Avaya VisAbility™ Management Suite

Release 1.3

Implementation Guidelines

555-233-163
Issue 7
May 2003

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 website:

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 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
- 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.

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 Web site:

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

Table of Contents

PREFACE 1

PURPOSE 1
SCOPE OF THIS DOCUMENT 1
INTENDED AUDIENCE 1
CONVENTIONS USED IN THIS BOOK 1
ADDITIONAL RESOURCES 2
HOW TO ACCESS THIS BOOK ON THE WEB 3
TELL US WHAT YOU THINK! 3

APPLICATION ENVIRONMENT 4

VOICE AND MESSAGING SYSTEM COMPATIBILITY 4
OPERATING ENVIRONMENT 5
HARDWARE COMPONENTS 6
CONNECTIVITY / NETWORK CONNECTIONS 8
COMPUTING PLATFORM 9
CONNECTIVITY / NETWORK CONNECTIONS 9

IMPLEMENTATION SERVICES 10

PRODUCT PACKAGING 10
CUSTOMER IMPLEMENTATION OPTIONS 11
OVERVIEW OF AVAYA IMPLEMENTATION SERVICES 11
SERVICES ORGANIZATIONS INVOLVED IN AVAYA VISABILITY MANAGEMENT SUITE IMPLEMENTATIONS 13
RNIS SERVICE REQUEST DOCUMENTATION 13
AVAYA AND CUSTOMER RESPONSIBILITIES 15
SPECIFIC IMPLEMENTATION TASKS 15

APPENDIX A - OVERVIEW OF CUSTOMER AND AVAYA RESPONSIBILITIES FOR IMPLEMENTATION OF AVAYA VISABILITY MANAGEMENT SUITE 22

APPENDIX B - INSTALLATION OF RED HAT LINUX 7.3 TO HOST AVAYA VISABILITY MANAGEMENT SUITE 1.3 24

INSTALLING RED HAT LINUX 7.3 24
INSTALLING ADDITIONAL SOFTWARE 25
INSTALLING RED HAT PACKAGE MANAGER (RPM) FILES 25
DETERMINING WHETHER RPM FILES ARE ALREADY INSTALLED 26

INDEX 27

Preface

Purpose

This document, the Avaya VisAbility™ Management Suite Implementation Guidelines, provides the customer with an overall strategy for implementation of applications in the suite. It describes the roles and responsibilities of the customer and Avaya Services in the implementation of applications in the suite.

Avaya Remote Network Integration Services (RNIS) provides implementation services for applications in the VisAbility Management Suite. Avaya Authorized Business Partners may also provide implementation services for the Avaya VisAbility Management Suite. Details of implementation services offered by business partners must be obtained from the business partners and are not discussed in this document.

Scope of this Document

This document addresses:

- pre-implementation requirements of the network management computing platforms
- pre-implementation installation of the operating system on the computing platforms
- post-implementation verification checklist

Intended Audience

This document is intended for customers to describe the roles and responsibilities of the customer and Avaya Services in the implementation of applications in the suite.

Conventions Used in This Book

In this book, we use the following typographical conventions:

- We use bold type for emphasis and for any information that you should type; for example, **save translation**.
- We use Courier font for any information that the computer screen displays; for example, `login`.
- We use arrows to indicate options that you should select on cascading menus; for example, "Select File > Open" means choose the "Open" option from the "File" menu.

Additional Resources

You may find the following additional resources helpful:

- Avaya VisAbility™ Management Suite Advanced Converged Management Installation and Upgrade Instructions, 555-233-160
- Avaya VisAbility™ Management Suite Enhanced Converged Management Installation and Upgrade Instructions, 555-233-161
- Avaya VisAbility™ Management Suite Configuring Red Hat Linux, 555-233-152
- Avaya VisAbility™ Management Suite MultiVantage Configuration Manager

  > Installation and Configuration, 555-233-137
  > Help system
- Avaya VisAbility™ Management Suite MultiVantage Fault and Performance Manager

  > Installation and Configuration, 555-233-138
  > Help system
- Avaya VisAbility™ Management Suite MultiVantage Proxy Agent Installation and Configuration, 555-233-139
- Avaya VisAbility™ Management Suite Site Administration

  > Help system
  > Guided tour
- Avaya VisAbility™ Management Suite Terminal Emulator Help system
- Avaya VisAbility™ Management Suite Voice Announcement Over LAN Manager Help system
- Avaya™ ATM WAN Survivable Processor Manager

  > Installation and Configuration, 555-233-223
  > Help system
- ATM Installation, Upgrades, and Administration Using Avaya™ Communication Manager, 555-233-124
- Avaya™ Directory Enabled Management

  > Installation and Implementation, 555-038-101
  > Administration, 555-038-501
  > Data Schema, 555-233-164
  > Help systems (client and administration)
- Avaya™ Terminal Configuration

  > Administration, 555-250-103
  > Help system
- Avaya™ Voice Over IP Monitoring Manager

  > User Guide, 555-233-510
  > Help system

How to Access This Book on the Web

You can view or download the latest version of this book from the Avaya, Inc. Web site. You must have access to the Internet, an Internet browser, and Adobe Acrobat Reader with Search, version 5.0 or later. Adobe Acrobat Reader is available from http://www.adobe.com.

To view or download the latest version of the Avaya VisAbility Management Suite documentation:

1. Access http://www.avaya.com/support.
2. Click **Product Documentation**.
3. Click **System and Network Management**.
4. Locate the heading Avaya VisAbility Management Suite and click the link corresponding to the software release.
5. Locate the title of the book and click the link corresponding to the book.

The Help systems are integrated in the Avaya VisAbility Management Suite product applications.

Tell Us What You Think!

Let us know how this book measured up to your expectations. Your opinions are crucial to helping us meet your needs! Please complete and return the comment card at the front of this book. Optionally, send us your comments by mail, fax, or e-mail as follows:

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

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

E-mail
document@avaya.com
subject: Avaya VisAbility Management Suite Documentation Team

Application Environment

The Avaya VisAbility™ Management Suite offers a comprehensive set of network and system management solutions for converged voice and data environments. Avaya VisAbility Management Suite provides a standards-based infrastructure for an open application program interface and integrated network management in a converged, multi-vendor environment.

Avaya VisAbility Management Suite is comprised of a set of application programs providing systems administration, network management and business integration in a converged network environment. While many of the individual management products have been available on an individual basis, the Avaya VisAbility Management Suite integrates voice-centric management products and data-centric management products into a single suite with a common user interface.

Voice and Messaging System Compatibility

The Avaya VisAbility Management Suite Advanced Converged Management Offer connects to managed devices using IP. Non-IP enabled devices may relay alarms to the MultiVantage Proxy Agent using dial-up (serial) alarming. Avaya VisAbility Management Suite is compatible with voice systems, messaging systems and call management systems as shown in the table below:

Table 1: Avaya VisAbility Management Suite compatibility with voice systems, messaging systems and call management systems

System	Release
DEFINITY R, DEFINITY SI, DEFINITY CSI, DEFINITY ONE, IP600	Release 9, 10 or MultiVantage (System must be configured for IP administration)
S8100 Media Server	MultiVantage
S8300 Media Server	MultiVantage
S8700 Media Server	MultiVantage
INTUITY AUDIX	Release 5.1 and later
INTUITY AUDIX LX	Release IA 1.0-17.X
DEFINITY AUDIX	Release 3.1 or later
Multipoint Control Unit (MCU)	Release 7.2
S8300 INTUITY AUDIX	MultiVantage
IP600/DEFINITY ONE AUDIX	Release 9 or later
INTUITY Interchange	5.1 or later
Call Management System (CMS)	Release 8.3 or later
CONVERSANT	7.0 or later

Operating Environment

The application server components operate in either a Windows 2000 environment or a Red Hat Linux 7.3 environment as shown in table 2. All clients operate in a Windows XP or 2000 environment. Standalone applications, Avaya Site Administration and Avaya Voice Announcement over LAN Manager also operator in a Windows XP or 2000 environment. Avaya Terminal Emulator operates only in a Windows 2000 environment. For Windows XP environments, Avaya recommends third-party terminal emulation applications such as Procomm.

Table 2: Operating Environment of Server components for VisAbility Management Suite Applications

Application	Windows 2000 Pro	Windows 2000 Server	Linux 7.3	Solaris 8
Avaya ATM WAN Survivable Processor Manager		X		
Avaya VoIP Monitoring Manager		X		
Avaya Directory Enabled Management		X		
Avaya Terminal Configuration		X		
Avaya MultiVantage Configuration Manager			X	
Avaya MultiVantage Fault and Performance Manager			X	
Avaya MultiVantage Proxy Agent			X	
Avaya MultiService Console	X	X		X
Avaya MultiService Address Manager	X	X		X
Avaya MultiService Configuration Manager	X	X		X
Avaya MultiService Software Update Manager	X	X		X
Avaya MultiService VLAN Manager	X	X		X
Avaya MultiService QoS Manager	X	X		X
Avaya MultiService SMON Manager	X	X		X
NMSI	X	X		X

Hardware Components

Server applications that comprise the Avaya VisAbility Management Suite run in a Red Hat Linux 7.3 environment or in a Windows 2000 Server environment. The customer provides the hardware platform, operating system, software and network used by the suite.

The hardware needed to support the Avaya VisAbility Management Suite software solutions can be found in Table 3 for the Windows 2000 Server, Table 4 for the Red Hat Linux server, Table 5 for the Solaris 8 server, and Table 6 for the client PC. Use of machines that are below the recommended configurations may result in poor performance.

Table 3: Windows 2000 Server Hardware[1]

Component	Recommended	Comments
Processor	1.3 GHz Pentium 4	1.3 GHz Pentium 3 is acceptable
Hard Drive	40 GB Hard Drive	
Network Connectivity	10/100 Network Card	
RAM	1.5 GB RAM	
Modem	56K External Modem (connected to COM1)	This is strongly recommended and can be connected only when needed for remote access by Avaya Services. Note the modem can be on either the Windows 2000 Server or the Linux Server.
CD-ROM	CD-ROM	Needed for installation
Extra software	Anti-Virus; pcAnywhere (version 10 or later)	This is strongly recommended; pcAnywhere is needed for remote access by Avaya Services
Web Browser	Netscape 6.2 or greater or Internet Explorer 5.5/6.0	Needed for access to VisAbility Management Suite Home Page and Web based clients; Win XP needs IE 6.0

[1] The VisAbility Management Suite requires a Microsoft Windows 2000 Server operating system on a high-end desktop machine. A server class hardware platform is not required. Additionally, the Windows Server for the MultiService Network Management offer can run the Windows 2000 Professional OS rather than the Windows 2000 Server OS.

Table 4: Red Hat Linux 7.3 Server Hardware

Component	Recommended	Comments
Processor	1.3 GHz Pentium 4	1.3 GHz Pentium 3 is acceptable
Hard Drive	40 GB Hard Drive	
Network Connectivity	10/100 Network Card	
RAM	1.5 GB RAM	
Modem	56K External Modem (connected to COM1)	This is strongly recommended and can be connected only when needed for remote access by Avaya Services. Note the modem can be on either the Windows 2000 Server or the Linux Server.
Web Browser	Web Browser	Needed to download software updates from http://www.avaya.com/support
CD-ROM	CD-ROM	Needed for installation

Table 5: Solaris 8.0 Server Hardware

Component	Recommended	Comments
Processor	SPARC architecture processor (500 MHz)	Solaris is only needed if running HPOV on Solaris instead of Windows 2000
Hard Drive	40 GB Hard Drive	
Network Connectivity	10/100 Network Card	
RAM	1 GB RAM	
Modem	***Not required***	Remote access by Avaya Services can be achieved via access by modem into either the Windows or Linux server, followed by a telnet session into the Solaris server
Web Browser	Web Browser	Needed to download software updates from http://www.avaya.com/support
CD-ROM	*CD-ROM*	Needed for installation

Table 6: Client PC Hardware

Component	Recommended	Comments
Operating System	Microsoft Windows 2000/XP Professional	
Processor	600 MHz Pentium III	
Available Disk Space	1 GB	Required to install all suite client components
RAM	256 MB RAM	
Network Connectivity	TCP/IP 10/100 Network Card	
Modem	56K Modem	Optional (if needed for remote access of client machine)
CD-ROM	CD-ROM	Optional (can be used for client software installation)
Display	SVGA	
Linux Server Access	Xwindows or telnet	Optional (for access to Linux server for Avaya MultiVantage Fault and Performance Manager administration)
Web Browser	Netscape 6.2 or greater or Internet Explorer 5.5/6.0	Needed for access to VisAbility Management Suite Home Page and Web based clients; Win XP needs IE 6.0

Connectivity / Network Connections

The Avaya VisAbility Management Suite Advanced Converged offer requires a local (or wide) area network connection to all network devices to be managed systems and supporting databases (for Directory Enabled Management). The network connection must be in place and tested prior to implementation of the suite. Assistance with network setup is not part of this offer but may be performed by Avaya Services under a different offer.

Implementation requires the following network information:

- The IP address of each MultiVantage and DEFINITY® system
- The IP address of each INTUITY® Audix system
- The C-LAN port for each MultiVantage and DEFINITY® system

Computing Platform

The customer is responsible for obtaining the computing platform(s) used to host applications in the Avaya VisAbility Management Suite. The specifications for the computing platforms needed to support the Avaya VisAbility Management Suite software solutions can be found in Table 3 for the Windows 2000 Server and Table 4 for the Red Hat Linux server. In addition to the specifications for VisAbility Management Suite, Avaya recommends the use of servers that are certified for use with Red Hat Linux as listed on Red Hat's Hardware Compatibility List, which can be found at: (http://hardware.redhat.com/hcl/).

Use of a computing platform that is below the recommended configurations may result in poor performance.

Remote Access Hardware and Software

Tables 2 and 3 state the requirements for a modem and remote access software on Windows and Linux-based computing platforms. However, where multiple network management servers are present and connected via an IP network, only one network management server requires remote access capabilities. The remaining network management servers may be accessed through use of a Telnet session originating at the server with remote access. This arrangement is not dependent on the operating systems (Linux or Windows 2000 Server) of the network management servers. This topic is discussed in detail in "Remote Connectivity" on page 16.

Symmetric Multi-Processor (SMP) Support

Linux-based applications in the VisAbility Management Suite require the latest kernel from Red Hat to run properly in a Symmetric Multi-Processor (SMP) environment.

Microsoft and Red Hat each provide a website where customers can download patches to the Windows and Linux operating systems, respectively. It is strongly recommended that customers keep their servers up-to-date, as patches correct software bugs but also contain security updates.

Connectivity / Network Connections

The Avaya VisAbility Management Suite requires IP connectivity to all network devices to be managed systems and supporting databases (for Directory Enabled Management). The customer is responsible for designing and implementing local (or wide) area network connections. Network connections must be in place and tested prior to implementation of the suite. Assistance with network setup is not part of the Avaya VisAbility Management Suite offer but may be performed by Avaya Services under a different offer.

Implementation Services

The Remote Network Integration Services (RNIS) team, part of Avaya's Implementation Services Organization (ISO), provides implementation services for applications in the VisAbility Management Suite. Servicing North American, multinational and international accounts from its location in St. Petersburg, Florida, USA, ISO delivers implementation services, maintenance services and remote network management services for multi-vendor networks. There are over 300 highly trained associates that provide Tier 1 through Tier 3 level remote support, including remote implementation support, network troubleshooting, and performance optimization for WAN and LAN equipment.

In the U.S., on-site support is provided by the Field Services Organization (FSO) a team that is geographically distributed across the U.S. and dedicated to the data networking business. This team of over 500 service professionals is supported by an elite team of data communications professionals in the St. Petersburg Technical Assistance Center (TAC).

Both the Avaya Data Technical Assistance Center (TAC) engineers and the Field Services Organization (FSO) team have an average of 15+ years experience in supporting data networking products and telecommunications networks, while senior engineers average 20+ years experience.

Product Packaging

There are five offers in the Avaya VisAbility™ Management Suite:

- Standard Management
- Standard Management Plus
- Enhanced Converged Management
- Advanced Converged Management
- MultiService Network Management

Irrespective of product packaging, Avaya will provide implementation services for individual applications on the customer's computing platform:

- Avaya MultiVantage™ Configuration Manager
- Avaya MultiVantage™ Proxy Agent
- Avaya MultiVantage™ Fault and Performance Manager
- Avaya™ Directory Enabled Management with Avaya™ Terminal Configuration
- Avaya™ MultiService Network Manager with Avaya MultiService SMON™ Manager
- Avaya™ VoIP Monitoring Manager (full version)
- Avaya™ Site Administration
- Avaya™ Voice Announcement Over LAN Manager (Voice Announcement Board Administration)
- Avaya™ ATM WAN Survivable Processor Manager

Customer Implementation Options

Many of the applications within the VisAbility Management Suite are customer installable. Due to the complexity of application configuration, however, it is strongly recommended that customers seek professional implementation services from Avaya Services to implement any of the following applications:

- Avaya MultiVantage Configuration Manager
- Avaya MultiVantage Proxy Agent
- Avaya MultiVantage Fault and Performance Manager,
- Avaya Directory Enabled Management

If a customer attempts a self-installation and requires assistance with the installation or configuration of an application in the suite, they should contact the RNIS tier 2 technical support team at 1-800-237-0016, prompt 4. Note that charges may apply for RNIS implementation assistance.

Avaya's Technical Services Organization (TSO) provides warranty and maintenance services for an application only after that application has been properly installed and configured. An application is considered properly installed when the implementation verification tasks defined in "Implementation Verification" on page 18 have been successfully completed. Warranty and maintenance support is available at 1-800-237-0016, extension 73368 (or follow the prompts for "VisAbility Management Suite").

Overview of Avaya Implementation Services

Avaya implementation services are available for individual or small groups of applications in the suite. Due to installation and configuration complexities, it is strongly recommended that

Avaya Services implement Avaya MultiVantage Configuration Manager, Avaya MultiVantage Proxy Agent, Avaya MultiVantage Fault and Performance Manager, and Avaya Directory Enabled Management. The customer may choose to implement the remaining applications or have Avaya Services perform these implementations.

Basic implementation can be performed remotely using remote access technology (e.g., dial-up modem) to enable the RNIS Implementation Engineer(s) to have remote control/access to the customer servers. The remote RNIS engineer(s) will be in telephone contact with the designated customer representative as necessary during the implementation process. The customer representative will assist with the implementation, in particular, to verify server readiness (system powered-on and OS booted), verify availability of remote connectivity to the customer server(s) and managed devices (e.g., voice systems), and place product CDs into the server CD drive as directed by the remote engineer.   Once these activities have been completed, the customer representative is not required to assist with configuration and customization of the application software.

For customers in the U.S, on-site installation is available for an additional charge. When requested, a field technician will be dispatched to the customer site to take the place of the customer representative and act as the hands of the remote RNIS engineer in performing the implementation. The on-site technician will verify server readiness (system powered-on and OS booted), verify availability of remote connectivity to the customer server(s) and managed devices (e.g., voice systems), and place product CDs into the server CD drive as directed by the remote engineer. Once these activities have been completed, the technician will leave the customer site while the remote RNIS engineer completes configuration and customization of the application software.

Onsite Implementation is available as an add-on offer with any RNIS offer. With this offer, the RNIS Implementation Engineer will travel to the customer site to perform the implementation. Onsite Installation and Onsite Engineer should never be ordered together.

Basic implementation services include installation of an application within Avaya VisAbility Management Suite on a customer-supplied server, configuration of the application to operate with one voice or messaging system (MultiVantage, DEFINITY, or INTUITY) or one Avaya P130/P330/P580/P880 device/stack as appropriate for the application, and verification with that managed device. The application may be configured for additional managed devices under the Configuration of Managed Devices offer. Basic implementation services do not include setup of customer server hardware or operating environment, or design/implementation of network connectivity. At the customer’s option, Avaya Services will configure VisAbility Management Suite applications to work with additional managed devices as an additional service.

For Avaya VisAbility Management Suite applications that manage voice systems, some configuration parameters are required on the voice system to operate with the application. In particular, a login/password is required for all applications. An application-specific login is recommended to enable appropriate access rights and create an application-specific audit trail in the voice system log. In addition, some applications require configuration of the IP address of the network management server and alarm notification information into the voice system.

Note: In all cases, RNIS implementation services described in this document do not include administration of configuration parameters on any Avaya ECLIPS or DEFINITY voice systems.

The Solution Evaluation offer provides a 4-hour block of time for a RNIS engineer to work with the customer via telephone to assess configuration and customization requirements for any or all applications within the Avaya VisAbility Management Suite. This offer may be ordered in multiple units if more time is required. Where custom work is required, the evaluation will result in a proposed statement of work and price.

Services Organizations involved in Avaya VisAbility Management Suite Implementations

The RNIS Services Organization is composed of the following service groups:

- **Data Help Desk (DHD) –** the primary objective of the DHD is management and scheduling of RNIS Resources. The DHD team receives and tracks all requests received to engage RNIS Implementation provisioning. Requests are reviewed for assignment feasibility, entered into an internal tracking system and assigned to an Implementation Engineer and a Case Implementation Coordinator (CIC) associate.
- **Case Implementation Coordinator (CIC) –** an internal administrative group that tracks RNIS service orders from receipt to completion. This group interfaces with all sales teams for service order accuracy, confirms or negotiates service delivery dates with customers, and provides status on service progress throughout the life cycle of an order. Where applicable, the CIC team will see that the necessary FSO/ISO resources have been scheduled for service projects. At the completion of service, the CIC team contacts the customer to gain acceptance of the work performed.
- **RNIS Implementation Engineers** - The RNIS Implementation Engineers receive the order documentation, including the Implementation Request Form and Configuration Request Forms (described later in this document), from the DHD team and use this information to create the Installation Specification. The engineers communicate with customer technical contacts to gather additional information to add to the Installation Specification and Configuration files.

RNIS Service Request Documentation

When implementation services for applications within the Avaya VisAbility Management Suite are ordered, the customer must work with your account team to complete an Implementation Request Form and applicable Configuration Request Forms. These forms provide information that the RNIS Implementation Engineer will use to configure the VisAbility Management Suite software to meet customer requirements.

Based on information on the customer’s Implementation Request Form and Configuration Request Form(s) submitted with the order and direct communications with the customer technical contact, the RNIS Implementation Engineer will create an Installation Specification. This document will provide technical information to guide the implementation and will be available to Avaya technical services teams that provide maintenance support for the applications.

Implementation Request Form

The Implementation Request Form (IRF) provides RNIS with basic customer contact and site information, including:

- Order and Contact Information
- Product and Services Requested
- Application Description
- General Network Information

Configuration Request Form

In addition to the IRF, a Configuration Request Form (CRF) must be completed for key Avaya VisAbility Management Suite applications to be installed. The CRF contains information that describes the customer requirements for the implementation of the specific application, for example:

- information on each voice system or data device to be configured
- customer directory schema (for Directory Enabled Management)
- filters for forwarding of alarms (for MultiVantage Fault and Performance Management).

The Linux CRF must be submitted when one or more of the Linux-based VisAbility Management Suite applications is to be implemented:

- Avaya MultiVantage™ Fault and Performance Manager
- Avaya MultiVantage™ Proxy Agent
- Avaya MultiVantage™. Configuration Manager

The Windows CRF must be submitted when one or more of the following Windows-based applications is to be implemented:

- Avaya^{TM} Directory Enabled Management with Avaya^{TM} Terminal Configuration
- Avaya^{TM} ATM WAN Survivable Processor Manager
- Avaya^{TM} VoIP Monitoring Manager

Avaya and Customer Responsibilities

The table in Appendix A summarizes the responsibilities of the customer and Avaya RNIS for implementation of applications in Avaya VisAbility Management Suite.

Note: All customer requirements must be completed prior to the scheduled start date of implementation. For a complete list of customer responsibilities, please contact the RNIS Data Help Desk.

For all RNIS service orders, the customer has responsibility to:

- identify a principal contact for this work
- schedule a time with RNIS for the implementation
- complete and submit the Implementation Request form and Configuration Request forms

For remote implementation, the customer must make available an on-site contact to assist during installation. For on-site installations or implementations, the customer must provide Avaya personnel with access to appropriate facilities and computer systems.

Note: If required documentation is not provided to the RNIS Implementation Engineer or dial-up connectivity has not been verified at least 5 business days prior to the scheduled implementation date, the implementation will be rescheduled to the next available date.

Specific Implementation Tasks

Implementation of VisAbility Management Suite applications will include the following tasks:

- Platform and Network Readiness

  >Remote connectivity
  >
  >Computing platform
  >
  >IP connectivity
- Installation and configuration of one or more of the Avaya VisAbility Management Suite applications on customer management servers
- Implementation Verification

The remainder of this section describes these tasks in more detail.

Remote Connectivity

For remote implementations, it is required that the RNIS Implementation Engineer has remote access to the customer's network management server(s). This remote connectivity is also required by Avaya Services for ongoing maintenance support of installed VisAbility Management Suite applications. The customer is responsible for the installation, configuration and testing of modems on the server(s) prior to implementation of Avaya VisAbility Management Suite applications. Remote access typically takes the form of an analog modem connected directly to the server in conjunction with an analog phone line having a telephone number accessible on the public phone network. Testing must include:

- establishment of a dialup connection and initiation of a PCAnywhere session on a Windows server, and
- establishment of a dialup connection and initiation of a Telnet session from the Linux command prompt on a Linux server.

Where multiple network management servers are present and connected via an IP network, only one network management server requires remote access capabilities. The remaining network management servers may be accessed through use of a Telnet session originating at the server with remote access. This arrangement is not dependent on the operating systems (Linux or Windows 2000 Server) of the network management servers.

If a Linux server will "host" remote access, note in particular the requirement on the Linux server for a modem connected to serial port COM1 (ttyS0) of the server. While internal and USB modems can be configured to work with Red Hat Linux, Avaya recommends a US Robotics Sportster 56k external modem to provide reliable remote connectivity in support of remote implementation and maintenance services.

On Red Hat Linux-based servers, no additional software is required, as the Red Hat Linux installation loads Virtual Network Computing (VNC) software. The engineer will establish a dial-up point-to-point-protocol (PPP) session using VNC on the Linux server to continue with the installation, configuration and verification.

If a Windows 2000 Server-based server will "host" remote access, it is the customer's responsibility to obtain and load Symantec's PCAnywhere remote control software (version 10.0 or higher). This enables the Implementation Engineer to accomplish remote implementation of Avaya VisAbility Management Suite applications, and it is also required for warranty and maintenance services provided by Avaya Services.

Note that MultiVantage Proxy Agent, running in a Linux environment, may receive alarms from adjunct units, such as messaging systems and integrated voice response systems, over a serial link. Dial-up "serial" alarming is also used for DEFINITY voice systems running R9.1 and R9.2 software. Additional analog modem(s) and phone line(s) will be used to receive these alarms, as the modem on COM1 must be dedicated to implementation and maintenance. Typically, one modem is required to support alarm reception, while a second modem is required to support alarm forwarding. However, the number of required modems (and the possible need for a Serial I/O Board to provide additional serial ports) is dependent on the number of managed nodes using serial alarming, whether the proxy server is providing alarm reception only or must perform alarm forwarding and filtering, and if the managed nodes are duplicated for redundancy or high-reliability. As a result, the number of modems required to support serial alarming must be determined on a case-by-case basis by the RNIS implementation engineer.

Computing Platform

The customer is responsible for acquiring servers and loading Red Hat Linux and Windows 2000 Server operating systems. It is important that the computing platform meet the minimum requirements specified in paragraph 2.4. Failure to meet these requirements may result in poor system performance. If desired, Avaya services will install the Red Hat Linux or Windows 2000 Server operating systems for an additional charge.

When loading Red Hat Linux 7.3, it is important to note that the default settings are not appropriate for the Linux-based applications in Avaya VisAbility Management Suite. It is mandatory that the installation guidelines contained in Appendix B be closely followed. Deviation from these guidelines may result in the Linux-based applications failure to operate on the server or the platform acceptance test to fail, thus delaying the completion of the implementation process.

After Linux has been installed and configured on the computing platform, it is important that the customer verify that a dial connection can be established by dialing into the server via a phone line connected to the modem on port ttyS0 (COM1). A successful connection will be indicated by display of a Linux “login” prompt. Remote connectivity is required as a condition of warranty and post-warranty service. Where Avaya Services will provide remote implementation services, the customer must verify that a dialup connection can be established prior to the scheduled date of implementation.

IP Connectivity

Network verification is performed by the RNIS Implementation Engineer prior to implementation of any server-based application in Avaya VisAbility Management Suite. This test is performed to ensure that the network management server(s) have IP connectivity to all devices to be managed, including voice systems, messaging systems and data switches.

It is the customer’s responsibility to design and implement local and/or wide area networking such that each management server has IP connectivity to each device it will manage.

Application Installation and Configuration

Based on information on the customer’s Implementation Request Form and Configuration Request Form(s) submitted with the order and direct communications with the customer technical contact, the RNIS Implementation Engineer will create an Installation Specification. This document will provide technical information to guide the implementation and will be available to Avaya technical services teams that provide maintenance support for the applications.

Implementation Verification

Once an application is installed and configured for operation with one or more managed devices, the RNIS Implementation Engineer will perform an application-specific Acceptance Test to verify application implementation.

Avaya MultiVantage Fault and Performance Manager and MultiVantage Proxy Agent

Once the MultiVantage Fault and Performance Manager (FPM) and MultiVantage Proxy Agent have been installed and configured, the RNIS Implementation Engineer will perform the following steps to verify proper operation with each managed voice and messaging system for which the applications were configured:

- Establish a connection between each voice or messaging system and MultiVantage Proxy Agent
- Verify that each voice or messaging system can ***send*** alarms to the MultiVantage Proxy Agent
- Verify that the MFPM server can ***receive*** alarms from each voice system
- Verify that the MFPM server can retrieve ***configuration data*** from each voice system
- Generate a test alarm for each managed node and verify that MFPM received the alarm

In addition to verification of the application, the RNIS Implementation Engineer will assist the customer in understanding basic operations of MultiVantage FPM and MultiVantage Proxy Agent:

- Verify that the customer has changed the ***root*** and ***g3maadm*** logins for the VisAbility Management Suite Linux Server platform
- Verify that the customer can ***start*** and ***stop*** the MultiVantage Proxy Agent
- Verify that the customer can ***display*** the s**tatus** screen to view the status and statistics of the MultiVantage Proxy Agent connection and the managed node
- Verify that the customer can add/modify/delete managed devices from the Proxy Agent via the change managed-nodes command
- Verify that the customer can set/change voice system login information for the Proxy Agent via the change managed-nodes command

Avaya MultiVantage Configuration Manager

Once the MultiVantage Configuration Manager has been installed and configured, the RNIS Implementation Engineer will perform the following steps to verify proper operation with each managed voice system and each messaging system for which the application was configured:

- Verify successful client configuration by launching from START menu and VisAbility Management Suite homepage
- Change the default ‘admin’ password and report this to the customer
- Create at least one MultiVantage Configuration Manager user for the customer
- Verify the queue is running for each configured voice system and messaging system

- Kick-off an ‘initialization’ for each configured voice system (this can take some time, up to several hours)
- Add and then delete a station on each voice system
- Add and then delete a voice mail subscriber for each messaging system
- Ensure that a unique login for use by Configuration Manager has been administered on each voice system. (This is necessary to ensure that the Configuration Manager cache of system changes remains accurate.)
- Configure the Task Manager to run scheduled housekeeping tasks as recommended for each individual task and as directed by the customer

Avaya Directory Enabled Management and Avaya Terminal Configuration

Verify successful installation by launching from START menu and VisAbility Management Suite homepage.

Avaya MultiService Network Manager and Avaya MultiService SMON Manager

Verify successful installation by launching from START menu and VisAbility Management Suite homepage.

Avaya VoIP Monitoring Manager

Once the Avaya VoIP Monitoring Manager has been installed, the RNIS Implementation Engineer will assist the customer in performing the following steps to verify proper operation:

1. Make sure that voice system is configured with the IP address of the management server hosting the VoIP Monitoring Manager Server.
   Start the VoIP Monitoring Manager server application. From the Windows 2000 server hosting the VoIP Monitoring Manager Server application, select **Start > Programs > Avaya > VoIP Monitoring Manager > VoIP Monitoring Manager Server.**
2. From the machine hosting the VoIP Monitoring Manager client, select **Start > Programs > Avaya > VoIP Monitoring Manager > VoIP Monitoring Manager Client** to start the VoIP Monitoring Manager client.
3. Start a call between two IP phones.
4. From the Search dialog on the client, select the search option **Sessions active in the last 1 minute**. This is the default setting. If the Search dialog is not visible on the screen, click the **Search** button to display the Search dialog.
5. Click the **Search** button. The Search Results List updates with a list of Active Endpoints. At least two endpoints should appear in the list. It will also list the Endpoint type, IP address and phone number. Now, select the Endpoint from the list and click the **Report** button to view the QoS data for that Endpoint.
6. Hang up the call and wait one minute.
7. From the Search dialog, select the search option **Sessions active in the last 1 minute again.** If the Search dialog is not visible on the screen, click the **Search** button to display the Search dialog. Click the **Search** button to be informed that there are no active endpoints.
8. Select the **Sessions active from** radio button.
9. Click the top date drop-down arrow to access the calendar and time for the starting period of your Search. Select hours, minutes, seconds and AM/PM, then select the day. Click outside the calendar window to close the calendar. Click the bottom date drop-down arrow to access the calendar and time for the ending period of the query as described above. The top and bottom date fields display the selected date.
10. Click **Search**. The Search Results List updates with a list of Historical Endpoints. It will also list the endpoint type, IP address and phone number. To view the QoS data, select the Endpoint and click the **Report** button.

Avaya Site Administration with Avaya Terminal Emulator

Implementation verification for ASA depends on whether the customer will be using ASA as a standalone application or as “cut-thru” for MultiVantage Configuration Manager.

- Verify successful installation by launching from START menu and VisAbility Management Suite homepage.
- For upgrades from an existing version of Avaya Site Administration or its predecessor DEFINITY Site Administration, verify that all customer settings remain in place.
- For new installation where MultiVantage Configuration Manager will not be present, add one voice system, verify that ASA can connect automatically (if so desired by the customer) or via a manual connection.
- Where ASA will be used for cut-thru with MultiVantage Configuration Manager:
  > verify that the voice system is configured to allow ASA to automatically log in and that the ‘launch with parameters’ option is selected.

  > verify that MultiVantage Configuration Manager will launch ASA when the cut-thru is selected and that ASA automatically connects to the correct voice system as dictated by the focus of the MultiVantage Configuration Manager client.

Avaya ATM WAN Survivable Processor Manager (ASPM)

- Configure ASPM to connect to the PPN and verify connection. Once connected ASPM will retrieve WSP(s) name(s)
- Configure connectivity information for each WSP and verify
- Configure e-mail notification feature if desired by customer
- Configure scheduled WSP updates to run as desired by customer

Avaya Voice Announcement over LAN Manager

- Verify successful installation by launching from START menu and VisAbility Management Suite homepage.
- Configure at least one voice system in VAL Manager and verify IP connectivity to the voice system and VAL board.

Appendix A - Overview of Customer and Avaya Responsibilities for implementation of Avaya VisAbility Management Suite

Table 7: Customer and Avaya Responsibilities

	Customer	Avaya
1. Software/Hardware Procurement:		
1a. Platform and Software Procurement		
Server hardware	✓	
Windows 2000 Server Operating System	✓	
Red Hat Linux 7.3 Operating System	✓	
HP OpenView Network Node Mgr for Windows 2000 (optional)	✓	
1b. Connectivity Device Procurement		
Remote access equipment to support product maintenance	✓	
2. Platform Installation and Configuration:		
2a. Microsoft Windows 2000 Installation and Configuration	✓	
Hardware-specific patches and drivers loaded	✓	
LAN Interface Card configuration	✓	
Platform Acceptance Test	✓	
Verification of Platform Readiness		✓
2b. Red Hat Linux 7.3 Installation and Configuration	✓	
Hardware-specific patches and drivers loaded	✓	
LAN Interface Card configuration	✓	
Platform Acceptance Test	✓	
Verification of Platform Readiness		✓
2c. NMS O/S Installation and Configuration (optional)	✓	
Hardware-specific patches and drivers loaded	✓	
LAN Interface Card configuration	✓	
Install and Configure Trouble Ticketing software	✓	
Platform Acceptance Test	✓	
Verification of Platform Readiness		✓
3. Switch and Connectivity Configuration and Testing:		
Remote access (via phone line connectivity)	✓	
LAN and IP connectivity	✓	
Creation of application-specific administration UserID and Password on managed voice and messaging systems	✓	
Administration of server IP addresses on voice systems (where required)	✓	

4. Avaya VisAbility Management Suite Application Installation and Configuration:		
Avaya Site Administrator / Avaya Terminal Emulator	✓	✓
Avaya Voice Announcement over LAN Manager	✓	✓
Avaya Voice-over-IP Monitoring Manager	✓	✓
Avaya Network Manager	✓	✓
Avaya SMON Manager	✓	✓
Avaya ATM WAN Survivable Processor Manager	✓	✓
Avaya Directory-enabled Management		✓
Avaya MultiVantage Fault and Performance Manager		✓
Avaya MultiVantage Configuration Manager		✓
Avaya MultiVantage Proxy Agent		✓
Avaya Terminal Configuration	✓	✓
5. Avaya VisAbility Management Suite Integration with NMS:		
Avaya Network Manager	✓	✓
Avaya MultiVantage Fault and Performance Manager		✓
6. System Verification and Acceptance:		
Verify proper operation of Avaya VisAbility Management Suite applications	✓	
Customer acceptance		✓

Appendix B - Installation of Red Hat Linux 7.3 to host Avaya VisAbility Management Suite 1.3

This appendix specifies the options that you must select during the installation of Red Hat Linux 7.3 to support Avaya MultiVantage Fault and Performance Manager, Avaya MultiVantage Proxy Agent, and Avaya MultiVantage Configuration Manager. If an option is not specified in this document, select the default response.

Installing Red Hat Linux 7.3

1. At the "Install Type" prompt (screen #5), select the **Install** and **Server** options.
2. At the "Disk Partitioning Setup" prompt (screen #6), select **Manually Partition with Disk Druid**.
3. At the "Disk Setup" prompt (screen #7), click the **DELETE** button to delete any partitioning that appears for the hard drive.
4. Click the **ADD** button to add partitions in accordance with the table below.
   The precise partition sizes are shown for a 40GB hard drive. If the hard drive is bigger than 40GB, use the proportion column to partition the hard drive.

Table 8: Customer and Avaya Responsibilities

Mount Point	Partition Size (40MB HD)	Proportion of Disk Space (>40MB HD)	File System Type
/	800 MB	2%	ext3
/boot	100 MB	1%	ext3
/home	7000 MB	18%	ext3
/usr	13000 MB	33%	ext3
/var	13000 MB	33%	ext3
/swap	2048 MB	5%	swap
/tmp	3000 MB	8%	ext3
Total	38948 MB	100%	

5. At the "Network Configuration" prompt (screen #10), select the **static IP** check box.
6. Enter the static IP address; subnet mask; hostname (including domain name); gateway; and DNS addresses (including primary, secondary, and tertiary).

   Note: This step must be completed correctly to ensure that networking is set up properly. Please ensure that the IP address used is not in the 192.168.0.X range, as this is the range used by the PPP service.

7. At the “Firewall Configurations” prompt (screen #12), select **No firewall** with **Use default firewall rules**.

   Note: The VisAbility Management Suite installation process will override the setting and select the default firewall rules.

8. At the “Account Configuration” prompt (screen #15), enter the password for the root user, and then add users including one for Avaya remote services.

9. At the “Package Group Selection” prompt (screen #16), select **Classic X window System**, **GNOME**, and **Anonymous FTP Server**.

Installing Additional Software

1. After you install Red Hat, you must install the following individual RPM (Red Hat Package Manager) files from the Red Hat CD:
   a) mgetty
   b) mgetty-sendfax
   c) uucp
2. In addition, verify that the following RPM files were loaded during the Red Hat installation:
   a) ppp
   b) vnc
   c) vnc-server

If you need to install an RPM, following the instructions below.

Installing Red Hat Package Manager (RPM) files

1. Insert the Red Hat installation CD in the CD-ROM drive (May be #1, #2 or #3 depending on the RPM required).

2. Open the Terminal Emulation program.

3. Mount /dev/cdrom (unless the CD ROM auto-mounted already).

4. Type: **`cd /mnt/cdrom/RedHat/RPMS.`**

5. At the $ prompt, type: **`rpm -hiv <name of RPM package>.`**

Determining whether RPM files are already installed

At the $ prompt in the terminal emulation window, type:
`rpm -qa <name of RPM package>.`

To search for RPM files using a partial RPM package name, at the $ prompt type:
`rpm -qa | grep <partial name>.`

For example, type: **`rpm -qa | grep vnc`** to determine if any RPM packages containing the letters "vnc" have been installed.

Once this has been done, the customer should try to dial into the server via an analog DID line connected to the modem on COM1. They should get a Linux "login" prompt. The customer must ensure this works prior to the due date. If the modem does not answer, or a login prompt is not received, perform the following steps:

1. Log on to the Linux system as root.

2. Edit the /etc/inittab file with your favorite editor.

3. Add the following line to the file:

   ```
   S0:2345:respawn:/sbin/mgetty –D ttyS0 -s 38400 -x 0
   ```

   NOTE:
   Make sure the entry after the "`-D`" option is the correct port for the modem you are using. "`ttyS0`" is used since that is the port for COM1 on most servers.

4. Write and quit the file.

5. At the "#" prompt, type **`init q`** and press the ENTER key.

   The "#" prompt appears, and you now have an mgetty process running. To verify this process, type **`ps –efw | grep mgetty`** and press the ENTER key. You will see the process running. An example of this process is:

   ```
   root   21213   1    0    Mar19  10:20:30   /sbin/mgetty –D ttyS0 -s 38400 -x 0
   ```

Index

Additional Resources 2
Application Description 14
Application Environment 4
Application Installation and Configuration ..18
ATM WAN Survivable Processor Manager (ASPM) 21
Avaya and Customer Responsibilities.........15
Avaya MultiVantage Configuration Manager 19
Avaya MultiVantage Fault and Performance Manager and MultiVantage Proxy Agent.....18
Case Implementation Coordinator (CIC) 13
Client PC Hardware 8
compatibility with voice systems, messaging systems and call management systems...........4
Computing Platform................................9, 17
Configuration Request Form........................14
Connectivity / Network Connections 8, 9
Conventions Used in This Book.....................1
Customer and Avaya Responsibilities..........22
Customer Implementation Options 11
Data Help Desk (DHD) 13
Determining whether RPM files are already installed 26
Directory Enabled Management and Terminal Configuration 19
General Network Information 14
Hardware Components...................................6
How to Access This Book on the Web...........3
Implementation Request Form 14
Implementation Services 10
Implementation Verification 18
Installing Additional Software 25
Installing Red Hat Linux 7.3 24
Installing Red Hat Package Manager 25
Intended Audience 1
IP Connectivity 17
Linux CRF...14
MultiService Network Manager and MultiService SMON Manager 19
Operating Environment 5
Operating Environment of Server components 5
Order and Contact Information 14
Overview of Avaya Implementation Services 12
Product and Services Requested 14
Product Packaging.......................................10
Purpose of the Document 1
Red Hat Linux 7.3 Server Hardware 7
Remote Access hardware and software..........9
Remote Connectivity...................................16
RNIS Implementation Engineers.............13
RNIS Service Request Documentation 14
Scope of this Document 1
Services Organizations involved in Avaya VisAbility Management Suite Implementations..13
Site Administration with Terminal Emulator 21
Solaris 8.0 Server Hardware...........................7
Specific Implementation Tasks 15
Symmetric Multi-Processor (SMP) support...9
Tell Us What You Think!..............................3
Voice and Messaging System Compatibility .4
Voice Announcement over LAN Manager ..21
VoIP Monitoring Manager...........................20
Windows 2000 Server Hardware 6
Windows CRF...15