Specific Network Address
- Search Using QoS Values

See Also

Advanced Search Dialog

No Data is Displaying on a Report

There are many reasons why data may not display on the report.

Possible Solutions

- If you are using MSDE, data older than 30 days is removed from the database.
- If you are using SQL server, data older than 100 days is removed from the database.
- Check the VoIP Monitoring Manager Options. You may have an incorrect Windows SNMP Agent Community ID or RTCP Listen Port setting.

See Also

Troubleshooting

Error Messages

About Detailed Reports or Summary Reports

Interpreting the Values Using Detailed or Summary Reports

No Endpoint Data Available

If you receive the following error message then the endpoint whose report is being viewed is not currently active. Wait until the endpoint becomes active again and more data will be displayed, or close the report if you are finished viewing it.

There is no data currently available for this endpoint.

Explanation

This happens when calls are too short to produce reporting data, or the reporting data has been lost.

If the actual call duration is comparable to the reporting period (or shorter than the reporting period), there may be no RTCP packets received. The endpoints normally provide a *reception report*, but in this situation none will be received before the call ends.

Endpoints are identified by data that they send in RTCP packets. Hence if no packet is received, at least one of the session participants cannot be identified. The report shows *unknown endpoint*.

Calls that do not generate one or more RTCP packets are reported as having the default duration of five seconds. The actual call may have been longer – up to 10 or 15 seconds.

Even if one RTCP packet is generated during a short call, it could be lost due to other environmental factors. For example, one participant might have silence suppression enabled, with the packet sent during the suppression period.

See Also

Troubleshooting – No Data is Displaying on a Report

About Detailed Reports and Summary Reports

No Endpoints Matched the Search

If you receive the following error message then it could be due to one of the situations as described:

No endpoint matched the given search.

- There are no endpoints reporting to the RTCP Monitor or the chosen VoIP Monitoring Manager Server
- The calls are active, but since no data is being sent to the RTCP Monitor, the ip-network-region form and the system-parameters ip-options form for the Avaya voice system are not configured correctly.
- There were no endpoints that matched the QoS parameters in the search
- There were no endpoints that matched the search for phone number, SIP username, Network Address, or date range as specified in the Search dialog

Try Broadening Search By:

- Select a different date range in the Search dialog
- Use a more general phone number pattern
- Search for all endpoints instead of just those matching a given phone number, SIP username, or network address

See Also

Run a Search

Search Using QoS Values

Components of VoIP Monitoring Manager

Server Unavailable

If you receive one of the following error messages then the VoIP Monitoring Manager Server has not been started. You must start the VoIP Monitoring Manager Server and verify that the machine you have attempted to connect with is the machine running the VoIP Monitoring Manager Server. If you are using the Web Client, you must refresh your browser to reconnect to the Server.

Not connected to VoIP Monitoring Manager Server.

The VoIP Monitoring Manager Server on [computer name inserted] is not currently available. Please ensure the server is running and try connecting again.

> ℹ If you are running the Web Client, the error message will be slightly different as follows:
>
> ***The Avaya VoIP Monitoring Manager Server is not currently available. Please ensure the server is running and refresh this page in your browser.***
>
> For this situation, check the server is running and refresh the browser page (F9 on you keyboard will refresh for most browsers).

See Also

Troubleshooting

Connect to a New Server

Server Version Error

If you receive the following error message you will need to ensure the VoIP Monitoring Manager Server is running the same version as the VoIP Monitoring Manager Client.

The VoIP Monitoring Manager Server on [computer name inserted] is running an incompatible version. Please select a compatible Server or upgrade the Client and/or Server.

Try

- Check the Host Name Server dialog.
- Check that the version number for the Client is the same for the Server
- From the Client, **Help > About menu**.
- From the Server dialog, click **Help > About menu**. If the version numbers are not the same, you will need to close all browsers and download the correct Server version.

> ℹ If you are running the Web Client, the error message will be slightly different as follows:
>
> ***The VoIP Monitoring Manager Server is an incompatible version. Please close all your browsers and try again.***
>
> For this situation, close all browsers and then retry using the Web Client. This will result in the correct Web Client automatically downloaded from the server.

See Also

Troubleshooting

Connect to New Server

Some Fields Are Blank in the Exported Data

Some fields are blank in the Exported Data because the endpoints did not report the data.

See Also

Export Results List

Export Report Data

Unknown Error

If you receive the following error message then it is important that you contact customer support so that they can help you and the error can be fixed.

An unknown error occurred. Please contact customer support if this error continues.

See Also

Troubleshooting

Web Client Displaying Incorrect Time

The Web Client will display an incorrect time if you have the JRE 1.4.01 installed. It is recommended that you use the Sun JRE 1.4.2_06 that is supplied with the VoIP Monitoring Manager installation.

See Also

Starting the VoIP Monitoring Manager Web Client

Windows SNMP Agent Connection Error

If you receive the following error message then VoIP Monitoring Manager Server is not connected to the Windows SNMP Agent. If you were viewing a report you will need to open another report, or run a search. You may also need to check that the Windows SNMP Agent is installed and running on the VoIP Monitoring Manager or check the VoIP Monitoring Manager Options has a correct SNMP Community ID.

The server could not reconnect to the SNMP Agent. This server will not be able to retrieve data until this issue is resolved. Try doing another search to make the server try to reconnect to the SNMP Agent, or connect to another server.

See Also

VoIP Monitoring Manager Server Error Messages

Components of VoIP Monitoring Manager

Server Error Messages

Server Error Messages

This part of help lists some common Server error messages that may occur as a result of mis-configuration or incorrect usage.

See Also

Check for a Valid Community ID

Installing VoIP Monitoring Manager

VoIP Monitoring Manager Options

Check SNMP Installation

The Simple Network Management Protocol (SNMP) Agent is the Windows SNMP service that runs on your computer. SNMP is a protocol for communications between remote network management stations and managed network elements (such as AVAYA™ devices).

The VoIP Monitoring Manager Server needs the Windows SNMP Agent installed as it enables the RTCP Monitor to collect and publish the data. The Windows SNMP service is provided with the Windows 2000 CD but is not installed by default. You will be prompted during the VoIP Monitoring Manager install to install it from the Windows 2000 CD.

See Also

Check Windows SNMP Agent is Installed and Running

Check for a Valid Community ID

Troubleshooting

Components of VoIP Monitoring Manager

Could Not Resolve Host Name

If you receive the following error messages then the machine running the VoIP Monitoring Manager Server is not correctly configured for TCP/IP. If your IT department cannot resolve this problem, please contact customer support.

```
Error starting Server [text of exception raised inserted] Server exiting.
```

See Also

VoIP Monitoring Manager Server Error Messages

Components of VoIP Monitoring Manager

Excessive Packet Loss

Packet Loss is the result of packets being lost in the transmission from one endpoint to another. When packet loss occurs there could be a drop out of words or partial words in the conversation. At low levels, poor voice quality would result. At high levels, the conversation becomes unintelligible. Packet Loss can result from line congestion.

General Server Error

If you receive the following error messages then you either need to reboot the machine and restart the VoIP Monitoring Manager Server or contact customer support.

```
Unknown error starting server. Try rebooting. Please contact customer support
if this error continues. Server exiting.
```

See Also

VoIP Monitoring Manager Server Error Messages

Components of VoIP Monitoring Manager

Invalid RTCP Port

If you receive the following error messages then the number entered in the RTCP Listen Port field in the VoIP Monitoring Manager Options is not valid. Enter a number in the range of 1 – 65535.

```
Please enter a port in the range 1 to 65535.
```

See Also

VoIP Monitoring Manager Options

VoIP Monitoring Manager Server Error Messages

Components of VoIP Monitoring Manager

Ports used by Server

The following ports are used:

Port	**Function**
161	SNMP Service listens on this port
162	SNMP Trap service listens on this port. Required on the machine running the trap collector (if you are collecting traps).
1099	RMI registry runs on this port
5005	RTCP Listen port. Endpoints send RTCP to the VMM server on this port. If any of the IP endpoints are on the other side of a firewall from the VMM server, the firewall needs to be configured to let these packets through.

See Also

Problems Binding to Port 162

Problems Binding to Port 162

When installing the VoIP Monitoring Manager, the Windows SNMP Service and the Windows SNMP Trap Service are also installed. As the Windows SNMP Trap Service opens Port 162 it is possible that it is bound to it. The Windows SNMP Service is required by the VoIP Monitoring Manager to run the RTCP Monitor but the Windows SNMP Trap service is not required. To prevent the Trap Service from starting automatically and therefore binding to Port 162, set the Trap Service properties to manual at startup.

To Set the Trap Service Startup to Manual

1. From Windows select **Start > Settings > Control Panel**.
2. Double-click **Administrative Tools** to open it.
3. Double-click **Services** shortcut to open it.
4. From Services, scroll down to **SNMP Trap Service** to select it.
5. Right-click **SNMP Trap Services**, select **Properties.**
6. From SNMP Trap Services Properties dialog, click **Stop.**
7. Select **Startup** drop-down arrow and select **Manual**.
8. Click **OK** and close all open folders.

See Also

Troubleshooting

Configure SNMP Service for Sending Traps

RMI Registry Error

If you receive any of the following error messages then the VoIP Monitoring Manager Server is unable to start and you will need to reboot the machine running the VoIP Monitoring Manager Server.

Problem with RMI Registry. Ensure that port 1099 is available. You can do this by rebooting server PC. Server exiting...

Unknown problem with RMI Registry. Try rebooting. Please contact customer support if this error continues. Server exiting…

See Also

VoIP Monitoring Manager Server Error Messages

VoIP Monitoring Manager Options

Set RTCP Port Error

If you receive the following error message then there is a problem setting the RTCP port. You need to consider checking the following as indicated on the error message:

```
Setting the RTCP Port failed.

Please check:

The SNMP community ID has write access

The SNMP Agent is running

The port is not in use by another application
```

See Also

Windows SNMP Agent

VoIP Monitoring Manager Options

Server Cannot Connect to SNMP

This condition is not apparent unless you view the Windows Event Viewer on the server. On a client, it will not be possible to generate reports, but no relevant information is available in the event log.

This condition is caused by incomplete or incorrect installation of the server. The following DLL files cannot be found in c:\WINNT\System32\:

Msvcp70.dll

Msvcr70.dll

Mfc70.dll

To verify that this condition has occurred, look in the System Log section of the Windows Event Viewer for event ID 1102 with the following message:

> SNMP Service is ignoring Extension Agent DLL <path and file name> because it is missing or misconfigured.

If you verify this problem, copy the required DLL files from the installation CD to the required directory.

Correct operation

If the service starts normally, the following information is displayed in Application section of the Window Event Viewer:

- Informational event with ID 500: You are using *RtpMib.dll version 3.0.x*

  (the text shown in italics in this message may vary depending on the version of VoIP Monitoring Manager that is installed.)

- Event Properties with Event ID 500: The Avaya RTCP Monitor has started successfully.

SNMP Service Error

If you receive any of the following error messages then it is possible that the Windows SNMP Agent is not running, or an incorrect SNMP Community ID or an ID without read access is being used. You can restart the VoIP Monitoring Manager Server.

Could not communicate with the SNMP Agent. Please ensure the Agent is running and that the correct Community ID is being used. If further problems are encountered, try running the VoIP Monitoring Manager Server installation again.

SNMP problem encountered. This probably indicates that the SNMP Agent part of the VoIP Monitoring Manager Server installation is corrupted. Please re-run the VoIP Monitoring Manager Server installation again. The VoIP Monitoring Manager Server cannot function correctly until this is fixed. Server exiting...

See Also

Check for a Valid Community ID

VoIP Monitoring Manager Server Error Messages

VoIP Monitoring Manager Options

Server Already Running

If you receive the following error messages then you have tried to open more than one VoIP Monitoring Manager Server on the same machine. Click Ok on the error message dialog to close this dialog and close the second instance of the Monitoring Manager.

There is an instance of the Avaya VoIP Monitoring Manager Server already running.

See Also

VoIP Monitoring Manager Server Error Messages

Unable to establish database connection

This message is displayed when you make an unsuccessful attempt to connect VoIP Monitoring Manager server to a database. Any of the following conditions can cause this error to be displayed:

- The database server name is incorrect (or the IP address is incorrect), or is not accessible on your network.
- The ID is incorrect for the database.
- The password is not correct.

The full message is:

> Unable to establish database connection(s) using specified credentials. Please check the database server name, user name and password.

Windows SNMP Agent is Not Running

If you receive this error message then you will need to check that the SNMP Service is installed and running.

Windows SNMP Agent is Not Running

See Also

VoIP Monitoring Manager Server Error Messages

VoIP Monitoring Manager Options

Reference Information

Characteristics of RTCP

Error data is derived from RTCP as follows:

- RTCP provides support for real-time conferencing for large groups within an Internet, including source identification and support for Gateways (like audio and video bridges) and multicast-to-unicast translators.
- RTCP provides information about Round Trip Time, Jitter, Packet Loss, and other data useful for analyzing voice quality.
- Endpoints transmitting real time data send an RTP stream, which carries the actual data (e.g. audio, video). The endpoints also send a corresponding RTCP stream. For more information see RFC 1889 located at http://www.ietf.org/rfc/rfc1889.txt.

See Also

Components of VoIP Monitoring Manager

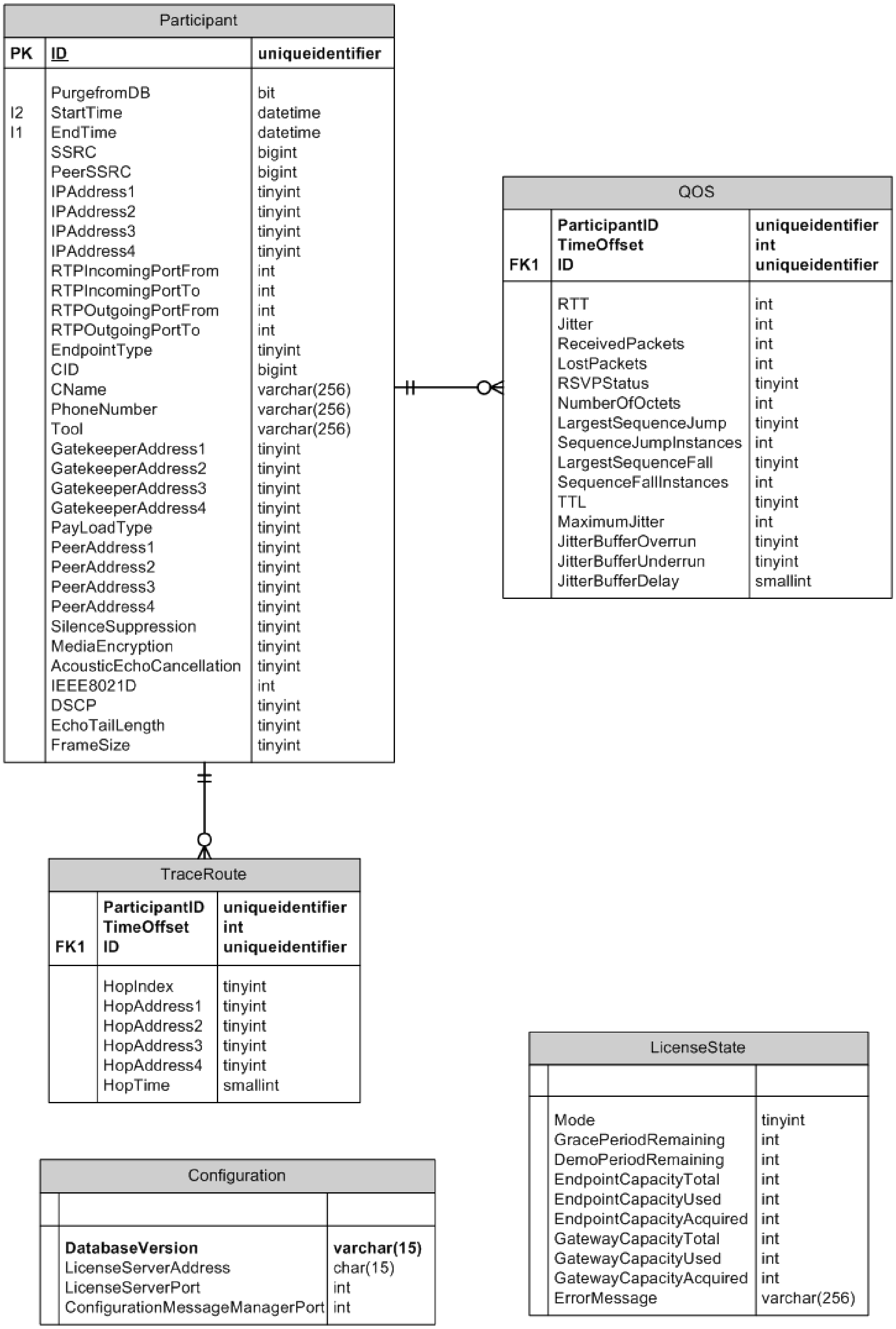
Troubleshooting

Database Schema

```
/**

* Create the Vmm schema.
*/
USE Vmm

GO

/** Drop the Participant table if it already exists. */

IF EXISTS (SELECT * FROM sysobjects WHERE NAME LIKE 'Participant')

DROP TABLE Participant
GO

/** Create the Participant table. */

CREATE TABLE Participant

(

ID uniqueidentifier not null PRIMARY KEY, -- The unique ID of the session participant.
StartTime DateTime, -- Date and time of the first report received.
EndTime DateTime, -- The time the session finishes.
SSRC bigint, -- Synchronization source identifier.

PeerSSRC bigint, -- Synchronization source identifier of the peer.
IPAddress1 tinyint, -- IP Address of the participant for this session (Octect 1).

IPAddress2 tinyint, -- IP Address of the participant for this session (Octect 2).
IPAddress3 tinyint, -- IP Address of the participant for this session (Octect 3).
IPAddress4 tinyint, -- IP Address of the participant for this session (Octect 4).
RTPIncomingPortFrom smallint, -- Port on remote machine from which the RTP stream is
being received.

RTPIncomingPortTo smallint, -- Port on local machine from which the RTP stream is being
sent.
RTPOutgoingPortFrom smallint, -- Port on local machine from which the RTP stream is
being sent.

RTPOutgoingPortTo smallint, -- Port on remote machine from which the RTP stream is being
received.
EndpointType tinyint, -- The type of endpoint.

CName varchar(256), -- The RTP canonical name of the participant.
PhoneNumber varchar(256), -- Phone number of this participant from phone SDES item

Tool varchar(256), -- The TOOL from the TOOL RTCP SDES item
GatekeeperAddress1 tinyint, -- The gatekeeper address for this participant (Octect 1).
GatekeeperAddress2 tinyint, -- The gatekeeper address for this participant (Octect 2).

GatekeeperAddress3 tinyint, -- The gatekeeper address for this participant (Octect 3).
GatekeeperAddress4 tinyint, -- The gatekeeper address for this participant (Octect 4).

PayLoadType tinyint, -- Payload type of received packets.
PeerAddress1 tinyint, -- IP address of peer endpoint (Octect 1).
PeerAddress2 tinyint, -- IP address of peer endpoint (Octect 2).
PeerAddress3 tinyint, -- IP address of peer endpoint (Octect 3).

PeerAddress4 tinyint, -- IP address of peer endpoint (Octect 4).
SilenceSuppression tinyint, -- The Silence suppression metric.
MediaEncryption tinyint, -- The Silence suppression metric.
AcousticEchoCancellation tinyint, -- The acoustic echo cancellation metric.
IEEE8021D smallint, -- The 802.1D metric.
DSCP tinyint, -- The DiffServ Code Point (DSCP) metric.
EchoTailLength tinyint, -- The echo tail length metric.
FrameSize tinyint -- The frame size metric.
)

GO

/** Create the Participant table indexes. */

CREATE NONCLUSTERED INDEX StartDateIndex ON Participant (StartTime)

GO

/** Drop the QOS table if it already exists. */

IF EXISTS (SELECT * FROM sysobjects WHERE NAME LIKE 'QOS')

DROP TABLE QOS
GO

/** Create the QOS table. */

CREATE TABLE QOS

(

ParticipantID uniqueidentifier not null, -- Participant ID that this QoS data applies
to.
TimeOffset int not null, -- Time of the QoS entry from session start.
RTT smallint, -- Round trip time.
Jitter int, -- Jitter.
ReceivedPackets int, -- Count of RTP packets received since the last time an RTCP packet
was received.
LostPackets int, -- A count of RTP packets since the last time an RTCP packet was
received.
RSVPStatus tinyint, -- The RSVP status metric.

NumberOfOctets int, -- The Received RTP Octets metric.
LargestSequenceJump tinyint, -- The Largest sequence jump metric.
SequenceJumpInstances int, -- The number of sequence jump instances metric.
LargestSequenceFall tinyint, -- The Largest Sequence Fall metric.
SequenceFallInstances int, -- The number of sequence fall instances metric.
TTL tinyint, -- The Time To Live metric.
MaximumJitter smallint, -- The Maximum Jitter metric.
JitterBufferOverrun tinyint, -- The number of jitter buffer over-runs metric.

JitterBufferUnderrun tinyint, -- The number of jitter buffer under-runs metric.
JitterBufferDelay smallint -- The Jitter Buffer Delay metric.
)
```

```
/** Create the QOS table indexes. */

CREATE CLUSTERED INDEX ParticipantID ON QOS (ParticipantID)

GO

/** Drop the TraceRoute table if it already exists. */

IF EXISTS (SELECT * FROM sysobjects WHERE NAME LIKE 'TraceRoute')

DROP TABLE TraceRoute
GO

/** Create the TraceRoute table. */

CREATE TABLE TraceRoute

(

ParticipantID uniqueidentifier not null, -- The participant ID for which the QOS samples
are recorded.
TimeOffset int not null, -- Time offset of the trace route from the session start.
HopIndex tinyint, -- Hop count index.
HopAddress1 tinyint, -- IP Address for the network hop (Octect 1).
HopAddress2 tinyint, -- IP Address for the network hop (Octect 2).
HopAddress3 tinyint, -- IP Address for the network hop (Octect 3).
HopAddress4 tinyint, -- IP Address for the network hop (Octect 4).
HopTime smallint -- Round trip delay to the hop address in milliseconds.

)

/** Create the TraceRoute table indexes. */

CREATE CLUSTERED INDEX ParticipantID ON TraceRoute (ParticipantID)

GO

/** Drop the Configuration table if it already exists. */

IF EXISTS (SELECT * FROM sysobjects WHERE NAME LIKE 'Configuration')

DROP TABLE Configuration
GO

/** Create the Configuration table. */

CREATE TABLE Configuration

(

DatabaseVersion int not null -- Database version number.
)
```

Entity Relationship Diagram



Participant

PK	**ID**	**uniqueidentifier**
	PurgefromDB	bit
I2	StartTime	datetime
I1	EndTime	datetime
	SSRC	bigint
	PeerSSRC	bigint
	IPAddress1	tinyint
	IPAddress2	tinyint
	IPAddress3	tinyint
	IPAddress4	tinyint
	RTPIncomingPortFrom	int
	RTPIncomingPortTo	int
	RTPOutgoingPortFrom	int
	RTPOutgoingPortTo	int
	EndpointType	tinyint
	CID	bigint
	CName	varchar(256)
	PhoneNumber	varchar(256)
	Tool	varchar(256)
	GatekeeperAddress1	tinyint
	GatekeeperAddress2	tinyint
	GatekeeperAddress3	tinyint
	GatekeeperAddress4	tinyint
	PayLoadType	tinyint
	PeerAddress1	tinyint
	PeerAddress2	tinyint
	PeerAddress3	tinyint
	PeerAddress4	tinyint
	SilenceSuppression	tinyint
	MediaEncryption	tinyint
	AcousticEchoCancellation	tinyint
	IEEE8021D	int
	DSCP	tinyint
	EchoTailLength	tinyint
	FrameSize	tinyint

QOS

	ParticipantID	**uniqueidentifier**
	TimeOffset	**int**
FK1	**ID**	**uniqueidentifier**
	RTT	int
	Jitter	int
	ReceivedPackets	int
	LostPackets	int
	RSVPStatus	tinyint
	NumberOfOctets	int
	LargestSequenceJump	tinyint
	SequenceJumpInstances	int
	LargestSequenceFall	tinyint
	SequenceFallInstances	int
	TTL	tinyint
	MaximumJitter	int
	JitterBufferOverrun	tinyint
	JitterBufferUnderrun	tinyint
	JitterBufferDelay	smallint

TraceRoute

	ParticipantID	**uniqueidentifier**
	TimeOffset	**int**
FK1	**ID**	**uniqueidentifier**
	HopIndex	tinyint
	HopAddress1	tinyint
	HopAddress2	tinyint
	HopAddress3	tinyint
	HopAddress4	tinyint
	HopTime	smallint

LicenseState

	Mode	tinyint
	GracePeriodRemaining	int
	DemoPeriodRemaining	int
	EndpointCapacityTotal	int
	EndpointCapacityUsed	int
	EndpointCapacityAcquired	int
	GatewayCapacityTotal	int
	GatewayCapacityUsed	int
	GatewayCapacityAcquired	int
	ErrorMessage	varchar(256)

Configuration

	DatabaseVersion	**varchar(15)**
	LicenseServerAddress	char(15)
	LicenseServerPort	int
	ConfigurationMessageManagerPort	int

Handling Jitter

Removing Jitter

Jitter can result from bad queuing strategies set-up on network equipment. Check your equipment manual for recommended settings. To remove jitter the endpoints need to collect packets and hold them long enough to allow the slowest packets to arrive, allowing them to be played at even intervals in the correct sequence, which causes additional delay.

Jitter Effects

Jitter can create audible voice-quality problems if the variation is greater than 60ms. Symptoms of excessive jitter could be reported as crackling or static. A faulty microphone or other hardware problems can be reported as a similar sound problem to jitter but they are not related. You need to rule out that this is not the cause of the problem.

See Also

Troubleshooting

Interpreting the Values Using Summary Reports or Detailed Reports

Interpreting RSVP Status

The RSVP status can change during a session. For example, if the RSVP status for a single endpoint in a session has changed between significant states (such as Failed and Success) then VoIP Monitoring Manager will use the label **Various** to represent this situation. However, if the status has only changed from Pending to Success, then VoIP Monitoring Manager will report Success. Also, the RSVP status can be different for each endpoint in the session. For example, RSVP may be disabled for one endpoint in the session, and enabled for the other.

The RSVP status can be:

Unknown: Information about the RSVP status was not available.

Disabled: The end-point has been configured to ignore RSVP signaling.

Not in Use: RSVP is enabled for use but there is no receiver RTP channel session active, or no attempt has been made by the sender to protect the receiver's RTP channel (i.e. no Path message has been received).

Reservation Pending: This state indicates that the receiver has responded to the first Path message it has received since the call started with a Resv message, and is waiting for a ResvConf to confirm the reservation is installed.

Reservation Failed: This state indicates that the receiver has had a reservation fail or timeout, or an existing reservation was torn down prematurely.

Reservation Success: This state shows that the receiver’s receiving RTP channel is protected by an installed RSVP reservation. Ideally this reservation will need to be successfully refreshed until the RTP session ends.

Various: The RSVP status for a single endpoint in a session has changed between significant states (such as Failed and Success).

Interpreting Terminal Names

The canonical name or CNAME is the unique identifier for each participant within one RTP session, or set of related RTP sessions.

The format is user@host, or host if a user name is not available as on single-user systems. For both formats, host is either the fully qualified domain name or IP address of the host from which the real-time data originates.

For Avaya VoIP systems CNAMEs are of the format:

IP Telephone	`ext<extension>@<IP address>`
IP Softphone	`ext<extension>@<IP address>`
Gateway Board	`gwp@<IP address>`
Gateway Box	`gwt@<IP address>`

See Also

Export Results List

Some Fields are Blank in the Exported Data

SNMP Community ID

An authentication ID allowing read and/or write access to SNMP information. This is set as part of the VMM Server configuration. A single field is used to set both the SNMP Read Community ID and the SNMP Write Community ID.

A community ID with both read and write privileges must be available to VoIP Monitoring Manager (via the SNMP dialog). When creating the community ID, ensure that it has both read AND write privileges

SNMP Read Community ID

The read ID is necessary for obtaining information from the agent, for example, client queries and existing configuration settings. The read ID must match the ID defined in the Windows SNMP Service Properties dialog.

SNMP Write Community ID

The read ID is necessary for obtaining information from the agent, for example, client queries and existing configuration settings. The read ID must match the ID defined in the Windows SNMP Service Properties dialog.

TTL Considerations

For a number of reasons, packets may not get delivered to their destination in a reasonable length of time. For example, a combination of incorrect routing tables could cause a packet to loop endlessly. A solution is to discard the packet after the packet has been forwarded a certain number of times and send a message to the originator, who decides whether to resend the packet.

The initial TTL value is set, usually by a system default, in a field of the IP packet header with a value in the range 0 to 255. The original idea of TTL was that it would specify a certain time span in seconds that, when exhausted, would cause the packet to be discarded.

Since each router is required to subtract at least one count from the TTL field, the count usually indicates the number of router hops the packet has remaining before it must be discarded. Each router that receives a packet subtracts one from the count in the TTL field. When the count reaches zero, the router detecting it discards the packet and sends an Internet Control Message Protocol (ICMP) message back to the originating host.

VoIP Monitoring Manager reports the TTL value detected by the endpoint for each RTP packet it receives.

Glossary

#

802.1D: 802.1D is reported only if it is enabled.

802.1p: 802.1p is the IEEE endorsed Layer 2 traffic prioritization setting.

802.1Q: The 802.1Q field indicates the Virtual LAN to which this device has been assigned.

A

Acoustic Echo Cancellation: The acoustic echo cancellation metric indicates if an endpoint is configured for full-duplex, half-duplex or acoustic echo cancellation mode. The acoustic echo cancellation metric is an enumerated type metric. The possible values are: 0 = Half-duplex, 1 = Full-duplex, 2 = AEC. There is no acoustic echo cancellation on the VoIP engines. Acoustic echo cancellation is a feature for IP phones only.

Alarm: A Trap or Alarm is a message sent by a Windows SNMP Agent to a Trap Manager, console, or terminal to indicate the occurrence of a significant event, such as a specifically defined condition or a threshold that was reached. It is also referred to as an Alarm. The Trap Manager is typically configured to be the HP OpenView or Avaya Network Management Console but any Trap Manager application can be used with the AVAYA VoIP Monitoring Manager.

Apache: Apache HTTP server is an open-source HTTP server that is maintained by the Apache Software Foundation. A free download is available from http://www.apache.org. Follow the links to the HTTPD (HTTP daemon, web server). Note that Apache is installed as part of the Integrated Management Windows Server.

AVAYA-VMON-MIB: The AVAYA-VMON-MIB is used for the storage of VoIP Monitoring Manager trap configuration. (The ASN.1 definitions of this MIB and associated Traps are included as text files in the installation.)

C

Canonical Name: The canonical name or CNAME is the unique identifier for each participant within one RTP session, or set of related RTP sessions. The format is user@host, or host if a user name is not available as on single-user systems. For both formats, host is either the fully qualified domain name or IP address of the host from which the real-time data originates. For Avaya VoIP systems CNAMEs are of the format: IP Telephone: ext<extension>@<IP address>, IP Softphone: exs<extension>@<IP address>, Gateway Board: gwp@<IP address>, Gateway Box: gwt@<IP address>.

Child Endpoint: The terms parent and child endpoints are purely for describing the way endpoints are displayed in the Results List. A parent is like the branch in a tree view. A child is like a leaf in a tree view. The same endpoint can be shown as both a parent and a child. Click on the expanding icon positioned in the far left column of the Results List to expand the tree which displays a sub list with the child endpoints. A child endpoint represents a session between itself and its parent. This is different from a parent endpoint that just represents a physical endpoint.

CLAN: The CLAN is an IP interface (LAN interface) on an Avaya media server and provides control signalling to IP phones, Softphones, and other media gateways.

CNAME: Refer to Canonical Name.

Codec: A Codec is an encoder/decoder. In the context of RTP, it is the type of encoding used for the payload of the RTP packets exchanged as part of a conversation. For example, some RTP Codecs are G.723, G.711 aLaw and G.729. Session Properties shows which Codec is in use. RTP does not distinguish between different sub-types of codec (such as g729A and g729B).

D

Differentiated Services Code Point: The DiffServ Code Point (DSCP) metric represents the value of the IP DSCP field of the incoming RTP packets. The DSCP metric is a number in the range 0-63 and is used to specify the level of service a packet should receive whilst traversing the network.

DSCP: Refer to Differentiated Services Code Point.

E

Echo Tail Length: The echo tail length metric represents the length of echo cancellation processing determined by the distance between the gateway and the endpoint. The echo tail length metric is represented in milliseconds and can have typical value ranging from 8ms to 32ms.

Endpoint Type: The Results List displays an image representing the endpoint type in the left-hand column as follows: IP Phone - Standalone desk phone with a dedicated Ethernet dual hub, its own screen, handset, dial pad and feature access buttons; Soft Phone - Software only phone which is installed on any PC running the Windows operating system; Media Gateway - a network VoIP device.

EndTime: The EndTime column in the exported file displays the date and time the session ended. This column appears in the Session Table of the exported file.

F

Framesize: Frame size is the logical units into which data is partitioned for processing. In the case of a voice coder/decoder (codec) this is the time sliced blocks used by the codec algorithm. For example, the G.729 codec breaks the input audio signal into 10ms blocks for encoding purposes. Therefore, if the RTP packet payload is in 30ms blocks then there are 3 frames per packet. VoIP Monitoring Manager displays the framesize in the Session Properties tab of the report dialog.

G

Gatekeeper: The Gatekeeper column in the Session Table displays the media server or CLAN that controls the endpoint.

Gateway: A Gateway is generally used as a bridge between signaling protocols and bearer media. In this context, the Gateways allow IP endpoints to communicate with non-IP endpoints (e.g. the traditional circuit switched world of analogue and digital phones). AVAYA Gateways also perform the task of mixing the media channels in a conference call. A pair of Gateways can also be set up as an IP trunk.

H

HopAddress: The Hop Address column in the Trace Route Table is the IP address of each network node in the trace route.

HopCount: The HopCount column in the Trace Route Table indicates the hop number, that is, the position in the path node of the trace route.

HopTime: The HopTime column in the Trace Route Table displays in milliseconds the round-trip-time of the trace route packet, from the source to each path node in the trace route.

I

Interval: The period during which the specified number of warnings must be received to trigger an alarm (trap).

J

Jitter: Jitter is a measure of variance in the time it takes for communications to traverse from the sender (application) to the receiver, as seen from the application layer, or the difference between when a packet is supposed to be received and when it is actually received. Jitter is sometimes described as the statistical average variance in delivery time between packets or datagrams. Avaya VoIP Monitoring Manager reports Jitter in milliseconds.

Jitter Buffer Over Runs: The number of jitter buffer over-runs metric represents the number of times during a call the actual jitter exceeded the maximum size to which the jitter buffer is allowed to grow. This metric is an 8-bit unsigned integer.

Jitter Buffer Under Runs: The number of jitter buffer under-runs metric represents the number of times during a call the jitter buffer became empty or starved. This metric is an 8-bit unsigned integer.

L

Largest Sequence Fall: The Largest Sequence Fall metric represents the number of packets that are received later than expected, that is, after a higher-numbered packet was received. For example, if five packets arrive in the order 1, 2, 5, 3, 4, the largest sequence fall is 2 (generally indicating that 2 packets arrived later than expected). Note: A value of 0xFF implies that there were too many packets out of order to be able to calculate the correct value.

Largest Sequence Jump: The Largest Sequence Jump metric represents the maximum number of consecutive packets lost in the last RTCP reporting interval. It is based on sequence numbers assigned to packets as they are created. For example, when the following packet sequence numbers 1,2,3,8 are received, the largest Sequence Jump is 4. Note: A value of 0xFF implies that there were too many packets lost to be able to calculate the correct value.

LargestSeqFall: Refer to Largest Sequence Fall.

LargestSeqJump: Refer to Largest Sequence Jump.

M

Maximum Jitter: The Maximum Jitter metric represents the maximum value of jitter seen in the RTCP reporting interval. This metric would be useful to identify transient spikes of jitter in a session. This metric is a 32-bit unsigned integer. The unit is defined by the profile of the RTP session.

Media Encryption: The Media Encryption metric indicates whether media encryption is enabled or disabled for the RTP session. The Media encryption metric is an enumerated type metric. The possible values are: 0 = No encryption, 1 = AEA1.2, 2 = AES, 3-255 = Reserved for future use.

N

Number Sequence Falls: The number of sequence fall metric represents how many times during the RTP session there was at least one packet that was out of order.

Number Sequence Jumps: The number of sequence jump instances metric represents how many times during the reporting interval there was at least one packet which was lost.

NumberSeqFalls: Refer to Number Sequence Falls.

NumberSeqJumps: Number Sequence Jumps.

O

Octet: The Octet column in the Session Table indicates the size of the packets in octets.

P

Packet: A packet is the logical grouping of information that includes a header containing control information and (usually) the user data. The term packet is most often used to refer to the application layer data units.

Parent Endpoint: The terms parent and child endpoints are purely for describing the way endpoints are displayed in the Results List. A parent is like the branch in a tree view. A child is like a leaf in a tree view. The same endpoint can be shown as both a parent and a child. A parent endpoint is any endpoint listed as a result of a search. You click on the expanding key icon positioned in the far left column to expand the parent endpoint and show the child endpoints.

ParticipantID: The ParticipantID column assigns a unique identifier to each participant in the exported file. Each exported session has two participants. The exported data contains three sets of data. This data is listed in three separate tables that are separated by a blank row: Session Table, Time-varying Data Table and the TraceRoute Table. For every session a participant was involved in there will be a unique pair: SessionID and ParticipantID, enabling you to associate the session data, time-varying data and the trace route data as belonging to that participant in a specific session. Use the ParticipantID to identify the participant in each table to analyze the data.

Payload: Payload refers to the contents of a packet. In RTP it is encoded audio that is the user data of a packet. The payload identifies which codec is being used.

Perceived Delay: Perceived delay is the total effect RTT and Jitter have on a phone user's conversation.

Q

QoS: Refer to Quality of Service.

Quality of Service: QoS is the measure of the level of quality that a service requires or receives. The VoIP Monitoring Manager monitors and displays the 3 main factors that determine the quality of VoIP calls. These factors are Jitter, Round Trip Time, and Packet Loss. On the Summary Report each of the three factors display as a separate gauge.

R

RcvrIPAddr: The RcvrIPAddr column displays the IP address of this session participant (i.e. endpoint). This column appears in the Session Table of the exported file.

RcvrPHONE: The RcvrIPAddr column displays the phone number of the participant. This column appears in the Session Table of the exported file.

Real-Time Transport Control Protocol: A protocol providing support for applications with real-time properties, including timing reconstruction, loss detection, security, and content identification. It reports information about the RTP stream.

Real-Time Transport Protocol: Real-Time Transport Protocol is the protocol used for transmitting real-time data. For more information see IETF RFC 1889 located at: http://www.ietf.org/rfc/rfc1889.txt

Resource ReSerVation Protocol: RSVP is a protocol for reserving network bandwidth on the routers and switches between two endpoints in a session (in some other protocol, such as RTP). There are two reservations per session, one for each direction the data has to travel. For further reference see the IETF RFCs 2205 and 2750 located at: http://www.ietf.org/rfc/rfc2205.txt and http://www.ietf.org/rfc/rfc2750.txt

Round Trip Time: Round trip time is the length of time (in milliseconds) it takes a packet to traverse the network and return (thus being a round trip). It is the sum of the two one-way network delays between two endpoints. Callers can experience difficulties in carrying on a normal conversation when the one-way network delay exceeds 500 milliseconds (ms). However, some users may elect to tolerate this.

RSVP: Refer to Resource ReSerVation Protocol.

RSVP Status: The RSVP status for an endpoint shows whether the RSVP is enabled on the endpoint, and if it is, whether a reservation was established for the received RTP data stream.

RTCP: Refer to Real-Time Transport Control Protocol.

RTCP Listen Port: The RTCP Listen Port is the configurable port that is used to collect RTCP information from the AVAYA endpoints. The number must be from 1025 through 65535. The default port is 5005. Users are advised to avoid choosing ports in the reserved and 'well-known' ranges.

RTP: Refer to Real-Time Transport Protocol.

RTP MIB: The RTP MIB stores the information for the active RTP Sessions. The reference for the definition of the RTP MIB is located at: http://www.ietf.org/rfc/rfc2959.txt

RTP Session: A session is a VoIP connection between two IP endpoints. For more information see RFC 1889 located at: http://www.ietf.org/rfc/rfc1889.txt

RTT: Refer to Round Trip Time.

S

Session Table: The Session table is the exported table containing data that generally remains the same during a session. As a result, there is one entry per session in this table. The Session table will display in Microsoft Excel at the top of the same worksheet as the Time-varying Data table and the Trace Route table. The data in the Session table is indexed by SessionID and ParticipantID.

SessionID: The SessionID column assigns a unique identifier to each session in the exported file. Each exported session contains three sets of data. This data is listed in three separate tables that are separated by a blank row: Session Table, TimeStamped DataTable and the TraceRoute Table. Use the SessionID to identify the session in each table to analyze the data.

Silence Suppression: In Voice over IP (VoIP), silence suppression is a method of detecting the silence in audio and purposefully dropping silent packets at the sender to conserve network bandwidth. The receiver will generate comfort noise or conceal the loss of packets when packets are dropped. Because the receiver conceals loss and generates comfort noise, silence suppression is usually imperceptible to the listener. The silence suppression will be reported as enabled, disabled or unknown.

Simple Network Management Protocol: SNMP is a standard protocol for communicating with network devices.

SNMP: Refer to Simple Network Management Protocol.

StartTime: The StartTime column in the exported file displays the date and time the session started. This column appears in the Session Table of the exported file.

T

Time-To-Live: Time-to-live (TTL) is a value in an Internet Protocol (IP) packet that tells a network router if a packet has been forwarded towards its destination too many times and should be discarded.

Time-varying Data Table: The Time-varying Data table is one of the exported tables containing the time-varying data for the sessions in the Session table. The data in this table is indexed by SessionID, ParticipantID, and a time offset. The SessionID and ParticipantID enable the data to be linked to corresponding sessions in the Session table. The time offset indicates when this set of information was reported (in seconds since the start of each call). The Time-varying Data table will display in Microsoft Excel below the Session table on the same worksheet. To view the information more easily, you may want to copy the table and paste it to another worksheet.

TimeOffset: The TimeOffset column displays the number of seconds since the session started for this set of data. This column appears in the Time-varying Data Table of the exported file.

TOOL: The TOOL value is the name and version of the application generating the stream, for example, Avaya VoIP Engine v.123. This information may be useful for diagnosis. The TOOL value should remain constant for the duration of the session.

Trace Route Table: The Trace Route table contains information about the route in the network that the RTP packets traverse between the two endpoints of the call. It will display in Microsoft Excel below the Time-varying Data table.

Trap: Refer to Alarm

TTL: Refer to Time-To-Live.

V

Voice over Internet Protocol: Voice over Internet Protocol (VoIP) is the technology standard that supports Internet telephony. It provides the capability for live voice communication over the Internet so that you can talk using the multimedia capabilities of your computer, in the same way you would talk using a telephone.

VoIP: Refer to Voice over Internet Protocol.

W

Windows SNMP Agent: The Windows SNMP Agent runs as an operating-system-managed service. It is optionally installed with the Windows Operating System.

Index