Avaya VoIP Monitoring Manager Release 3.0

Configuration

555-233-510
Issue 6
June 2005

Notice

Every effort was made to ensure that the information in this document was complete and accurate at the time of printing. However, information is subject to change.

Warranty

Avaya Inc. provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language as well as information regarding support for this product, while under warranty, is available through the following Web site: http://www.avaya.com/support.

Preventing Toll Fraud

"Toll fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there may be a risk of toll fraud associated with your system and that, if toll fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Fraud Intervention

If you suspect that you are being victimized by toll fraud and you need technical assistance or support, in the United States and Canada, call the Technical Service Center's Toll Fraud Intervention Hotline at 1-800-643-2353.

Disclaimer

Avaya is not responsible for any modifications, additions or deletions to the original published version of this documentation unless such modifications, additions or deletions were performed by Avaya. Customer and/or End User agree to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation to the extent made by the Customer or End User.

How to Get Help

For additional support telephone numbers, go to the Avaya support Web site: http://www.avaya.com/support. If you are:

- Within the United States, click the *Escalation Management* link. Then click the appropriate link for the type of support you need.
- Outside the United States, click the *Escalation Management* link. Then click the *International Services* link that includes telephone numbers for the international Centers of Excellence.

Providing Telecommunications Security

Telecommunications security (of voice, data, and/or video communications) is the prevention of any type of intrusion to (that is, either unauthorized or malicious access to or use of) your company's telecommunications equipment by some party.

Your company's "telecommunications equipment" includes both this Avaya product and any other voice/data/video equipment that could be accessed via this Avaya product (that is, "networked equipment").

An "outside party" is anyone who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf. Whereas, a "malicious party" is anyone (including someone who may be otherwise authorized) who accesses your telecommunications equipment with either malicious or mischievous intent.

Such intrusions may be either to/through synchronous (time-multiplexed and/or circuit-based), or asynchronous (character-, message-, or packet-based) equipment, or interfaces for reasons of:

- Utilization (of capabilities special to the accessed equipment)
- Theft (such as, of intellectual property, financial assets, or toll facility access)
- Eavesdropping (privacy invasions to humans)
- Mischief (troubling, but apparently innocuous, tampering)
- Harm (such as harmful tampering, data loss or alteration, regardless of motive or intent)

Be aware that there may be a risk of unauthorized intrusions associated with your system and/or its networked equipment. Also realize that, if such an intrusion should occur, it could result in a variety of losses to your company (including but not limited to, human/data privacy, intellectual property, material assets, financial resources, labor costs, and/or legal costs).

Responsibility for Your Company's Telecommunications Security

The final responsibility for securing both this system and its networked equipment rests with you - Avaya's customer system administrator, your telecommunications peers, and your managers. Base the fulfillment of your responsibility on acquired knowledge and resources from a variety of sources including but not limited to:

- Installation documents
- System administration documents
- Security documents
- Hardware-/software-based security tools
- Shared information between you and your peers
- Telecommunications security experts

To prevent intrusions to your telecommunications equipment, you and your peers should carefully program and configure:

- Your Avaya-provided telecommunications systems and their interfaces
- Your Avaya-provided software applications, as well as their underlying hardware/software platforms and interfaces
- Any other equipment networked to your Avaya products

TCP/IP Facilities

Customers may experience differences in product performance, reliability and security depending upon network configurations/design and topologies, even when the product performs as warranted.

Standards Compliance

Avaya Inc. is not responsible for any radio or television interference caused by unauthorized modifications of this equipment or the substitution or attachment of connecting cables and equipment other than those specified by Avaya Inc. The correction of interference caused by such unauthorized modifications, substitution or attachment will be the responsibility of the user. Pursuant to Part 15 of the Federal Communications Commission (FCC) Rules, the user is cautioned that changes or modifications not expressly approved by Avaya Inc. could void the user's authority to operate this equipment.

Product Safety Standards

This product complies with and conforms to the following international Product Safety standards as applicable:

Safety of Information Technology Equipment, IEC 60950, 3rd Edition, or IEC 60950-1, 1st Edition, including all relevant national deviations as listed in Compliance with IEC for Electrical Equipment (IECEE) CB-96A.

Safety of Information Technology Equipment, CAN/CSA-C22.2 No. 60950-00 / UL 60950, 3rd Edition, or CAN/CSA-C22.2 No. 60950-1-03 / UL 60950-1.

Safety Requirements for Information Technology Equipment, AS/NZS 60950:2000.

One or more of the following Mexican national standards, as applicable: NOM 001 SCFI 1993, NOM SCFI 016 1993, NOM 019 SCFI 1998.

The equipment described in this document may contain Class 1 LASER Device(s). These devices comply with the following standards:

- EN 60825-1, Edition 1.1, 1998-01
- 21 CFR 1040.10 and CFR 1040.11.

The LASER devices used in Avaya equipment typically operate within the following parameters:

Typical Center Wavelength	Maximum Output Power
830 nm - 860 nm	-1.5 dBm
1270 nm - 1360 nm	-3.0 dBm
1540 nm - 1570 nm	5.0 dBm

Luokan 1 Laserlaite

Klass 1 Laser Apparat

Use of controls or adjustments or performance of procedures other than those specified herein may result in hazardous radiation exposures. Contact your Avaya representative for more laser product information.

Electromagnetic Compatibility (EMC) Standards

This product complies with and conforms to the following international EMC standards and all relevant national deviations:

Limits and Methods of Measurement of Radio Interference of Information Technology Equipment, CISPR 22:1997, EN55022:1998, and AS/NZS 3548.

Information Technology Equipment - Immunity Characteristics - Limits and Methods of Measurement, CISPR 24:1997 and EN55024:1998, including:

- Electrostatic Discharge (ESD) IEC 61000-4-2
- Radiated Immunity IEC 61000-4-3
- Electrical Fast Transient IEC 61000-4-4
- Lightning Effects IEC 61000-4-5
- Conducted Immunity IEC 61000-4-6
- Mains Frequency Magnetic Field IEC 61000-4-8
- Voltage Dips and Variations IEC 61000-4-11

Power Line Emissions, IEC 61000-3-2: Electromagnetic compatibility (EMC) - Part 3-2: Limits - Limits for harmonic current emissions.

Power Line Emissions, IEC 61000-3-3: Electromagnetic compatibility (EMC) - Part 3-3: Limits - Limitation of voltage changes, voltage fluctuations and flicker in public low-voltage supply systems.

Federal Communications Commission Statement

Part 15:

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Part 68: Answer-Supervision Signaling

Allowing this equipment to be operated in a manner that does not provide proper answer-supervision signaling is in violation of Part 68 rules. This equipment returns answer-supervision signals to the public switched network when:

- answered by the called station,
- answered by the attendant, or
- routed to a recorded announcement that can be administered by the customer premises equipment (CPE) user.

This equipment returns answer-supervision signals on all direct inward dialed (DID) calls forwarded back to the public switched telephone network. Permissible exceptions are:

- A call is unanswered.
- A busy tone is received.
- A reorder tone is received.

Avaya attests that this registered equipment is capable of providing users access to interstate providers of operator services through the use of access codes. Modification of this equipment by call aggregators to block access dialing codes is a violation of the Telephone Operator Consumers Act of 1990.

REN Number

For MCC1, SCC1, CMC1, G600, and G650 Media Gateways:

This equipment complies with Part 68 of the FCC rules. On either the rear or inside the front cover of this equipment is a label that contains, among other information, the FCC registration number, and ringer equivalence number (REN) for this equipment. If requested, this information must be provided to the telephone company.

For G350 and G700 Media Gateways:

This equipment complies with Part 68 of the FCC rules and the requirements adopted by the ACTA. On the rear of this equipment is a label that contains, among other information, a product identifier in the format US:AAAEQ##TXXXX. The digits represented by ## are the ringer equivalence number (REN) without a decimal point (for example, 03 is a REN of 0.3). If requested, this number must be provided to the telephone company.

For all media gateways:

The REN is used to determine the quantity of devices that may be connected to the telephone line. Excessive RENs on the telephone line may result in devices not ringing in response to an incoming call. In most, but not all areas, the sum of RENs should not exceed 5.0. To be certain of the number of devices that may be connected to a line, as determined by the total RENs, contact the local telephone company.

REN is not required for some types of analog or digital facilities.

Means of Connection

Connection of this equipment to the telephone network is shown in the following tables.

For MCC1, SCC1, CMC1, G600, and G650 Media Gateways:

Manufacturer’s Port Identifier	FIC Code	SOC/ REN/ A.S. Code	Network Jacks
Off premises station	OL13C	9.0F	RJ2GX, RJ21X, RJ11C
DID trunk	02RV2-T	0.0B	RJ2GX, RJ21X
CO trunk	02GS2	0.3A	RJ21X
	02LS2	0.3A	RJ21X
Tie trunk	TL31M	9.0F	RJ2GX
Basic Rate Interface	02IS5	6.0F, 6.0Y	RJ49C
1.544 digital interface	04DU9-BN	6.0F	RJ48C, RJ48M
	04DU9-IKN	6.0F	RJ48C, RJ48M
	04DU9-ISN	6.0F	RJ48C, RJ48M
120A4 channel service unit	04DU9-DN	6.0Y	RJ48C

For G350 and G700 Media Gateways:

Manufacturer’s Port Identifier	FIC Code	SOC/ REN/ A.S. Code	Network Jacks
Ground Start CO trunk	02GS2	1.0A	RJ11C
DID trunk	02RV2-T	AS.0	RJ11C
Loop Start CO trunk	02LS2	0.5A	RJ11C
1.544 digital interface	04DU9-BN	6.0Y	RJ48C
	04DU9-DN	6.0Y	RJ48C
	04DU9-IKN	6.0Y	RJ48C
	04DU9-ISN	6.0Y	RJ48C
Basic Rate Interface	02IS5	6.0F	RJ49C

For all media gateways:

If the terminal equipment (for example, the media server or media gateway) causes harm to the telephone network, the telephone company will notify you in advance that temporary discontinuance of service may be required. But if advance notice is not practical, the telephone company will notify the customer as soon as possible. Also, you will be advised of your right to file a complaint with the FCC if you believe it is necessary.

The telephone company may make changes in its facilities, equipment, operations or procedures that could affect the operation of the equipment. If this happens, the telephone company will provide advance notice in order for you to make necessary modifications to maintain uninterrupted service.

If trouble is experienced with this equipment, for repair or warranty information, please contact the Technical Service Center at 1-800-242- 2121 or contact your local Avaya representative. If the equipment is causing harm to the telephone network, the telephone company may request that you disconnect the equipment until the problem is resolved.

A plug and jack used to connect this equipment to the premises wiring and telephone network must comply with the applicable FCC Part 68 rules and requirements adopted by the ACTA. A compliant telephone cord and modular plug is provided with this product. It is designed to be connected to a compatible modular jack that is also compliant. It is recommended that repairs be performed by Avaya certified technicians.

The equipment cannot be used on public coin phone service provided by the telephone company. Connection to party line service is subject to state tariffs. Contact the state public utility commission, public service commission or corporation commission for information.

This equipment, if it uses a telephone receiver, is hearing aid compatible.

Canadian Department of Communications (DOC) Interference Information

This Class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

This equipment meets the applicable Industry Canada Terminal Equipment Technical Specifications. This is confirmed by the registration number. The abbreviation, IC, before the registration number signifies that registration was performed based on a Declaration of Conformity indicating that Industry Canada technical specifications were met. It does not imply that Industry Canada approved the equipment.

Installation and Repairs

Before installing this equipment, users should ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. The customer should be aware that compliance with the above conditions may not prevent degradation of service in some situations.

Repairs to certified equipment should be coordinated by a representative designated by the supplier. Any repairs or alterations made by the user to this equipment, or equipment malfunctions, may give the telecommunications company cause to request the user to disconnect the equipment.

Declarations of Conformity

United States FCC Part 68 Supplier's Declaration of Conformity (SDoC)

Avaya Inc. in the United States of America hereby certifies that the equipment described in this document and bearing a TIA TSB-168 label identification number complies with the FCC's Rules and Regulations 47 CFR Part 68, and the Administrative Council on Terminal Attachments (ACTA) adopted technical criteria.

Avaya further asserts that Avaya handset-equipped terminal equipment described in this document complies with Paragraph 68.316 of the FCC Rules and Regulations defining Hearing Aid Compatibility and is deemed compatible with hearing aids.

Copies of SDoCs signed by the Responsible Party in the U. S. can be obtained by contacting your local sales representative and are available on the following Web site: http://www.avaya.com/support.

All Avaya media servers and media gateways are compliant with FCC Part 68, but many have been registered with the FCC before the SDoC process was available. A list of all Avaya registered products may be found at: http://www.part68.org by conducting a search using "Avaya" as manufacturer.

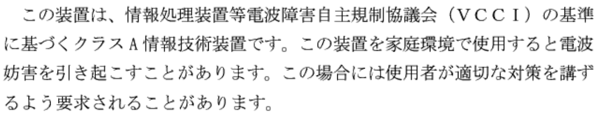
European Union Declarations of Conformity

Avaya Inc. declares that the equipment specified in this document bearing the "CE" (*Conformité Europeénne*) mark conforms to the European Union Radio and Telecommunications Terminal Equipment Directive (1999/5/EC), including the Electromagnetic Compatibility Directive (89/336/EEC) and Low Voltage Directive (73/23/EEC).

Copies of these Declarations of Conformity (DoCs) can be obtained by contacting your local sales representative and are available on the following Web site: http://www.avaya.com/support.

Japan

This is a Class A product based on the standard of the Voluntary Control Council for Interference by Information Technology Equipment (VCCI). If this equipment is used in a domestic environment, radio disturbance may occur, in which case, the user may be required to take corrective actions.



この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

To order copies of this and other documents:

Call: Avaya Publications Center
Voice 1.800.457.1235 or 1.207.866.6701
FAX 1.800.457.1764 or 1.207.626.7269

Write: Globalware Solutions
200 Ward Hill Avenue
Haverhill, MA 01835 USA
Attention: Avaya Account Management

E-mail: totalware@gwsmail.com

For the most current versions of documentation, go to the Avaya support Web site: http://www.avaya.com/support.

Contents

Preface

Purpose

The purpose of this book is to provide the following information:

- An overview of Avaya VoIP Monitoring Manager capabilities and components.
- Procedures for starting and using Avaya VoIP Monitoring Manager.
- A description of how to interpret Avaya VoIP Monitoring Manager reports.

Intended Audience

This book is intended for network managers familiar with network management and its fundamental concepts.

Conventions Used in This Book

The following typographical conventions are used:

- **Bold** type is used to indicate information that you type, buttons in a window, selections in a menu, and the **Enter** key on the keyboard. It is also used for emphasis.
- `Courier` font is used for any information that the computer screen displays.
- Arrows indicate options that you select from cascading menus; for example, “Select File > Open” means choose the “Open” option from the “File” menu.

Support Resources

Avaya provides a variety of planning, consulting, and technical services. The following sections describe the resources and services that are available.

Avaya Technology and Consulting (ATAC)

Avaya Technology and Consulting (ATAC) works with client teams to develop detailed solutions for connectivity to Avaya Communication Manager solutions. The ATAC also designs network configurations. Due to configuration complexities, we strongly recommend that you contract for professional implementation services for the following Avaya Integrated Management products:

- Avaya MultiSite Administration
- Avaya Fault and Performance Manager
- Avaya Proxy Agent

Communications, Solutions, and Integration (CSI) Group of Software Services

Avaya Communications, Solutions, and Integration (CSI) Group of Software Services offers customers the following services:

- Platform readiness verification
- Remote implementation and installation
- Network management server configuration
- Customer acceptance verification
- Custom on-site services

The CSI Group consists of the following two teams:

- **Converged Solutions Implementation Engineering**

  The Converged Solutions Implementation Engineering (CSIE) team implements multi-site media gateway (G350/G650/G700) deployment projects for both voice and data design. The overall direction of the CSIE team is to bring the correct methodology to these complex deployments that span various regions and to provide continuity to the overall project from the voice and data implementation standpoint.

- **Data Network Implementation Engineering (formerly RNIS)**

  The Data Network Implementation Engineering team implements and/or upgrades existing or new data networks. This team analyzes the customer's network design requirements and performance expectations, and then creates the hardware and software installation specification used to implement data devices including Cajun, VPN, Wireless LAN, Secure Gateways, Extreme, and multi-vendor data equipment.

The CSI Group provides support on a contract basis. You can purchase various implementation offers from the CSI Group in Tampa, Florida. See Table 1: Customer-Accessible Resources on page 11 for contact information.

Avaya Technical Service Organization (TSO)

The Avaya Technical Service Organization (TSO) provides support to the Avaya Integrated Management client teams, field technicians, and customers. The TSO will bill customers for support on a time and materials basis if the following conditions exist:

- Customers do not provide remote access.
- Customers do not have a current maintenance agreement.
- Customers do not procure and install the required systems and software as defined in the Avaya Integrated Management Services Support Plan.
- Customers request support that is outside the purchase agreement.

The TSO does ***not*** support hardware or software that customers purchase from third-party vendors.

Avaya Network Management Software Systems Support Group (NMSSS)

The Avaya Network Management Software Systems Support Group (NMSSS) in Tampa Bay, Florida answers customer calls about products in Avaya Integrated Management. NMSSS will either answer your questions directly or connect you with an associate who can answer questions about the products.

Customized Management Solutions for Avaya Integrated Management

The Integrated Management Product Team understands customer's needs and is focused on customer satisfaction. See Table 1: Customer-Accessible Resources on page 11 for contact information. The Product Team will assist customers with Avaya Integrated Management projects and will provide:

- **Project Management** — An Integrated Management project person will work with the customer to access configuration and customization requirements for any or all applications within each Avaya Integrated Management offer. If custom work is required, the evaluation will include a proposed statement of work and price. Note that this offer is *not* intended to provide installation for customers that choose to implement Integrated Management applications using Avaya Services or third-party implementation services.
- **Training** — Basic training can be performed remotely using an interactive medium to display the applications and a conference bridge for audio. On-site training can be customized to meet the customer's needs. Customized training will focus on application functionality that is relevant to the customer and provide focused knowledge transfer to facilitate application-specific training.

Avaya Contact Information

Table 1 and Table 2 provide contact information that you may use if you need assistance during the process of installing and setting up Avaya Integrated Management. To access the links in Table 2, you must be able to access the Avaya intranet.

Table 1: Customer-Accessible Resources

Resource	Contact Information
Avaya Support Center	http://www.avaya.com/support
Network Management Software Systems Support (NMSSS)	+1 800 237-0016
Communications, Solutions, and Integration (CSI) Group of Software Services	+1 800 730-9108, prompt 3
Integrated Management Product Team	Send email to: AIMtraining@avaya.com
Toll Fraud Intervention	+1 800 643-2353, prompt 1

Table 2: Avaya Internal Resources

Resource	Contact Information
Avaya System Management Support	http://aem-support.dr.avaya.com
Avaya Technology and Consulting (ATAC)	+1 888 297-4700, prompt 2,6 http://forum.avaya.com (requires a password)
Communications, Solutions, and Integration (CSI) Group of Software Services	http://associate2.avaya.com/sales_market/products/data-implementation-services/
Integrated Management Services Support Plan	http://associate2.avaya.com/solution/support_plans/#Enterprise

Product Documentation

The latest version of Avaya Integrated Management product documentation, including this book, is available from the Avaya Support Web Site. To view or download these books from the Web, you must have access to the Internet, an Internet browser, and Adobe Acrobat Reader, version 5.0 or later. Adobe Acrobat Reader is provided on the System Management CD and is also available from http://www.adobe.com. See How to Access Books on the Web for instructions on how to view or download these books.

How to Access Books on the Web

To view or download books from the Avaya Support Web Site, follow these steps:

1. Access http://www.avaya.com/support.
2. In the left column, click **System and Network Management**.
3. Scroll to **Integrated Management**, locate the product name, and click the link corresponding to the software release to display a list of available books for that product.

Tell Us What You Think!

Let us know how this book measured up to your expectations. Your opinions are crucial to helping us meet your needs! Please send us your comments by mail, fax, or e-mail as follows:

Mail: Avaya Inc.
Avaya Integrated Management Documentation Team
Room 3C-313
307 Middletown Lincroft Rd.
Lincroft, NJ 07738
USA

Fax: Avaya Integrated Management Documentation Team
+ 1 732 852-2469

E-mail: document@avaya.com
Subject: Avaya Integrated Management Documentation Team

Chapter 1: Overview

What is Avaya Voice Over IP Monitoring Manager?

Avaya Voice Over IP (VoIP) Monitoring Manager is a VoIP Quality of Service (QoS) monitoring tool. It enables you to monitor and review the quality of a call on an Avaya VoIP network.

Avaya VoIP Monitoring Manager allows you to view the QoS data (that is, jitter, round trip time (RTT) and packet loss) experienced at the endpoints and during a session. This data displays in real-time or for previously active endpoints. With this information, you can begin to troubleshoot and isolate problems.

Avaya VoIP Monitoring Manager allows you to:

- **Search Endpoints.** You can search endpoints active from a specified time in the past or between a date range. Advanced search options enable you to narrow your search to match phone numbers, SIP user names, network addresses, or QoS levels.
- **View Reports.** Once you have a list of endpoints, you can select one or more endpoints in a session and view the associated reports. The reports display QoS data such as jitter, round trip time (RTT), and packet loss. This is particularly useful for monitoring media gateways or locating problems at a particular endpoint.

  Since you can view reports for endpoints involved in a session, this information will assist you with determining problems that occur between two endpoints or in an isolated area of the network.
- **Export Reports.** You can export the report data to a comma separated value (csv) file. 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.
- **Generate Automatic Alarms.** You can generate Simple Network Management Protocol (SNMP) Traps/Alarms, which allow the VoIP Monitoring Manager to alert you when the jitter, RTT, or packet loss reaches certain levels. You can routinely monitor the network and troubleshoot problems.

Avaya VoIP Monitoring Manager Components

The Avaya VoIP Monitoring Manager incorporates the Avaya VoIP Monitoring Manager Real-time Transport Control Protocol (RTCP) Monitor and the Avaya VoIP Monitoring Manager Server, which accepts connections from the Avaya VoIP Monitoring Manager Client. The server software must be installed on the network to work correctly. A Windows SNMP Agent must also be installed on the server.

VoIP Monitoring Manager also uses a database. During installation, the VoIP Monitoring Manager Integrated MSDE Database is installed by default. However, you can choose to install a different Microsoft SQL database.

The components are described in more detail in the following sections.

Avaya VoIP Monitoring Manager Server

The Avaya VoIP Monitoring Manager Server acts as a proxy between the MSDE database and the Avaya VoIP Monitoring Manager Client. It manages connectivity to the database and provides an interface to configure the Avaya VoIP Monitoring Manager RTCP Monitor. The server resides on the same PC as the RTCP Monitor. The database can reside on the same PC as the server and RTCP Monitor, or it can reside on a separate machine.

Avaya VoIP Monitoring Manager RTCP Monitor

The Avaya VoIP Monitoring Manager 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 using Microsoft SQL.

Avaya VoIP Monitoring Manager Client

The Avaya VoIP Monitoring Manager Client provides the graphical user interface (GUI). The client does not communicate with the RTCP Monitor, does not use the Windows SNMP service, and does not communicate with the database. The data that is displayed is gathered from the Avaya VoIP Monitoring Manager Server. The client may be installed on the same machine as the server, or it may be installed on another machine on the network.

Avaya 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 Avaya VoIP Monitoring Manager Server installed. To run the Avaya VoIP Monitoring Manager Client as a Web application, the following requirements must be met:

- The VoIP Monitoring Manager Server 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

  Note:

  The server installation will apply this configuration.
- The PC you will use to access the Avaya VoIP Monitoring Manager Server must be able to connect to the VoIP Monitoring Manager Server via a web browser and have the following software installed:
  - Microsoft Internet Explorer 6.0 or later
  - SUN Java 2 Runtime Environment, SE v1.4.2_06

If you run the Web client, you will not have access to some of the features—such as connecting to a new server and copying — that are available in the application.

WebLM License Server

The WebLM License Server manages your licenses for Avaya Integrated Management products. It is required when you purchase the VoIP Monitoring Manager license key to activate VoIP Monitoring Manager beyond the 90-trial period. The WebLM License Server is not required to use the 90-day trial version.

Chapter 2: Using Avaya VoIP Monitoring Manager

Overview

This chapter describes how to

- start the Avaya VoIP Monitoring Manager Server
- start the Avaya VoIP Monitoring Manager Client
- start the Avaya VoIP Monitoring Manager Web Client
- search for endpoints
- view reports
- view session data
- export data
- change the settings of the VoIP Monitoring Manager Server

Note:

Avaya VoIP Monitoring Manager Server must be installed and running on the network before you start the Avaya VoIP Monitoring Manager Client or the Avaya VoIP Monitoring Manager Web Client.

Starting the Avaya VoIP Monitoring Manager Server

To start the Avaya VoIP Monitoring Manager Server, perform the following steps:

1. From the machine where the VoIP Monitoring Server software is installed, select **Start > Programs > Avaya > VoIP Monitoring Manager > Server**.

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

2. In the License Server box, enter the IP address of the WebLM server.
3. In the Port Number box, enter the port number of the WebLM server.

4. Click the **OK** button.

   The About dialog box appears and displays the licensing information.

5. Click the **Close** button.

   Avaya VoIP Monitoring Manager Server window appears.

Starting the Avaya 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.

Note:

> The Avaya VoIP Monitoring Manager Server must be running before you start the Avaya VoIP Monitoring Manager Client.

To start the Avaya VoIP Monitoring Manager Client, perform the following steps:

1. From the machine where the VoIP Monitoring Manager Client software is installed, select **Start > Programs > Avaya > VoIP Monitoring Manager > Client**.

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

2. In the License Server box, enter the IP address of the WebLM server.
3. In the Port Number box, enter the port number of the WebLM server.
4. Click the **OK** button.

   The About dialog box appears and displays the licensing information.

5. Click the **Close** button.

   Avaya VoIP Monitoring Manager Client window appears. Now you can search for endpoints and then view the QoS data in a report format.

Starting the Avaya 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 Avaya VoIP Monitoring Manager Server installed.

The VoIP Monitoring Manager Web Client has the following limitations:

- You can access only one monitor that is directly connected to the server running the VoIP Monitoring Manager Server.
- You cannot connect to a new server.
- You cannot use the Copy function.

These limitations are imposed by the security restrictions associated with running unsigned applets.

Note:

> The Avaya VoIP Monitoring Manager Server must be running before you start the Avaya VoIP Monitoring Manager Web Client.

To start the Avaya VoIP Monitoring Manager Web Client, perform the following step:

1. Using Microsoft Internet Explorer 6.0 or later, go to
   `http://VMMServerMachineName/VoIPMonMgr/ClientApplet.html`
   where **VMMServerMachineName** is the machine running the VMM Server.

   The License Server Administration dialog box appears, which enables you to log into the WebLM server that manages your Avaya licenses. The license server is required to activate Avaya VoIP Monitoring Manager beyond the 90-day trial period. If you do not have a license to use Avaya VoIP Monitoring Manager, you can use the software for a 90-day trial period.
2. In the License Server box, enter the IP address of the WebLM server.
3. In the Port Number box, enter the port number of the WebLM server.
4. Click the **OK** button.

   The About dialog box appears and displays the licensing information.
5. Click the **Close** button.

   Avaya VoIP Monitoring Manager Web Client window appears. Now you can search for endpoints and then view the QoS data in a report format.

To exit the Avaya VoIP Monitoring Manager Web Client, close Microsoft Internet Explorer.

Searching for Endpoints

You can search for endpoints active in the past or between a date range. You can also use the Advanced Search options to narrow the search based on phone number, SIP user name, network addresses, or QoS value. Once you have completed your search, the Results List provides a list of endpoints. You can then select an endpoint from the Results List to view QoS data for that endpoint in a report format.

To run a search, perform the following steps:

1. Perform one of the following steps:
   - Select **Edit > Search**.
   - Click **Search** on the Endpoint pane.
2. From the Search dialog box, click the drop down arrow to select a time period to search 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 then 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.
5. Click **Search**.

   The Results List provides a list of endpoints. Select an endpoint to view its report.

Viewing Reports

You can generate reports for endpoints and media gateways from the VoIP Monitoring Manager Client.

There are two types of endpoint reports:

- Summary Reports

  Summary Reports display the QoS data as a reading on a gauge. The needle on the gauge shows the average values measured and the black inner arc shows the minimum and maximum values measured.
- Detailed Reports

  Detailed Reports show how the QoS values changes during the call and when this occurred. 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.

There are three types of media gateway reports:

- Summary Media Gateway Link Reports

  Summary Media Gateway Link Reports display the aggregate QoS data of all the VoIP sessions for the selected media gateway as a reading on a gauge.

- Detailed Media Gateway Link Reports

  Detailed Media Gateway Link Reports show the aggregate jitter, RTT, and percent loss on a graph for VoIP session going between the two selected media gateways.

- Trace Routes Media Gateway Link Reports

  Trace Routes Media Gateway Link Reports show the probable routes used between the two selected media gateways.

To view an Endpoint report, perform the following steps:

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

   The Report button becomes enabled.

2. Click **Report**.

   The Endpoint reports appear.

3. Click the tab of the Endpoint report you want to view.

To view a Media Gateway Link report, perform the following steps:

1. From the System pane, select a media gateway or click on the expanding icon and select a child endpoint that was in a session with the parent endpoint.

   The Report button becomes enabled.

2. Click **Report**.

   The Media Gateway Link reports appear.

3. Click the tab of the Media Gateway Link report you want to view.

For more information about reports, see Interpreting Reports on page 25.

Viewing the Session Data

Reports show both endpoints involved in a session. The reports show the parent endpoint involved in the session in the top part of the report with the child endpoint below.

The terms parent and child endpoints are used to describe 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. You will see 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.

To view sessions in a report, perform the following steps:

1. Click on the expanding icon positioned in the far left column of the Results List.

   A sub list appears.

2. Select a **child endpoint** from the sub list.
3. Click the **Report** button.

   The reports appear.

Exporting the Data

The data in the Results List or from a single report can be exported to a comma separated value (cvs) file. The cvs file can be opened in most database and spreadsheet programs. Exporting the data to a spreadsheet enables you to manipulate the data so you can create your own reports. The data exported is divided into the following tables:

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

To export data, perform the following steps:

1. Select **File > Export Result List** or click the **Export** button located at the bottom of the **Result List**.

   The Save dialog box appears.

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. If you want to export a single report, open your report and click the **Report** button.

   Note:

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

Changing the VoIP Monitoring Manager Server Settings

Data that is reported depends on settings that are made in the server. The default settings are a good starting point, but are intended only as a guide. Changing some settings can help you obtain better reports. Over time, you will be able to fine-tune the server settings in order to highlight abnormal operation for your specific environment.

Generating Traps

Rules are set to generate traps that notify you when the VoIP network QoS parameters have reached unacceptable levels. Rules are defined in the Trap Threshold Settings dialog box, which provides a tab for Call Traps and a tab for System and Terminal Traps. To open the Trap Threshold Settings dialog box, from the VoIP Monitoring Manager Server window, select **Edit > Trap Settings**.

More than one rule can be set 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, all conditions must 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 Monitoring Manager creates traps based on two sets of rules:

- Call Traps

  If a specified condition occurs anywhere in the system, a trap is sent immediately.

- System Traps

  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.

Recommended Trap Settings

Values that you use to trigger traps 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 Manger is installed are a useful starting point. These settings are based on an environment with high-quality telecommunications facilities. For example, in this environment it is reasonable to expect RTT of less than 300. Recommended trap settings are provided in Table 3.

Table 3: Recommended Trap Settings

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

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 Threshold Settings dialog box.

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

System Traps

A System Trap (also called a System Alarm) is where a trap has been triggered because the number of warnings has exceeded the defined threshold. The conditions for the System Trap are defined in the Trap Threshold Settings dialog box.

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 Trap is generated. To generate an trap as soon as the thresholds are reached, use an interval of zero (0).

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

Chapter 3: Interpreting Reports

Overview

This chapter describes how to interpret the Avaya VoIP Monitoring Manager reports.

Endpoint Reports

You can generate the following reports for endpoints:

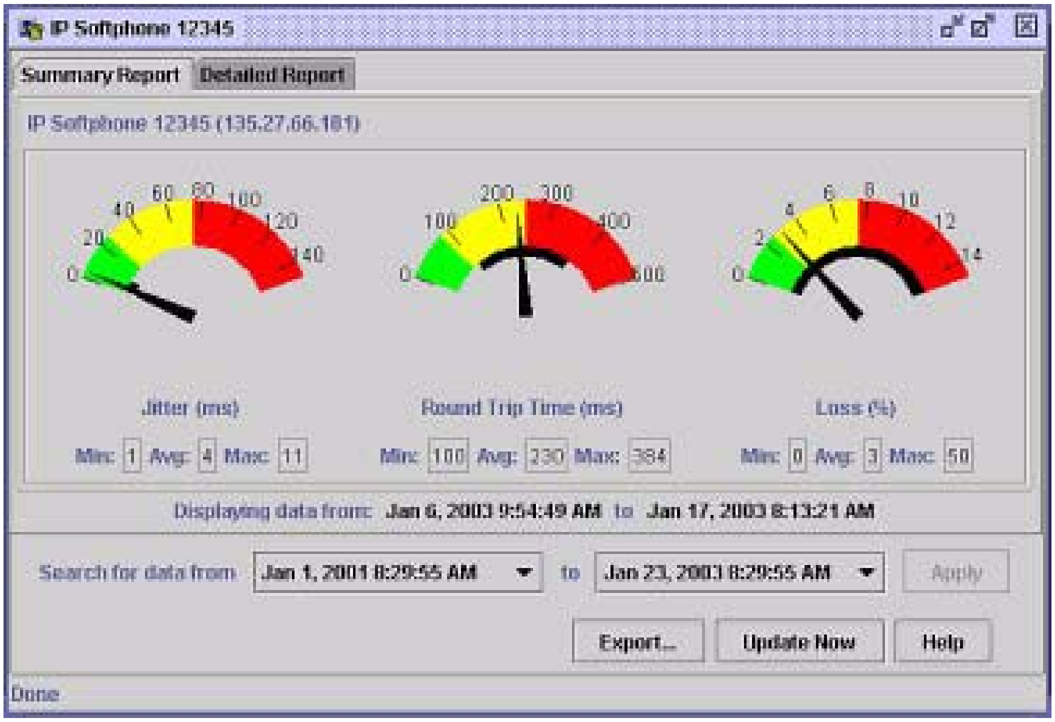
- Summary Report
- Detailed Report

Interpreting Summary Reports for Endpoints

Figure 1 shows a sample Summary Report for an endpoint. Summary Reports show the QoS data as a reading on a gauge. The needle on the gauge shows the average values measured and the black inner arc shows the minimum and maximum values measured. Each of the three QoS parameters is displayed on a separate gauge. You can alter these values by selecting **Edit > Report Properties**. Summary Reports also show the date range during which the data was collected, the type of endpoint that was monitored, and the phone number and IP address of that endpoint.

You interpret the Summary Reports by noting where the needle on each gauge is positioned. When the needle is positioned in either the yellow or red ranges, it indicates degradation in the QoS. Table 4: Values for the Summary Reports on page 26 describes the values for each of the three QoS parameters on a Summary Report.

Figure 1: Summary Report



IP Softphone 12345 (135.27.66.181)

Jitter (ms) Min: 1 Avg: 4 Max: 11

Round Trip Time (ms) Min: 100 Avg: 230 Max: 384

Loss (%) Min: 0 Avg: 3 Max: 50

Displaying data from: Jan 6, 2003 9:54:49 AM to Jan 17, 2003 8:13:21 AM

Search for data from Jan 1, 2001 8:29:55 AM to Jan 23, 2003 8:29:55 AM

Done

Table 4: Values for the Summary Reports

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

Interpreting Detailed Reports for Endpoints

Figure 2 shows a sample Detailed Report for an endpoint. Detailed Reports show how the QoS values change during the call and when this occurred. This information 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. Each point on the line graph represents the maximum value since the last point displayed.

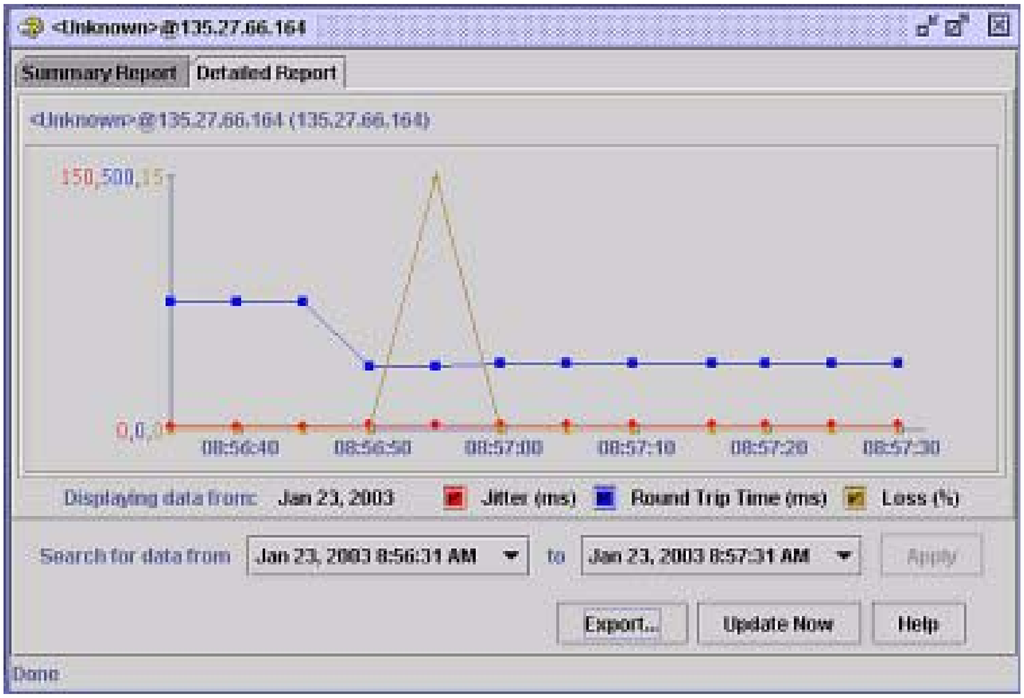
Each of the QoS parameters is represented on the graph by a different color. This makes it easier to see the data on the same line graph. You can uncheck the display of one or more of the QoS parameters on the active line graph. The QoS parameter colors are as follows:

- Jitter is shown in red.
- Round Trip Time is shown in blue.
- Packet Loss is shown in brown.

Detailed Reports provide a tool tip that enables you to point your mouse at the data on the line graph to see the exact data measured. You can also alter the date range to show more or less detail.

You interpret the Detailed Report by noting where the sampled points for each QoS value appears on the line graph and when this may have occurred. The default upper values on the Y-axis indicate unacceptable limits. Select **Edit > Report Properties** to change the lower and upper limits of each QoS value.

Figure 2: Detailed Report



<Unknown>@135.27.66.164

<Unknown>@135.27.66.164 (135.27.66.164)

Displaying data from: Jan 23, 2003

Search for data from Jan 23, 2003 8:56:31 AM to Jan 23, 2003 8:57:31 AM

Done

Table 5 describes the values for each of the three QoS parameters on a Detailed Report.

Table 5: Values for Detailed Reports

QoS	Lower Acceptable	Middle Warning	Upper Not Acceptable
Jitter (ms) (Displayed Red)	0 to 50ms Conversation was smooth.	50 to 150ms Crackling, static or intermittent delay could be reported.	> 150ms
Round Trip Time (ms) (Displayed Blue)	0 to 180ms No delay reported.	180 to 500ms Slight pause in the conversation if at the lower end of the range to more lengthy delays at the top end of the range could be reported.	> 500ms
Packet Loss (%) (Displayed Brown)	0 to 10% No drop out in conversation.	10 to 30% Drop out and missing parts of the conversation could be reported.	> 30%

Media Gateway Link Reports

You can generate the following reports for media gateways:

- Summary Media Gateway Link Report
- Detailed Media Gateway Link Report
- Trace Routes Media Gateway Link Report

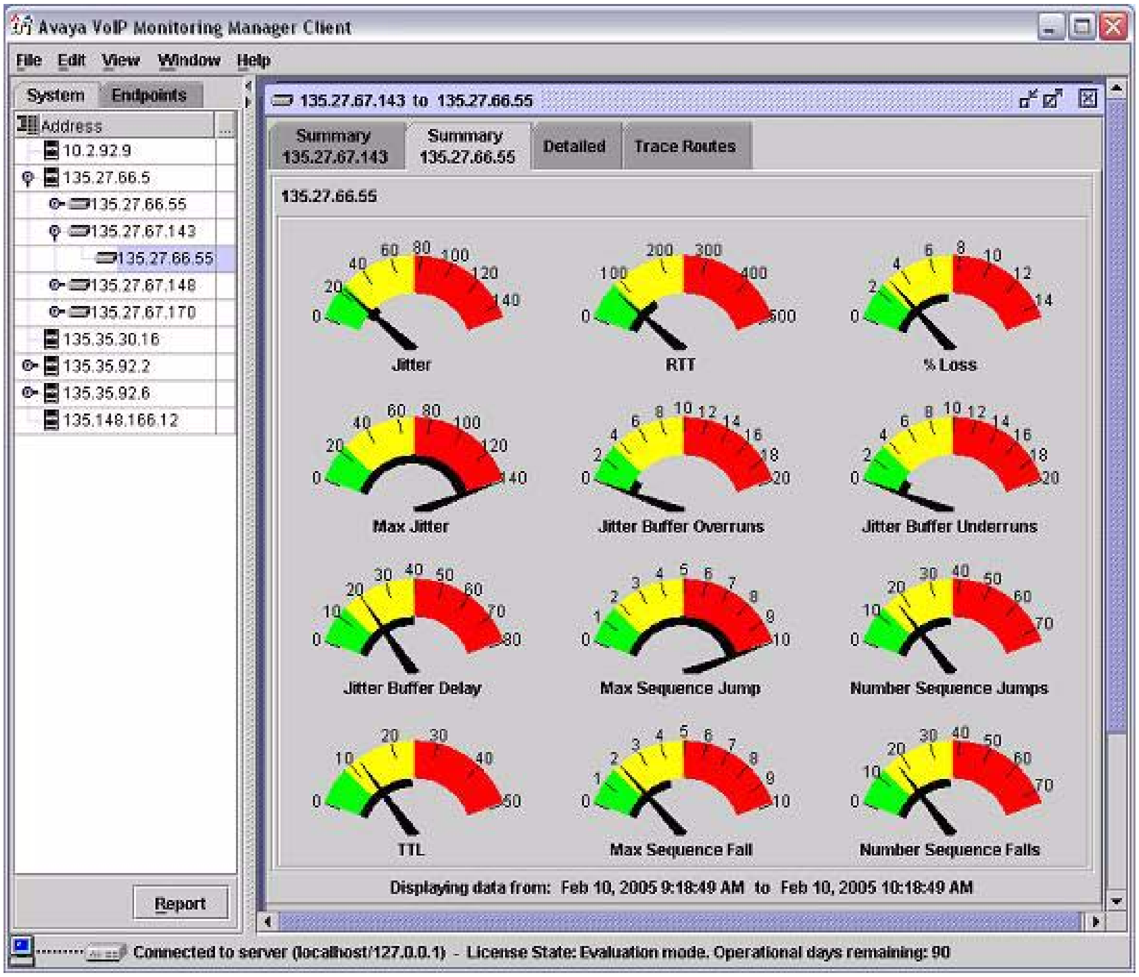
Interpreting Summary Media Gateway Link Reports

Summary Media Gateway Link reports display 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

Figure 3 shows a sample Summary Media Gateway Link report.

Figure 3: Summary Media Gateway Link Report



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

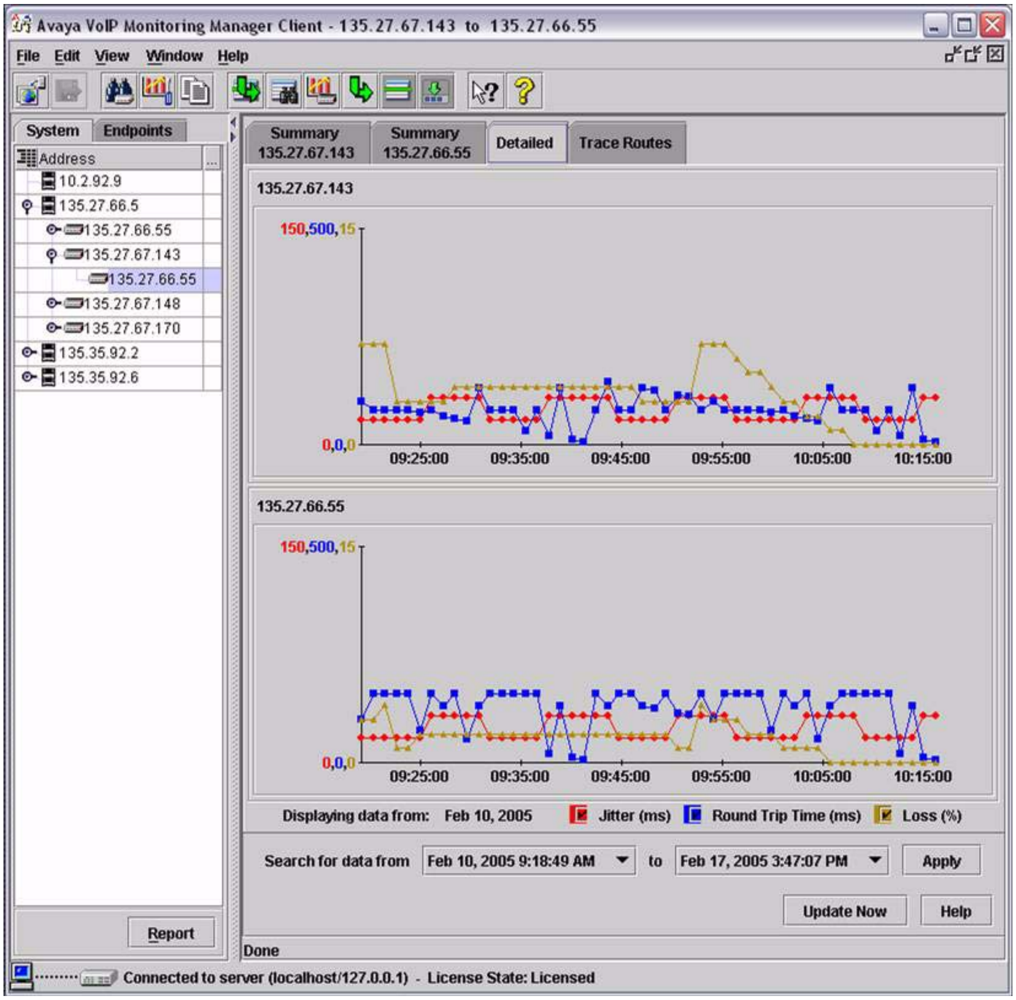
Connected to server (localhost/127.0.0.1) - License State: Evaluation mode. Operational days remaining: 90

Interpreting Detailed Media Gateway Link Reports

Detailed Media Gateway Link reports show 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 appears at the top of the report, and child endpoint appears at the bottom of the report.

Figure 4 shows a sample Detailed Media Gateway Link report.

Figure 4: Detailed Media Gateway Link Report



Avaya VoIP Monitoring Manager Client - 135.27.67.143 to 135.27.66.55

Displaying data from: Feb 10, 2005

Search for data from Feb 10, 2005 9:18:49 AM to Feb 17, 2005 3:47:07 PM

Done

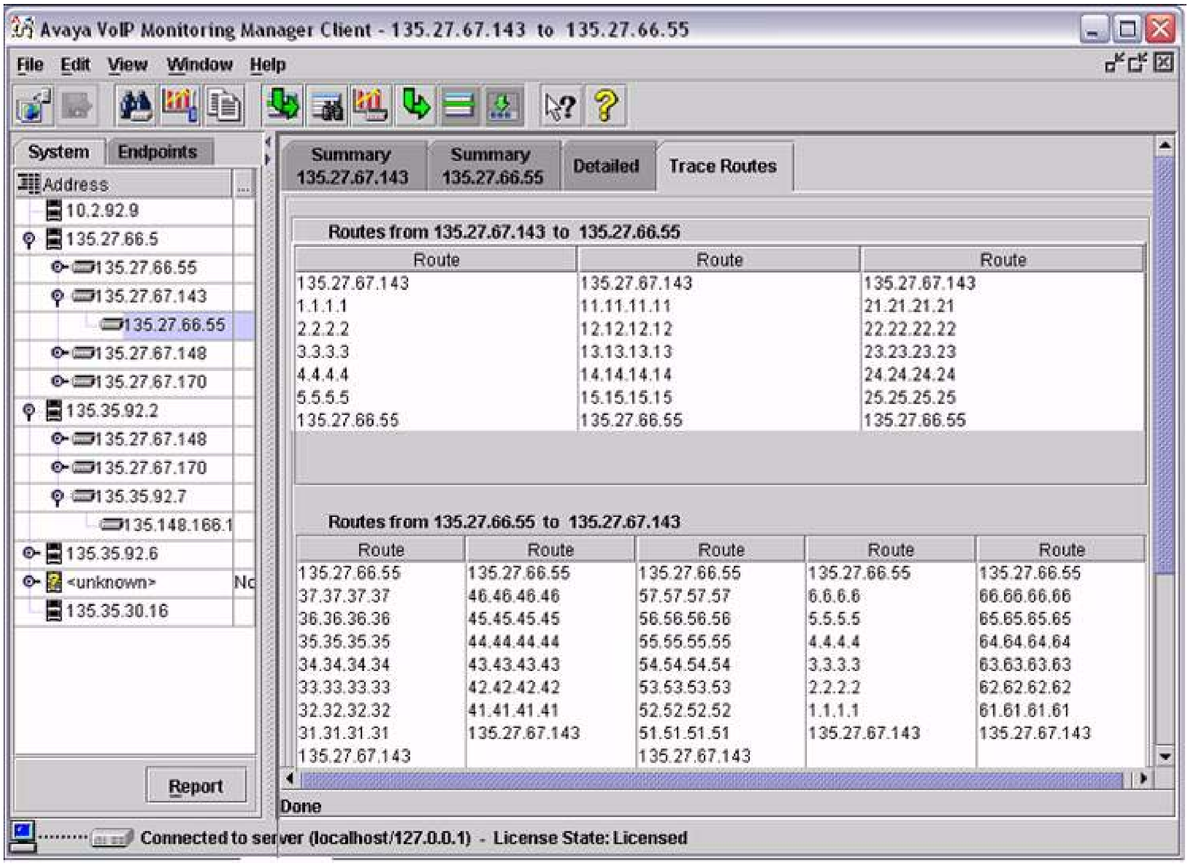
Connected to server (localhost/127.0.0.1) - License State: Licensed

Interpreting Trace Routes Media Gateway Link Reports

The Trace Routes Media Gateway Link reports show the probable routes used between the two selected media gateways.

Figure 5 shows a sample Trace Routes Media Gateway Link report.

Figure 5: Trace Routes Media Gateway Link Report



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

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		

Done

Connected to server (localhost/127.0.0.1) - License State: Licensed

Difference Between Endpoint and Session Reports

The QoS data that appears on an endpoint report is an aggregation of all the sessions that are active at this endpoint. 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. Because an endpoint can participate in multiple concurrent sessions, a high value on the report indicates that one or more of the sessions is experiencing degradation of quality. It does not indicate which 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 must narrow your search by either searching for a specific QoS value or altering the date of the report.

Glossary

802.1

The 802.1p and 8021Q metrics represents the value of incoming RTP packets of the 802.1ptag field and the 802.1Q tag field respectively. Both are a 16-bit unsigned integer.These metrics are sent for the first RTP packet received.

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

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.

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 with the Avaya VoIP Monitoring Manager.

Apache

Apache HTTP server is an open-source HTTP server that is maintained by the ApacheSoftware Foundation. A free download is available from http://www.apache.org follow the links to the HTTPD(HTTP daemon, web server).

AVAYA-VMON-MIB

The AVAYA-VMON-MIB is for the storage of RTCP data received from IP endpoints in the IP telephony system. (The ASN.1 definitions of this MIB and associated Traps are included as text files in the installation.)

C

Canonical Name (CNAME)

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.

You click on the expanding icon positioned in the far left column of the Results List to expand the tree to display 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.

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 types of payload (such as g729A, g729B, and so on). The value reported by VoIP Monitoring Manager is the sum of all types of g729 data received.

D

DiffServ 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. This value is sent for the first RTP packet received, and resent when the DSCP value has changed from the previously reported value.

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. The default value is 16ms.

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 telephony switch that manage/administers 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.

VoIP Monitoring Manager: 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.

H

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

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

HopTime (ms) The HopTime column in the Trace Route Table displays the results in milliseconds the round-trip-time of the trace route packet, from the source to each path 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. We tend to think of jitter as the statistical average variance in delivery time between packets or datagrams. Jitter displays in milliseconds.

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.

Jitter Buffer Over Runs

The number of jitter buffer over-runs metric represents the number of times during a call the jitter buffer was too small. 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 (LargestSeqFall)

The Largest Sequence Fall metric represents the number of packets that are received from when an out-of-order packet was expected to be received.

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 (LargestSeqJump)

The Largest Sequence Jump metric represents the maximum number of consecutive packets lost in the last RTCP reporting interval.

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.

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 displayed in milliseconds. 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 (NumberSeqFalls)

The number of sequence fall metric represents how many times during the RTP session there was at least 1 packet that was out of order.

Number Sequence Jumps (NumberSeqJumps)

The number of sequence jump instances metric represents how many times during the reporting interval there was at least 1 packet which was lost.

O

Octet

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

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.

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.

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 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.

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

Q

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

- Jitter is shown on the Detailed Report in red.
- Round Trip Time is shown on the Detailed Report in blue.
- Packet Loss is shown on the Detailed Report in brown.

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 (RTCP) 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.

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

Real-Time Transport Protocol (RTP)

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)

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

Round Trip Time (RTT)

Round trip time is the length of time 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. It 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.

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.

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).

RTCP Listen Port The RTCP Listen Port is the configurable port that is used to collect the RTCP packets sent by Avaya endpoints. The default port is 5005. You can change the port that is used in the RTCP Monitor Properties dialog.

RTP 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.

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?number=1889

S

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, Time-varying Data Table 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 field will be reported as enabled, disabled or unknown.

Session Table The Session Table is one of the exported tables 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, Time-varying Data Table, and the TraceRoute Table. Use the SessionID to identify the session in each table to analyze the data.

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

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.

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.

Time-To-Live (TTL) 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. 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.

TOOL The TOOL value is the name and version of the application generating the stream, e.g., 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 or 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 generally configured to be the Gateway Alarm Manager (GAM) or Network Alarm Manager (NAM) but any Trap Manager application can be used with the Avaya VoIP Monitoring Manager.

V

VoIP or Voice over Internet Protocol VoIP is an acronym for Voice over Internet Protocol. This is the technology standard that allows 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.

W

Windows SNMP Agent 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.

Index