

Avaya™ VoIP Monitoring Manager User Guide

555-233-510
Issue 2
August 2002

Avaya™ VoIP Monitoring Manager User Guide

Copyright 2002, Avaya Inc. ALL RIGHTS RESERVED

The products, specifications, and other technical information regarding the products contained in this document are subject to change without notice. All information in this document is believed to be accurate and reliable, but is presented without warranty of any kind, express or implied, and users must take full responsibility for their application of any products specified in this document. Avaya disclaims responsibility for errors which may appear in this document, and it reserves the right, in its sole discretion and without notice, to make substitutions and modifications in the products and practices described in this document.

Avaya™ is a registered trademark of Avaya, Inc.

ALL OTHER TRADEMARKS MENTIONED IN THIS DOCUMENT ARE PROPERTY OF THEIR RESPECTIVE OWNERS.

Preface 5

The Purpose of this Manual 5
Who Should Use this Manual 5
Organization of this Manual 6

Chapter 1 — What is Avaya™ VoIP Monitoring Manager? 7

What is Avaya™ VoIP Monitoring Manager? 7
What You Can Do With Avaya™ VoIP Monitoring Manager 8
Search Endpoints 8
View Reports 8
Generate Automatic Alarms 8
Components of Avaya™ VoIP Monitoring Manager 9
Avaya™ VoIP Monitoring Manager Server 9
Avaya™ VoIP Monitoring Manager RTCP Monitor 9
Avaya™ VoIP Monitoring Manager Client 9
Avaya™ VoIP Monitoring Manager Client as an Applet 10
What You Need to Run Avaya™ VoIP Monitoring Manager 10
Operating System 10
Software 10
Processor 10
RAM 10
Video 10
Free Disk Space 10

Chapter 2 — Installing the Software 11

Installing the Server software 11
Ensuring Windows SNMP Agent is installed 12
Installing the Client software 12
Solving Installation Problems 13
Changing Avaya™ VoIP Monitoring Manager Server Properties . . . 13
Set Windows SNMP Agent to Start Automatically 14
Check for a Valid Community ID 14

Chapter 3 — How to Use Avaya™ VoIP Monitoring Manager 15

Before You Start Using Avaya™ VoIP Monitoring Manager 15
How to Start Avaya™ VoIP Monitoring Manager 15
Search for Endpoints 16
View Reports 16
View Reports contd. 17
View the Session Data 17

Chapter 4 — Interpreting Reports *19*

About Reports 19
Summary Reports 19
Detailed Reports 20
Difference Between the QoS Data for an Endpoint and a Session . . . 20
Interpreting the Values Using Summary Reports 21
Interpreting the Values Using Detailed Report 22

Glossary *23*

Index *27*

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.

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**
- **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 specfied time into 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.

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. 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 Avaya™ VoIP Monitoring Manager Server resides on the same PC as the RTCP Monitor.

Avaya™ VoIP Monitoring Manager RTCP Monitor

The VoIP Monitoring Manager implements the RTCP Monitor 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. (The reference is RFC 2959 located at http://www.ietf.org/rfc/rfc2959.txt)
- The proprietary AVAYA-VMON-MIB which stores the data. (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 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.

Avaya™ VoIP Monitoring Manager Client as an Applet

The Client can run as Applet from within a browser. This is useful if you only have the Server installed. You will need to have the Sun Java Plug-in to run the Client as an Applet. You can only access one monitor that is directly connect to the machine running the Avaya™ VoIP Monitoring Manager Server, and certain functionality is limited such as connecting to a new server and copying the reports.

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 128 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 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.

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 the ID 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 of 5005 as the default should work in most situations.

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 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 searching endpoints and viewing reports. It includes the following sections:

- **Before You Start Using the VoIP Monitoring Manager**
- **How to Start the VoIP Monitoring Manager**
- **Run a Search**
- **View Reports**

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 network.

How to Start Avaya™ VoIP Monitoring Manager

To Start Avaya™ VoIP Monitoring Manager

1. 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.

2. 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 value. 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.

View Reports contd.

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 click the **Show Details** button. You can also zoom in or out to see more or less of the data, by altering the date range on the report.

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 displays.

4 Interpreting Reports

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

- **About Reports**
- **Interpreting Summary Reports.**
- **Interpreting Detailed Reports.**

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
- RSVP status
- Codec

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 1. Summary Report

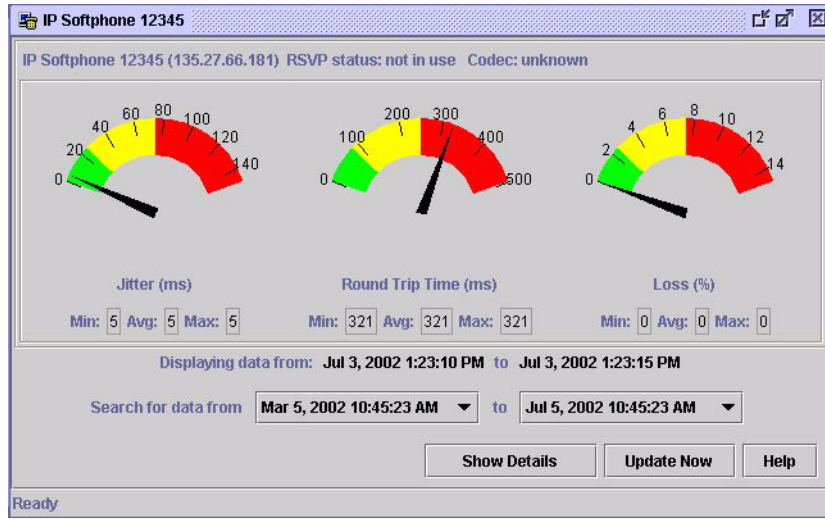


Table 1. The Values for the Summary Reports

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 upper values on the Y-axis indicate unacceptable limits.

Figure 2. Detailed Report

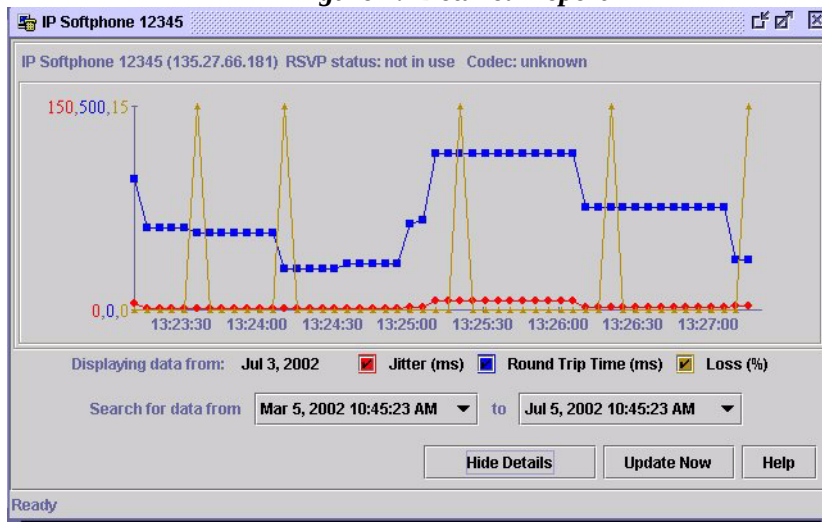


Table 3. The Values for Detailed Reports

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.

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. 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 Results 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 Results List will separate endpoints involved in a session with a comma (,). Conference calls are separated by a colon (:).

For example, if the following phone numbers **8616,1111:1222, 8904** display in the Results List then the Gateway has three active sessions.

Telephone 8616 could be in a session with another softphone. The Non-IP telephones 1111 and 1222 could be in a conference with an IP phone. Telephone 8904 could be in a session with an IP phone.

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 set up on the network equipment. Check your equipment manual for recommended levels for your equipment. 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 150ms. 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 the cause of the problem.

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 could be a drop out 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 refers to 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 monitors and displays the 3 main factors that determine the quality of VoIP calls. These factors are Jitter, Round Trip Time, and Packet Loss. On the Summary Reports each of the 3 factors displays as a separate gauge. The Detailed Reports displays the QoS as follows:

- 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 Control Protocol or RTCP

RTCP is 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

Real-Time Transport Protocol is responsible for carrying data with real-time properties. For more information see **IETF 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**

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.

Resource ReSerVation Protocol or 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, 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 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 VoIP Monitoring Manager.

Voice over Internet Protocol or VoIP

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 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 collect and publish the data.

Index

Numerics
5005 9

A
Add/Remove Windows Components 12
Advanced Search 8
alarm, defined 26
Applet 9, 10
ASN.1 definitions 9
AVAYA-VMON-MIB 9

B
blue 20, 25
brown 20, 25
Browser 10

C
changing
  server properties 13
Client 9
  installing 12
Codec 23
Community ID 13
components
  Client 9
  RTCP Monitor 9
  Server 9
copyright 2
crackling 22

D
delay 24
  no delay 22
detailed
  interpreting 21
Detailed Reports 16, 20
dial-up connection 9
difference between endpoint & session 20
disk space requirements 10
downloading this software, explained 11
drop out 21, 22

E
endpoint 20
  difference between session and 20

G
gateway, defined 23
generating automatic alarms 8
GUI 9

H
http
  //www.ietf.org/rfc/rfc1889.txt 25
  //www.ietf.org/rfc/rfc1889.txt?number=188 25
  //www.ietf.org/rfc/rfc2205.txt 26
  //www.ietf.org/rfc/rfc2750.txt 26
  //www.ietf.org/rfc/rfc2959.txt 9

I
IETF RFC 1889 25
IETF RFCs 2205, 2750 26
installing
  client software 12
  server software 11
  SNMP agent 12
intermittent delay, QoS values indicating 21, 22
interpreting reports 21

J
jitter 7, 20, 21, 24
  removing 24

L
Listen Port 13
loss 21

M
match
  phone number, network address, QoS 8
missing parts of the conversation 21
modifying
  server properties 13

O
operating system requirements 10

P
packet 24
packet loss 7, 20, 24, 25
pauses
  QoS values indicating 21
pauses, QoS values indicating 22
payload, defined 24
processor requirements 10
purpose of Avaya VoIP Monitoring Manager 9
purpose of this manual 5

Q
QoS 25
Quality of Service 25
query
  customizing using filters 8

R
RAM requirements 10
Real-Time Transport Control Protocol 25
Real-Time Transport Protocol 25
red 20, 25
removing jitter 24
reports
  interpreting 21
requirements 10
Resource ReSerVation Protocol 26
result list 23
Results List 17
RFC 1889 25
RFC 2959 9
Round Trip Time 20, 21, 25
RSVP status 7
RSVP, defined 26
RTCP 25
  Monitor 9
RTP
  MIB 9
  Session 25
RTT 25

S
Server 9
server properties, changing 13
Session 20
session, difference between endpoint and 20
Simple Network Management Protocol Agent 10, 26
SNMP
  ensuring agent is installed 12
SNMP agent
  see if it is running 14
SNMP Agent, defined 26
SNMP traps, generating automatically 8
SNMP, default port 9
software requirements 10
Start
  Applet 10
  Before 15
  How to 15
static, QoS values indicating 22
summary
  interpreting 21
Summary Reports 16

T
trademarks 2
trap, defined 26
traps, generating automatically 8
troubleshooting
  installation problems 13

V
video requirements 10
View Reports 8, 16, 17
Voice Codec 7
Voice over IP, defined 26

W
web site, if you download this product from 11
who should use this manual 5
Windows 2000 10
Windows SNMP Agent 9