Avaya™ VoIP Monitoring Manager User Guide

555-233-510
Issue 1
June 2002

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.

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 Web site:

http://www.avaya.com/support/

If you are:

- Within the United States, click *Escalation Lists*, which includes escalation phone numbers within the USA.
- Outside the United States, click *Escalation Lists* then click *Global Escalation List*, which includes phone numbers for the regional 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.

Voice Over Internet Protcal (VoIP)

If the equipment supports Voice over Internet Protocol (VoIP) facilities, you may experience certain compromises in performance, reliability and security, even when the equipment performs as warranted. These compromises may become more acute if you fail to follow Avaya's recommendations for configuration, operation and use of the equipment. YOU ACKNOWLEDGE THAT YOU ARE AWARE OF THESE RISKS AND THAT YOU HAVE DETERMINED THEY ARE ACCEPTABLE FOR YOUR APPLICATION OF THE EQUIPMENT. YOU ALSO ACKNOWLEDGE THAT, UNLESS EXPRESSLY PROVIDED IN ANOTHER AGREEMENT, YOU ARE SOLELY RESPONSIBLE FOR (1) ENSURING THAT YOUR NETWORKS AND SYSTEMS ARE ADEQUATELY SECURED AGAINST UNAUTHORIZED INTRUSION AND (2) BACKING UP YOUR DATA AND FILES.

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.

The equipment described in this manual complies with standards of the following organizations and laws, as applicable:

- Australian Communications Agency (ACA)
- American National Standards Institute (ANSI)
- Canadian Standards Association (CSA)
- Committee for European Electrotechnical Standardization (CENELEC) – European Norms (EN’s)
- Digital Private Network Signaling System (DPNSS)
- European Computer Manufacturers Association (ECMA)
- European Telecommunications Standards Institute (ETSI)
- FCC Rules Parts 15 and 68
- International Electrotechnical Commission (IEC)
- International Special Committee on Radio Interference (CISPR)
- International Telecommunications Union - Telephony (ITU-T)
- ISDN PBX Network Specification (IPNS)
- National ISDN-1
- National ISDN-2
- Underwriters Laboratories (UL)

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 Laser products, equipment classification and requirements:

- IEC 60825-1, 1.1 Edition
- 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

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.

This equipment complies with Part 68 of the FCC Rules. On the rear 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.

The REN is used to determine the quantity of devices which 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 table.

Manufacturer’s Port Identifier	FIC Code	SOC/REN/ A.S. Code	Network Jacks
Off/On premises station	OL13C	9.0F	RJ2GX, RJ21X, RJ11C
DID trunk	02RV2-T	0.0B	RJ2GX, RJ21X
CO trunk	02GS2	0.3A	RJ21X
CO trunk	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, 1KN, 1SN	6.0F	RJ48C, RJ48M
120A2 channel service unit	04DU9-DN	6.0Y	RJ48C

If the terminal equipment (for example, the MultiVantage^{TM} Solution equipment) 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.

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 digital apparatus does not exceed Class A limits for radio noise emission set out in the radio interference regulation of the Canadian Department of Communications.

Le Présent Appareil Nomérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils manicures de la class A préscrites dans le reglement sur le brouillage radioélectrique édicté par le ministére des Communications 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://support.avaya.com/elmodocs2/DoC/SDoC/index.jhtml/

All MultiVantage™ system products 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.

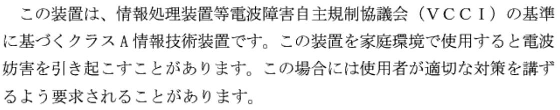
European Union Declarations of Conformity

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). 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) signed by the Vice President of MultiVantage™ Solutions research and development, Avaya Inc., can be obtained by contacting your local sales representative and are available on the following Web site:
http://support.avaya.com/elmodocs2/DoC/IDoC/index.jhtml/

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。

Network Connections

Digital Connections - The equipment described in this document can be connected to the network digital interfaces throughout the European Union.
Analogue Connections - The equipment described in this document can be connected to the network analogue interfaces throughout the following member states:

Belgium	Germany	Luxembourg
Netherlands	Spain	United Kingdom

LASER Product

The equipment described in this document may contain Class 1 LASER Device(s) if single-mode fiber-optic cable is connected to a remote expansion port network (EPN). The LASER devices operate within the following parameters:

- Maximum power output –5 dBm to -8 dBm
- Center Wavelength 1310 nm to 1360 nm
- CLASS 1 LASER PRODUCT IEC 60825-1: 1998

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

To order copies of this and other documents:

Call: Avaya Publications Center
Voice 1.800.457.1235 or 1.410.568.3680
FAX 1.800.457.1764 or 1.410.891.0207
Write: Globalware Solutions
200 Ward Hill Avenue
Haverhill, MA 01835 USA
Attention: Avaya Account Management
E-mail: totalware@gwsmail.com

Table of Contents

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.**
- **Understanding the Graphs -** Explains how to interpret the graphs.
- **Glossary -** Provides a glossary of commonly used terms.

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?**
- **What you can do with Avaya™ VoIP Monitoring Manager?**
- **Avaya™ VoIP Monitoring Manager components**
- **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, in an easy to use interface.

Avaya™ VoIP Monitoring Manager is able to display the QoS data such as Jitter, Round Trip Time (RTT) and Packet Loss experienced at the Endpoints or during a Session. It also shows the Voice Codec used and the RSVP status. It displays the QoS data in real-time or for historical data. With this information, you can begin to troubleshoot and isolate problems.

What You Can Do With Avaya™ VoIP Monitoring Manager

Query Endpoints

- Currently Active Endpoints or Historical Endpoints in a given date range
- Active Endpoints selected by IP Address, Phone Number or Host Name
- Historical Endpoints selected by IP Address, Phone Number or Host Name

Customize Query to Filter Based on QoS data

When searching for Active or Historical Endpoints, you can filter the query to display only those Endpoints with a set QoS level. This is particular useful for isolating problems on a Gateway where you have multiple Sessions and you need to narrow the query. A Session is a VoIP connection between two IP Endpoints.

Monitor an Endpoint

You can view the QoS data for an Active Endpoint on a graph. This is particular useful for monitoring Gateways or locating problems at a particular Endpoint. You can view multiple Endpoint graphs simultaneously.

Monitor a Session

You can view the QoS data for a complete Active Session on a graph. Viewing the data for a Session will assist with determining problems that occur between two Endpoints or in an isolated area of the network. You can view multiple Session graphs simultaneously.

Review Historical QoS Data

You can analyze the QoS data for Historical Endpoints and Sessions. This allows you to troubleshoot problems with any calls, even when they have already finished.

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.

Components of Avaya™ VoIP Monitoring Manager

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

Avaya™ VoIP Monitoring Manager RTCP Monitor

The RTCP Monitor is implemented as a Windows SNMP Agent. This Agent listens on a configurable port number (default 5005) for the RTCP packets from the Avaya Endpoints and stores the data in:

- The RTP MIB, which includes information for the active RTP Sessions. (RFC 2959 located at http://www.ietf.org/rfc/rfc2959.txt)
- The proprietary AVAYA-VMON-MIB which stores the historical data. (The ASN.1 definitions of this MIB and associated traps are included as text files in the installation)

Avaya™ VoIP Monitoring Manager Server

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

Avaya™ VoIP Monitoring Manager Client

The Avaya™ VoIP Monitoring Manager Client provides the graphical user interface (GUI) for Avaya™ VoIP Monitoring Manager. 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 Avaya™ VoIP Monitoring Manager Server. The Client may be installed on the same machine as the Avaya™ VoIP Monitoring Manager 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.

What You Need to Run Avaya™ VoIP Monitoring Manager

The minimum system requirements to install and operate Avaya™ VoIP Monitoring Manager are as follows:

Operating System

Windows 2000

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

400 MHz Pentium II or higher compatible Pentium

RAM

28 MB (256 MB preferred)

Video

SVGA 800 x 600 display

Free Disk Space

500 MB

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 automatically start and install the Avaya™ VoIP Monitoring Manager Server.

Alternatively, you can select to **save the file to disk** which maybe 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 change its properties.

   — Right-click on SNMP and select **Properties** from the context menu. The SNMP Service Properties dialog opens.

   — Select **Automatic** from the Startup Type drop down list and click **OK**.

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 Avaya™ VoIP Monitoring Manager Client.

Changing Avaya™ VoIP Monitoring Manager Server Properties

If you need to change the Server properties, open the Server properties dialog and change the SNMP Agent Community ID (default: public) and the RTCP Listen Port as follows:

To Change Avaya™ VoIP Monitoring Manager Server Properties

1. From the VoIP Monitoring Manager Server dialog, click **Properties**.

   The VoIP Monitoring Manager Server properties displays.

2. Type in a value in either the **SNMP Agent Community ID** or the **RTCP Listen Port** field. The Community ID must match as those defined in the Windows SNMP Service Properties dialog.

3. Click **OK** to save the changes 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 will result in a warning that it must match the port configured on the Avaya Call Processing. See http://www.iana.org/assignments/port-numbers and your Avaya Call Processing documentation. Also when entering a Windows SNMP Agent Community ID ensure it has write access (Default:private). It is unusual to change the listen port from the default 5005.

See if the Windows SNMP Agent is Running

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 Running

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.
   - **-** Right-click on **SNMP** and select **Properties** from the context menu. The SNMP Service Properties dialog opens.
   - **-** Select A**utomatic** from the **Startup Type** drop down list and click **OK**

Check for a Valid Community ID

The Community ID assigned for your Windows SNMP Agent must match the Community ID defined in the Avaya™ VoIP Monitoring Manager Server Properties dialog. By default it is public but it may have been changed.

To Check for a Valid Community ID

1. Click **Start > Settings > Control Panel > Administrative Tools >Services.**
2. Scroll down and select the **SNMP Service**.
3. Right-click on SNMP Service and select **Properties** from the context menu.
4. Select the **Security** tab.

   The Avaya™ VoIP Monitoring Manager Server Properties dialog must have a Community ID from the list of Community Names.

3 How to Use Avaya™ VoIP Monitoring Manager

This chapter explains how to use Avaya™ VoIP Monitoring Manager for querying Endpoints and to produce active or historical reports. It includes the following sections:

- **Start Using the VoIP Monitoring Manager**
- **Run a Query on Active Endpoints**
- **Run a Query on Historical Endpoints**
- **View QoS Data**
- **View Session Data**

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 network and running. Once you start the Avaya™ VoIP Monitoring Manager Client, you can run a Query, monitor Active Sessions and Endpoints, review Historical Endpoints or generate Traps/Alarms.

Start Avaya™ VoIP Monitoring Manager

To Start Avaya™ VoIP Monitoring Manager

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

   Avaya™ VoIP Monitoring Manager Server starts.

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

   Avaya™ VoIP Monitoring Manager Client starts. Now you can Query the Endpoints and then view the Endpoint or Session Data in a graphical format.

Run a Query on Active Endpoints

You run a Query to update the Query Results List with the Active Endpoints. Then you select an Endpoint from the list and click the Endpoint Data button to view the Quality of Service (QoS) data.

To Run a Query for Active Endpoints

1. From the Query dialog, select the query type option **All Endpoints**. The default setting is All (Active) Endpoints. If the Query dialog is not visible on the screen, click the New Query button to display the Query dialog.
2. Click the **Run** button.

   The Query Results List updates with a list of Active Endpoints. It will also list the Endpoint type, IP address and phone number. Now, you can select the Endpoint from the list and click the Endpoint Data button to view the QoS data for that Endpoint.

Run a Query on Historical Endpoints

You run a Query that specifies a previous date range. Once again the Query updates the Query Results List but with the Historical Endpoints. Then you select an Endpoint from the list and click the Endpoint Data button to view the QoS data for the Historical Endpoints.

To Run a Query on Historical Endpoints

1. From the Query dialog, select the query type option **All Endpoints**. (The default setting runs a query on All Endpoints.) If the Query dialog is not visible on the screen, click the New Query button to display the Query dialog.
2. Select the **Endpoint active in date range** radio button.
3. Click the top date drop-down arrow to access the calendar and time for the start period of your Query. You can select hours, minutes, seconds and AM/PM. You can also use the arrow buttons to scroll through the months and years. Once you have adjusted the time you must select the day.
4. Click outside the calendar window to close the calendar.

5. Click the bottom date drop-down arrow to access the calendar and time for the finishing period of your Query as described above.

   The top and bottom date fields display the selected date.

6. Click **Run and Close**.

   The Query Results List updates with a list of Historical Endpoints. It will also list the Endpoint Type, IP Address, Phone Number and start and end date. To view the QoS data, select the Endpoint and click the Endpoint Data button.

View the Qos Data for Endpoints

Once you run a Query, and the Query Results List updates, you select an Endpoint, and click the Endpoint Data button. A graph will open displaying the QoS data for the selected Endpoint. Alternatively, you can click the Endpoint Data icon or Session Data icon on the Tool Bar or from the Action menu.

To View the QoS Data for Active Endpoints

1. From the Query Results List, select an **Endpoint**.

   The Endpoint Data button enables.

2. Select the **Endpoint Data** button.

   The Active Endpoint graph opens, displaying the QoS data.

View the Session Data

To view the QoS data for a Session, you first need to run a query to update the Query Results List with the Endpoints. Then, click on the icon positioned in the far left column in the Query Results List to expand the tree. A sub list displays of child Endpoints that were involved in the Session with the parent Endpoint of the tree. You select a child Endpoint and click the Session Data button.

The terms parent and child Endpoints are purely for describing the way Endpoints are displayed in the Query 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 Query.

To View the Session Data

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

   A sub list displays.

2. Select a **child Endpoint** from the sub list.

   The Session Data button enables.

3. Click the **Session Data** button.

   The graph opens.

4 Understanding Graphs

This chapter provides a description on how to understand and interpret the active and historical graphs. It includes the following sections:

- **Understanding Active Graphs.**
- **Interpreting the Values on an Active Graph.**
- **Understanding Historical Graphs.**
- **Interpreting the Values on Historical Graphs.**

Understanding Active Graphs

The graphs enable you to view QoS data for Active Endpoints. The Active Endpoint graphs display as line graphs and the Session graphs display each Endpoint on a separate line graph.

Sampling Begins When You Open the Graph

The graph samples the Endpoints from the point you begin to view the graphs, updating the graph according to the time period set. QoS data will display as long as the Endpoint is active. The QoS data will stop displaying if the Endpoint stops being active and resume if it becomes active again.

Active Session graphs will update only as long as the Session is active. (Note that if a new Session starts between the same two Endpoints a new Query must be run to pick this up. VoIP Monitoring Manager considers this a new Session and will not display the new data on the old graph.)

The QoS Parameters are Color-Coded on the Active Graphs

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.

The Title Bar

The Title Bar shows the type of Endpoint, the phone number and the type of graph (i.e., Active or Historical). Below the Title Bar, the Codec used and RSVP status are displayed. You can also use the Minimize, Maximize and Close buttons on the Title Bar. When the graph is minimized, you will only see the Title Bar. You can double-click on the Title Bar to re-open it.

The Graph Scrolls Across the Screen

The graph automatically scrolls across the screen as it updates. It scrolls across from right to left. You can use the scroll bars to scroll the graph across the screen.

The Axes

The X-axis shows the time range and the Y-axis shows the value for each of the QoS parameters. The default upper values on the Y-axis are where we would expect serious degradation of voice quality. You can point your mouse at the sampled points on the line graph to see the exact time and measured data, similar to a tool tip. You can edit the scales of the axes in the Graph Properties dialog.

The Table

A table below the line graph shows the actual QoS values for the most recent sample, the minimum, the average and maximum values experienced since the graph was opened.

Update the Graph

You can update the graph by clicking on the **Update Graph** button to force an immediate sample of the Session. You can also alter the update time period, pause the graph, set automatic updates and global updates.

Interpreting the Values on an Active Graph

You interpret the graph by noting where the sampled data displays on the Y-axis. If you are using the default values, the upper values on the Y-axis indicate that the QoS data is reaching unacceptable limits. The following values show the ranges and possible reported problems.

Table 4-1. The Values for an Active Graph

QoS	**Lower** **Acceptable**	**Middle** **Warning**	**Upper** **Not Acceptable**
Jitter (ms) **Displayed** (Red)	**0 to 50ms** Conversation is 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%**

Difference Between the QoS Data for an Endpoint and a Session

The Active Endpoint graph displays a sample of the activity at the Endpoint. This sample is an average of all the activity. As an Endpoint can participate in multiple concurrent Sessions, a high value on the graph indicates that one or more of the Sessions is causing this result. It does not indicate which Session. In contrast, a Session graph displays the QoS data as experienced by both Endpoints for that Session only. To determine which Session caused the high value on the graph, you will need to narrow your Query using filters. Consult the VoIP Monitoring Manager Client’s Online Help on how to use this function.

Understanding Historical Graphs

The Historical graphs display the QoS data as a meter reading on a gauge. Each of the QoS parameters is displayed on a separate gauge, one for each of the three QoS parameters. The needle on the gauge shows the average values measured and the black inner arc shows the exact minimum and maximum values measured.

A Historical Endpoint graph displays only one set of the three gauges. The Historical Session graph displays the parent Endpoint on the top graph. The child Endpoint that was involved in the Session with the parent Endpoint displays on the graph below.

The Title Bar

The Title Bar shows the type of Endpoint, the phone number and the type of graph (i.e., Historical or Active). Below the Title Bar displays the Codec used and RSVP status.You can also use the minimize, maximize and close buttons on the graph. When the graph is minimized, you will only see the Title Bar. You can double click on the Title Bar to re-open it.

A Table Shows the Values

A table below the graph shows the minimum, average, and maximum values for each of the gauges.

Displays Start and End Dates

The start and end dates display at the bottom of the graphs. You will notice that a Session graph displays the date for the whole Session, even if the Session started or ended outside the date specified.

The Graph is Static

The graph does not update because the information has been compiled on previously Active Endpoints and Sessions.

Color-Coded Ranges

The color-coded ranges show the different levels of tolerance for the QoS data. The color-coded ranges are explained in the following section.

Available up to 30 Days

The historical data is stored for 30 days or until the stored data reaches 100 MB in the database. At that point, the oldest data will be deleted as necessary to make room for new data.

Interpreting the Values on Historical Graphs

You interpret the Historical graphs by noting where the needle is positioned on the gauges. If the needle is positioned in either the yellow or red ranges, then it is indicating degradation in the QoS.

Table 4-2. The Values for an Historical Graph

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%**

Glossary

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

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. Example RTP Codecs are G.723, G.711 aLaw and G.729. The Codec used will be displayed just under the Title Bar on the graphs.

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.

AVAYA VoIP Monitoring Manager

The Query Result List will display one or more phone numbers next to the Gateway Endpoint type. These are the phone numbers that are currently active and the Gateway is acting as an intermediary for. Therefore, the phone number of the Gateway can change and be multiple phone numbers. The Query Result List will separate Endpoints involved in a Session with a comma (,). Conference calls are separated by a colon (:). If the following phone number **8616,1111:1222, 8904** displays in the Query Result List then the Gateway has three active Sessions.

- Telephone 8616 (e.g., Softphone 9999 and telephone 8616 are in a Session)
- Telephones 1111 and 1222 are conferenced (e.g., IP phone 888 is in a Session with these two phones)
- Telephone 8904

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.

Removing Jitter

Jitter can result from bad queuing strategies setup on the equipment. Check the manual for recommended levels for your equipment. You also need to rule out a faulty microphone or other hardware problems. Removing jitter requires collecting packets and holding them long enough to allow the slowest packets to arrive in time 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 150ms. Symptoms of excessive jitter could be reported as crackling or static.

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 these packets being lost in the transmission from one Endpoint to another. When packet loss occurs there are drop outs of words or of 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.

Payload

Payload is the contents of a packet. In RTP, it is encoded audio that is the user data of a packet. See also Codec.

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. In VoIP Monitoring Manager, it is 3 factors that determine the quality of VoIP calls. These factors are Jitter, Round Trip Time, and Packet Loss.

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

Real-Time Transport Protocol

Real-Time Transport Protocol is responsible for carrying data with real-time properties. For more information see I**ETF RFC 1889 located at http://www.ietf.org/rfc/rfc1889.txt**

RTP Session

A Session is a VoIP connection between two IP Endpoints. For more detailed information see **RFC 1889 located at http://www.ietf.org/rfc/rfc1889.txt?number=1889**

RTCP or Real-Time Transport Control Protocol

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

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, Packets 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.**

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 experience difficulties in carrying on a normal conversation when the one-way network delay exceeds 500 milliseconds (ms). Each element of the network adds to round trip time including switches, routers, distance traveled through the network, and firewalls. Round trip time in excess of 500 ms can have a noticeable effect such as excessive delay. However, some users may elect to tolerate it.

RSVP or Resource ReSerVation Protocol

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

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 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 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

Simple Network Management Protocol 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).

You will need it to have it installed to run the VoIP Monitoring Manager as it enables the RTCP Monitor to publish the data. You can check to see if the Windows SNMP Agent is installed on the Server by seeing if it is listed in the Administrative Services.

- Click **Start > Control Panel > Administrative Services > Services**
- Scroll down until you see the **SNMP Agent** listed as started automatically.

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 change its properties.

To open the SNMP Service Properties dialog

- From the Services window, right-click on the **SNMP Service** and select **Properties** from the context menu.

  The SNMP Service Properties dialog opens.
- Select A**utomatic** from the **Startup Type** drop down list and click **OK.**

Index