



Avaya VoIP Monitoring Manager
Release 2.1
User Guide

555-233-510
Issue 5
June 2004

**Copyright 2004, Avaya Inc.
All Rights Reserved**

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.

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 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

Safety Requirements for Customer Equipment, ACA Technical Standard (TS) 001 - 1997

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 operate within the following parameters:

- Maximum power output: -5 dBm to -8 dBm
- Center Wavelength: 1310 nm to 1360 nm

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 and EN55022:1998.

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
- Powerline Harmonics IEC 61000-3-2
- Voltage Fluctuations and Flicker IEC 61000-3-3

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.

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 Européenne*) 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). This equipment has been certified to meet CTR3 Basic Rate Interface (BRI) and CTR4 Primary Rate Interface (PRI) and subsets thereof in CTR12 and CTR13, as applicable.

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>.

Table of Contents

<i>Preface</i>	7
The Purpose of this Manual	7
Who Should Use this Manual	7
Organization of this Manual	7
<i>Chapter 1 — What is Avaya VoIP Monitoring Manager?</i>	9
What is Avaya VoIP Monitoring Manager?	9
What You Can Do With Avaya VoIP Monitoring Manager	9
Components of Avaya VoIP Monitoring Manager	10
Avaya VoIP Monitoring Manager Server	10
Avaya VoIP Monitoring Manager RTCP Monitor	10
Avaya VoIP Monitoring Manager Client	11
Avaya VoIP Monitoring Manager Web Client	11
Server	12
Client	13
<i>Chapter 2 — Installing the Software</i>	15
Installing the Server Software	15
Ensuring Windows SNMP Agent is installed	15
Solving Installation Problems	16
Changing the RTCP Listen Port	16
<i>Chapter 3 — How to Use Avaya VoIP Monitoring Manager</i>	19
Before You Start Using Avaya VoIP Monitoring Manager	19
Configure Switch Administration Forms (SAT)	19
How to Start Avaya VoIP Monitoring Manager	21
To Start Avaya VoIP Monitoring Manager	21
View Reports	22
View the Session Data	23
Export the Data	23
Test Heading	23
Configuring the VoIP Monitoring Manager Server	24
Generating Traps & Alarms	24
Recommended Trap Settings	24
Call Traps	25
System Traps	26

<i>Chapter 4 — Interpreting Reports</i>	27
About Reports	27
Summary Reports	27
Difference Between the QoS Data for an Endpoint and a Session	28
Interpreting the Values Using Summary Reports	29
<i>Glossary</i>	33
<i>Index.</i>	47

Preface

Welcome to Avaya VoIP Monitoring Manager. This chapter provides an introduction to the structure and assumptions of this manual. It includes the following sections:

- ["The Purpose of this Manual"](#) - A description of the goals of this manual.
- ["Who Should Use this Manual"](#) - The intended audience of this manual.
- ["Organization of this Manual"](#) - A brief description of the subjects contained in the various sections of this manual.

The Purpose of this Manual

This manual contains information needed to use Avaya VoIP Monitoring Manager efficiently and effectively.

Who Should Use this Manual

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

Organization of this Manual

This manual is structured to reflect the following conceptual divisions:

- [Preface](#) - A description of the manual's purpose, intended audience, and organization.
- [What is Avaya VoIP Monitoring Manager?](#) - Includes an overview and system requirements.
- [Installing the Software](#) - Provides installation instructions.
- [How to Use Avaya VoIP Monitoring Manager](#) - Explains how to use the software.
- [Interpreting Reports](#) - Explains how to interpret the reports.
- [Glossary](#) - Provides a glossary of commonly used terms.
- [Index](#) - Provides an index of commonly used terms and where to locate them within the book.

1 What is Avaya VoIP Monitoring Manager?

This chapter provides a brief explanation about Avaya VoIP Monitoring Manager, what you can do with this tool, its components and minimum requirements.

- ["What is Avaya VoIP Monitoring Manager?"](#)
- ["Components of Avaya VoIP Monitoring Manager"](#)
- ["What You Need to Run Avaya VoIP Monitoring Manager"](#)

What is Avaya VoIP Monitoring Manager?

Avaya 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 Avaya VoIP Monitoring Manager you can view the QoS data i.e. the 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.

What You Can Do With Avaya VoIP Monitoring Manager

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, network addresses, or QoS levels.

View Reports

Once you have a list of endpoints, you can select an endpoint or endpoints in a session and view its report. The reports display the QoS data i.e. Jitter, Round Trip Time (RTT) and Packet Loss. This is particularly useful for monitoring gateways or locating problems at a particular endpoint. As you can view reports for endpoints involved in a session, this 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 SNMP Traps/Alarms, which allows the Monitoring Manager to alert you when the Jitter, RTT or Packet Loss reaches certain levels. You can routinely monitor the network, and troubleshoot problems.

Components of Avaya VoIP Monitoring Manager

The VoIP Monitoring Manager incorporates the Avaya VoIP Monitoring Manager RTCP Monitor and the Avaya VoIP Monitoring Manager Server, which accepts connections from the Avaya VoIP Monitoring Manager Client. The Server software needs to be installed onto the network to work correctly. You will also need to have a Windows SNMP Agent installed on the Server. The components and their relationship are described in more detail as follows:

Avaya VoIP Monitoring Manager Server

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

Avaya VoIP Monitoring Manager 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 SNMP.

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.)

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 and does not use the Windows SNMP service. The data that is displayed is gathered from the Server. The Client may be installed on the same machine as the Server, or it may be installed on another machine on the network. It is possible for the Server and the Client to communicate over a dial-up connection.

Avaya VoIP Monitoring Manager Web Client

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

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

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; connect to a new server, and export.

What You Need to Run Avaya VoIP Monitoring Manager

The minimum system requirements to install and operate Avaya VoIP Monitoring Manager for the Server and Client are listed. Operating System.

Server

Server	
Operating System	Windows 2000 Server (Preferred)
Software	The Simple Network Management Protocol Agent (SNMP Agent) is the Windows Service that runs on your computer. It is provided with the Windows 2000 CD but is not installed by default. When installing the VoIP Monitor Manager, you will be prompted to install it if it is not installed.
Processor	1.3 GHz Pentium 3 or higher
RAM	1.5 GB
Video	SVGA 800 x 600 display
Hard Drive	40 GB
Port	The Client and Server software communicate using Java Remote Method Invocation (RMI), and uses the port 1099 on the machine on which the Server is running. If this port is not available, the 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.

Client

Client	
Operating System	Windows 2000 or Windows XP
Processor	600 MHz Pentium 3 or higher
RAM	256 MB
Video	SVGA 800 x 600 display
Hard Drive	1 GB
Port	The Client and Server software communicate using Java Remote Method Invocation (RMI), and uses the port 1099 on the machine on which the Server is running. If this port is not available, the 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.

2 Installing the Software

This chapter explains how to install Avaya VoIP Monitoring Manager and includes the following sections:

- ["Installing the Server Software"](#)
- ["Installing the Client Software"](#)
- ["Solving Installation Problems"](#)

Installing the Server Software

The Avaya VoIP Monitoring Manager Server needs to be installed on the VoIP network. If you are downloading the program from a web site, select to **Run this program from its current location**. The installation program will start 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 on the saved program to start the install. If you are installing the program from a CD-Rom, insert the CD into your drive and follow the instructions.

Ensuring Windows SNMP Agent is installed

The installation will check to see if the Windows SNMP Agent is installed. The Windows SNMP Agent must be installed for the Avaya VoIP Monitoring Manager Server to function. If the Windows SNMP Agent is not installed, the **Add/Remove Windows Components** will automatically start and you will be prompted for the Windows 2000 CD location so that you can install the Windows SNMP Agent.

To see if the Windows SNMP Agent is installed:

1. Click **Start > Settings > Control Panel > Administrative Tools > Services**.
2. Scroll down until you see the SNMP Service 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. If it is listed but not set to run automatically, you will need to set it to start automatically as explained in ["Solving Installation Problems" on page 16](#).

Installing the Client Software

The Avaya VoIP Monitoring Manager Client can be installed on the same machine as the Avaya VoIP Monitoring Manager Server, or it may be installed on another machine on the network. You install the Client software using one of the options as described above for Installing the Server software.

Solving Installation Problems

Avaya VoIP Monitoring Manager Server needs to be installed on the network. The Server software and the **Windows SNMP Agent** must be running before you can start the Client.

Changing the RTCP Listen Port

If you need to change the RTCP Listen port, open the Server Options Dialog and change the Listen Port (default: 5005) as follows.

To Change the RTCP Listen Port:

1. On the **Edit** menu, click **Options**.
The **Server Options Dialog** displays.
2. Click the **RTCP** tab and enter the new **RTCP Listen Port**.
3. Click **OK** to save the changes and close the dialog or **Cancel** to close without saving.

Avaya VoIP Monitoring Manager Server will reset the properties and attempt to re-connect to the Windows SNMP Agent based on the new properties.



CAUTION

Changing the RTCP port displays a warning indicating it must match the port configured on the Avaya Communications Manager Server. See <http://www.iana.org/assignments/port-numbers> and your Avaya Communications Manager documentation. It is unusual to change the listen port from the default of 5005 as the default should be suitable in most situations.

Note: A SNMP Community ID with write privileges must be configured before changes can be applied.

Set Windows SNMP Agent to Start Automatically

You need to have the Windows SNMP Agent installed and running on the Avaya VoIP Monitoring Manager Server before you start the Client. It enables the RTCP Monitor to publish the data.

To check to see if the Windows SNMP Agent is **Installed** and **Set to Start Automatically**:

1. Click **Start > Settings > Control Panel > Administrative Tools > Services**.
2. Scroll down until you see the SNMP Service 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. If it is included but not set to run automatically, you will need to change its properties.

To Set Windows SNMP Agent to Start Automatically:

1. From Windows Service dialog as explained above, right-click on **SNMP** and select **Properties** from the context menu. The SNMP Service Properties dialog opens.
2. Select **Automatic** from the **Startup Type** drop down list and click **OK**.

Check for a Valid Community IDs

The Community IDs assigned for your Windows SNMP Agent must match the Community IDs defined in the **Server Options dialog**. By default, the Community ID with read-only privileges is 'public', and the Community ID with read-write privileges is 'private', but these may have been changed.

Read privileges are required for searching and deploying data. Write privileges are required for changing configuration options.

To Check for Valid Community IDs:

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.



CAUTION

The Community IDs in the Server Options dialog must match the IDs configured in the Windows SNMP Service in the list of Community Names.

3 How to Use Avaya VoIP Monitoring Manager

This chapter explains how to use Avaya VoIP Monitoring Manager for searching endpoints and viewing reports. It includes the following sections:

- ["Before You Start Using Avaya VoIP Monitoring Manager"](#)
- ["How to Start Avaya VoIP Monitoring Manager"](#)

Before You Start Using Avaya VoIP Monitoring Manager

Before you start the Avaya VoIP Monitoring Manager Client:

- Ensure that the Avaya VoIP Monitoring Manager Server and the Windows SNMP Agent are installed on the server PC.
- Configure the Switch Administration Forms (SAT).

Configure Switch Administration Forms (SAT)

There are two Switch Administration Forms (SAT) that need to be configured to send RTCP reports to the RTCP Monitor.

These forms are called:

- System-Parameters IP-Options Form
- IP-Network-Region Form

Configure IP-Network-Region Form

- Set the **RTCP 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.

Figure 1. IP Networks Region Form

1 | **2** |

IP Network Region

Region: **1**
 Name: **Master RegionMaster**

Audio Parameters
 Codec Set: **1**
 Location:
 UDP Port Range
 Min: **2050**
 Max: **3027**

DiffServ/TOS Parameters
 Call Control PHB Value: **34**
 VoIP Media PHB Value: **46**
 BBE PHB Value: **43**

Resource Reservation Parameters
 RSVP Enabled? **y**
 RSVP Refresh Rate(secs): **15**
 Retry upon RSVP Failure Enabled? **y**
 RSVP Profile: **guaranteed-service**

802.1p/Q Enabled? **n**
 Call Control 802.1p Priority: **7**
 VoIP Media 802.1p Priority: **6**
 802.1Q VLAN: **200**

Direct IP-IP Audio Connections? **y**
IP Audio Hairpinning? **y**
RTCP Enabled? **y**
RTCP Monitor Server Parameters
Use Default Server Parameters? **y**

Do Not Want to Set Default Parameters to Yes

In some cases, you may not want to set the Default Parameters to yes, set the field to **n (no)** and specify the IP address of the Windows 2000 PC running the Server for that network region.

This situation might be where you have multiple Servers 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 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.

Configure 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.

Figure 2. System-Parameters IP-Options Form

```

change system-parameters ip-options                                     page 1 of 1

                                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: 123.123.123.123
Default Server Port: 5005
Default RTCP Report Period(secs): 5
  
```

How to Start Avaya VoIP Monitoring Manager

To Start Avaya VoIP Monitoring Manager

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

Avaya VoIP Monitoring Manager Server starts.

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

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

Search for Endpoints

The first action required when using the VoIP Monitoring Manager Client is to search for endpoints. The search dialog enables you to search for endpoints active in the past or between a date range. You can also use the advanced search options to narrow your search to match a specific phone number, network address or QoS threshold. Once you have completed your search, the Results lists updates with a list of endpoint(s) where you can select an endpoint from to view its Quality of Service (QoS) data in a report format.

To Run a Search

1. From the Search dialog, click the **In the last** 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.

If you want to select a date range, click **From** and then click the calendar(s) drop down arrow to select the start (**From**) and end date (**To**) of the range. You can select the day, months, hours, minutes, seconds and AM/PM.

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

Once you run the search, you can view reports on selected endpoints and endpoints involved in a session.

View Reports

There are two types of reports, Summary Reports and Detailed 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 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.

How To View a Report

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 enables.
2. Click **Report**. The Report opens, displaying a summary of the QoS data.

To view a Detailed Report or the Session Properties, click its tab on top of the dialog.

View the Session Data

Reports can display both endpoints involved in a session. The reports display 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 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. 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

1. Click on the expanding icon positioned in the far left column of the Results List. A sub list displays.
2. Select a **child endpoint** from the sub list.
3. Click the Report button. The reports display.

Export the Data

You can export the data in the results list and/ or a from a single report to a comma separated value (csv) file. You can open this file 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 3 tables:

- Session Table
- TimeStamped Data
- Trace Route Table

Test Heading

To Export Data

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

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.

Configuring the VoIP Monitoring Manager Server

This section provides brief information for working with the server. Installing the server and performing the complete configuration is not within the scope of this guide, but changing some settings can help you to obtain better reports.

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. Over time, you will likely be able to fine-tune these settings to highlight abnormal operation.

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.

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.

Table 1. 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

System warning interval: 100 warnings, 24 hours

Terminal warning interval: 50 warnings, 24 hours

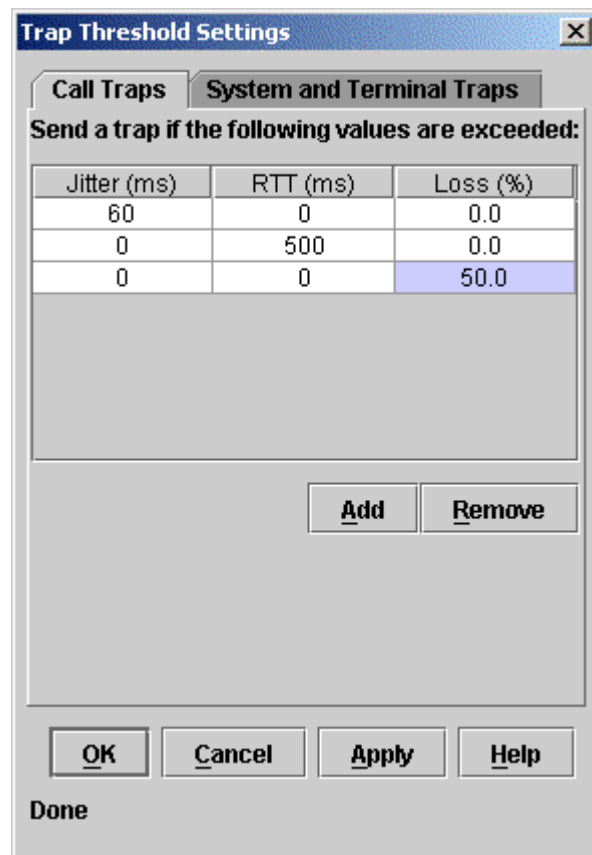
Call Traps and System Traps (following) show examples of dialogs with the suggested values.

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 dialog 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.

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.

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.

Trap Threshold Settings

Call Traps | **System and Terminal Traps**

Warnings

Log a warning if the following are exceeded:

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

Add **Remove**

System and Terminal Traps

Send Trap if:

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

Add **Remove**

OK **Cancel** **Apply** **Help**

Done

Example

The example dialog 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.

4 Interpreting Reports

This chapter provides a description on how to interpret the reports. It includes the following sections:

- ["About Reports"](#)
- ["Interpreting the Values Using Summary Reports"](#)
- ["Interpreting the Values Using Detailed Report"](#)

About Reports

As explained in the previous section, there are two types of reports, Summary Reports and Detailed 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. Each of the QoS parameters is displayed on a separate gauge, one for each of the three QoS parameters. You can alter these values using the Report Properties dialog accessed from the Edit menu.

Summary Report Features:

- Displays an average, minimum and maximum value for each QoS parameter
- Date range
- Type of endpoint
- Phone number and IP Address

Detailed Reports

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.

Each of the QoS parameters is represented on the graph by a different color. This makes it easier for you 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.

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

Detailed Report Features:

- Displays the QoS data as it changes during the call and shows when this occurred.
- QoS data is color coded.
- Ability to uncheck the display of one or more of the QoS data.
- A tool tip enables you to point your mouse at the data on the line graph to see the exact data measured.
- Alter the date range to show more or less detail.

Difference Between the QoS Data for an Endpoint and a Session

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

As 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, session reports displays the QoS data as experienced by both endpoints for that session only. To assist with isolating your analysis, use the advanced search features to narrow down the search for a specific QoS value or alter the date range of the reports.

Interpreting the Values Using Summary Reports

You interpret the Summary Reports by noting where the needle on the gauge 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 minimum and maximum values measured.

Figure 3. Summary Report

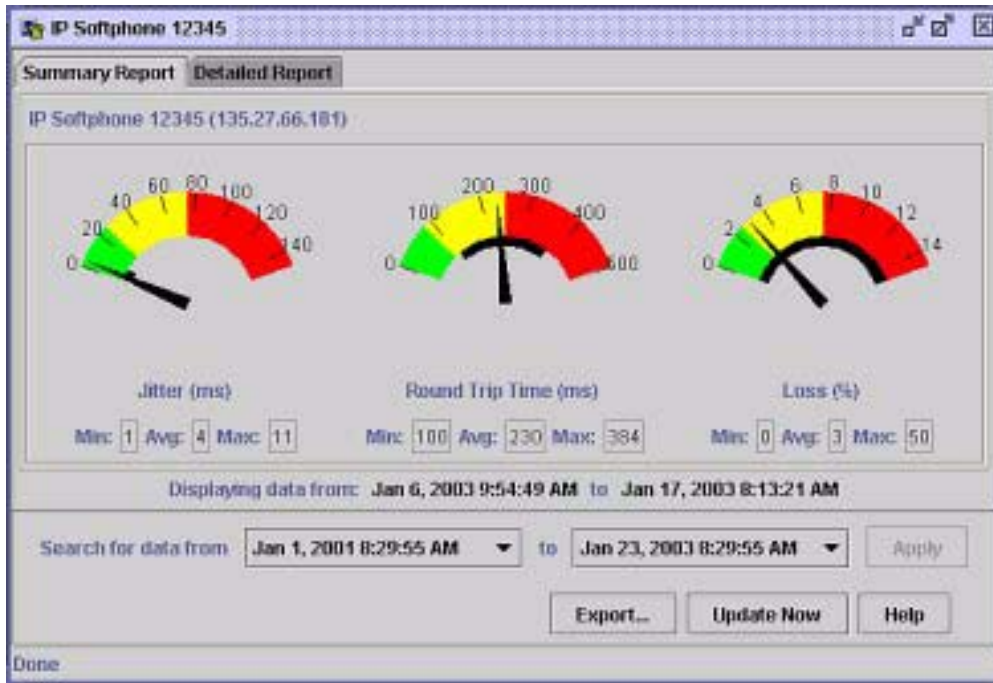


Table 2. The Values for the Summary Reports

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 the Values Using Detailed Report

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

Figure 4. Detailed Report

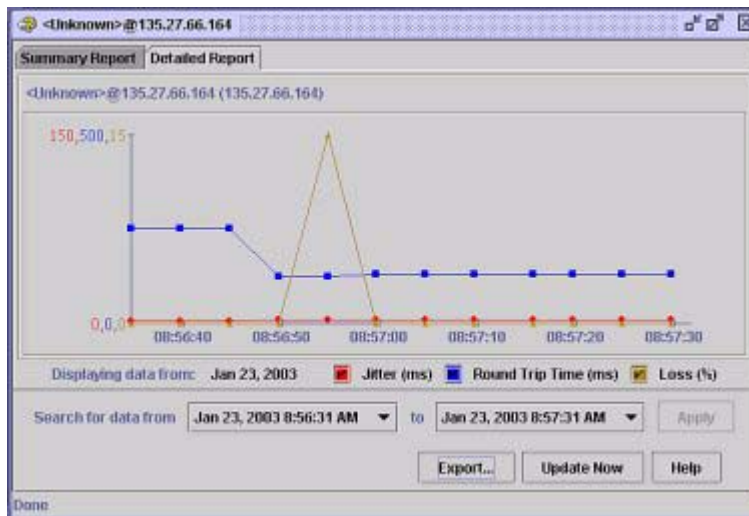


Table 3. The Values for Detailed Reports

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%

Glossary

This chapter provides a description of the key terms used in this document.

802.1

The 802.1p and 802.1Q metrics represent the value of incoming RTP packets of the 802.1p tag 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.

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

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 Apache Software 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.)

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

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

**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.

Octet

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

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, TimeStamped 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, timestamped 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.
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.

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
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 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 related to the Session. It will display in Microsoft Excel at the top of the same worksheet as the TimeStamped and Trace Route Table. It contains the following information:

- SessionID
- ParticipantID
- StartTime
- EndTime
- RcvrIPAddr
- CNAME
- RcvrPHONE
- TOOL
- Payload
- Gatekeeper
- DiffServ Code Point
- 802.1p
- 802.1Q
- Media Encryption
- Echo Tail Length
- Silence Suppression
- Acoustic Echo Cancellation

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.

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.

TimeOffset

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

TimeStamped Data Table

The TimeStamped Data Table is one of the exported tables containing data related to the call. The table displays all the data associated at a given point in time. The time is measured from the beginning of the session. It 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.

The SessionID and the ParticipantID columns link the information in the TimeStamp Data Table to the Session Table. If you have a session of interest in the Session Table, use the Ids to analyze the data.

The TimeStamped Data contains the following information:

- SessionID
- ParticipantID
- TimeOffset
- Jitter
- RTT
- LostPackets
- Packets
- RSVP
- LargestSeqJump
- NumberSeqJumps
- LargestSeqFall
- NumberSeqFalls
- Time-To-Live
- MaxJitter
- JitterBufferOverRuns
- JitterBufferUnderRuns

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 data related to the route of the call. It will display in Microsoft Excel below the TimeStamped Data Table. It contains the following information:

- SessionID
- ParticipantID
- HopCount
- HopTime (ms)
- HopAddress

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.

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.

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

Numerics

802.1D [33](#)

A

Acoustic Echo Cancellation [33](#)

Add/Remove Windows Components [15](#)

Advanced Search [2](#)

Applet [11](#)

AVAYA-VMON-MIB [33](#)

B

blue [28](#)

brown [28](#)

C

Canonical Name (CNAME) [34](#)

Child Endpoint [34](#)

Client [11](#)
installing [16](#)

CName [34](#)

Codec [34](#)

components
Client [10](#)
RTCP Monitor [10](#)
Server [10](#)

Configure
Switch Administration Forms [19](#)

crackling [31](#)

D

delay
no delay [31](#)

detailed
interpreting [29](#)

Detailed Reports [22](#), [28](#)

dial-up connection [11](#)

difference between endpoint & session [28](#)

DiffServ Code Point [34](#)

disk space requirements [12](#), [13](#)

downloading this software, explained [15](#)

drop out [29](#), [31](#)

DSCP [34](#)

E

Echo Tail Length [34](#)

endpoint [28](#)
difference between session and [28](#)

EndTime [35](#)

Export [10](#)

Export the Data [10](#)

F

Framesize [35](#)

G

Gatekeeper [35](#)

Gateway [35](#)

generating automatic alarms [10](#)

Glossary [33](#)

GUI [11](#)

H

HopAddress [35](#)

HopCount [36](#)

HopTime (ms) [36](#)

I

installing
client software [16](#)
server software [15](#)
SNMP agent [15](#)

intermittent delay, QoS values indicating [29](#),
[31](#)

interpreting reports [29](#)

IP-Network-Region Form [20](#)

J

jitter [9](#), [28](#), [29](#)

Jitter buffer delay [40](#)

Jitter Buffer Over Runs [36](#)

Jitter Buffer Under Runs [36](#)

L

Largest Sequence Fall (LargestSeqFall) [36](#)

Largest Sequence Jump (LargestSeqJump) [37](#)

Listen Port [16](#)

loss [29](#)

M

match

 phone number, network address, QoS [9](#)

Maximum Jitter [37](#)

Media Encryption [37](#)

missing parts of the conversation [29](#)

N

Number Sequence Falls (NumberSeqFalls) [37](#)

Number Sequence Jumps
 (NumberSeqJumps) [37](#)

O

operating system requirements [12](#)

P

Packet [37](#)

Packet Loss [38](#)

packet loss [9](#), [28](#)

Packetization delay [40](#)

Parent Endpoint [38](#)

ParticipantID [38](#)

pauses

 QoS values indicating [29](#)

pauses, QoS values indicating [31](#)

Payload [38](#)

Perceived Delay [38](#)

processor requirements [12](#), [13](#)

Propagation delay [40](#)

purpose of Avaya VoIP Monitoring Manager [10](#)

purpose of this manual [7](#)

Q

Quality of Service (QoS) [38](#)

query

 customizing using filters [9](#)

R

RAM requirements [12](#), [13](#)

RcvrIPAddr [39](#)

RcvrPHONE [39](#)

Real-Time Transport Control Protocol
 (RTCP) [39](#)

Real-Time Transport Protocol (RTP) [39](#)

red [28](#)

reports

 interpreting [29](#)

requirements [12](#)

Resource ReSerVation Protocol (RSVP) [39](#)

Results List [22](#)

Round Trip Time [28](#), [29](#)

Round Trip Time (RTT) [40](#)

RSVP Status [41](#)

RSVP status [9](#)

RTCP Listen Port [42](#)

RTCP monitor [10](#)

RTP MIB [10](#), [42](#)

RTP Session [42](#)

S

Server [10](#)

Session [28](#)

Session Table [43](#)

session, difference between endpoint and [28](#)

SessionID [42](#)

Silence Suppression [42](#)

Simple Network Management Protocol
 Agent [12](#)

SNMP

- ensuring agent is installed [15](#)

SNMP agent

- see if it is running [17](#)

SNMP traps, generating automatically [10](#)

software requirements [12](#)

Start

- Before [19](#)

- How to [19](#)

StartTime [43](#)

static, QoS values indicating [31](#)

summary

- interpreting [29](#)

Summary Reports [22](#)

System -Parameters IP-Options Form [21](#)

T

TimeOffset [43](#)

TimeStamped Data Table [44](#)

Time-To-Live (TTL) [45](#)

TOOL [45](#)

Trace Route Table [45](#)

Transport delay [40](#)

Trap or Alarm [46](#)

traps, generating automatically [10](#)

troubleshooting

- installation problems [16](#)

V

video requirements [12](#), [13](#)

View Reports [9](#), [22](#)

Voice Codec [9](#)

VoIP or Voice over Internet Protocol [46](#)

W

Web Client [11](#)

web site, if you download this product from
[15](#)

who should use this manual [7](#)

Windows 2000 [12](#)

Windows SNMP Agent [10](#), [46](#)

