



Avaya™ Interactive Response
Release 2.0
Maintenance

Issue 1.0
Publication Date: April 2006

Notice

While reasonable efforts were made to ensure that the information in this document was complete and accurate at the time of printing, Avaya Inc. can assume no liability for any errors. Changes and corrections to the information in this document might be incorporated in future releases.

Documentation disclaimer

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

Link disclaimer

Avaya Inc. is not responsible for the contents or reliability of any linked Web sites referenced elsewhere within this documentation, and Avaya does not necessarily endorse the products, services, or information described or offered within them. We cannot guarantee that these links will work all the time and we have no control over the availability of the linked pages.

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 Avaya Support Web site:

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

License

USE OR INSTALLATION OF THE PRODUCT INDICATES THE END USER'S ACCEPTANCE OF THE TERMS SET FORTH HEREIN AND THE GENERAL LICENSE TERMS AVAILABLE ON THE AVAYA WEB SITE <http://support.avaya.com/LicenseInfo/> ("GENERAL LICENSE TERMS"). IF YOU DO NOT WISH TO BE BOUND BY THESE TERMS, YOU MUST RETURN THE PRODUCT(S) TO THE POINT OF PURCHASE WITHIN TEN (10) DAYS OF DELIVERY FOR A REFUND OR CREDIT.

Avaya grants End User a license within the scope of the license types described below. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the Documentation or other materials available to End User. "Designated Processor" means a single stand-alone computing device. "Server" means a Designated Processor that hosts a software application to be accessed by multiple users. "Software" means the computer programs in object code, originally licensed by Avaya and ultimately utilized by End User, whether as stand-alone Products or pre-installed on Hardware. "Hardware" means the standard hardware Products, originally sold by Avaya and ultimately utilized by End User.

License type(s)

Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A "Unit" means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Product that permits one user to interface with the Software. Units may be linked to a specific, identified Server.

Shrinkwrap License (SR). With respect to Software that contains elements provided by third party suppliers, End User may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as "shrinkwrap" or "clickwrap" license accompanying or applicable to the Software ("Shrinkwrap License"). The text of the Shrinkwrap License will be available from Avaya upon End User's request (see "Third-party Components" for more information).

Copyright

Except where expressly stated otherwise, the Product is protected by copyright and other laws respecting proprietary rights. Unauthorized reproduction, transfer, and or use can be a criminal, as well as a civil, offense under the applicable law.

Third-party components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information identifying Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site:

<http://support.avaya.com/ThirdPartyLicense/>

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 can 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, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support Web site:

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

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 can be accessed by 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 might be otherwise authorized) who accesses your telecommunications equipment with either malicious or mischievous intent.

Such intrusions might 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 might 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 might 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 must carefully program and configure:

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

TCP/IP Facilities

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

Standards Compliance

Avaya Inc. is not responsible for any radio or television interference caused by unauthorized modifications of this equipment or the substitution or attachment of connecting cables and equipment other than those specified by Avaya Inc. The correction of interference caused by such unauthorized modifications, substitution or attachment is 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. might void the user's authority to operate this equipment.

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.

Canadian Department of Communications (DOC) Interference Information

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

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

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

European Union Declarations of Conformity



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

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

Trademarks

Avaya, the Avaya logo, and Interaction Reponse, are either registered trademarks or trademarks of Avaya Inc. in the United States of America and/or other jurisdictions.

All other trademarks are the property of their respective owners.

Downloading documents

For the most current versions of documentation, see the Avaya Support Web site:

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

Avaya support

Avaya provides a telephone number for you to use to report problems or to ask questions about your product. The support telephone number is 1 800 242 2121 in the United States. For additional support telephone numbers, see the Avaya Support Web site:

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

Contents

Maintenance.....	6
Customer maintenance activities	6
Solaris system event monitoring	8
Avaya maintenance support	8
Troubleshooting support.....	8
Hardware repair	9
Upgrades and migrations.....	9
System restoration.....	9
Remote access for maintenance.....	9
Remote access vs. other types of access	10
Effect of system state on system functions.....	11
Performing preventative maintenance	12
Effective IR system monitoring	12
System recovery plan	16
Preventative maintenance to do list.....	17
IR System Data Form	18
Managing IR system performance	19
Performance management guidelines	19
Changes that may affect performance.....	19
Recognizing symptoms of performance problems.....	20
Identifying the causes of problems	20
Checking system resources.....	23
Solving performance problems	25
Index.....	31

Maintenance

The topics in this section introduce you to maintenance for the IR system. You find out how to take care of your system and how to handle any performance problems that may arise. You also learn about the support services provided by Avaya.

This section includes the following topics:

Customer maintenance activities	6
Solaris system event monitoring	8
Avaya maintenance support.....	8
Remote access for maintenance.....	9
Performing preventative maintenance	12
Managing IR system performance	19

Customer maintenance activities

Monitoring the IR system

With regular monitoring of your Avaya IR system, you can spot problems before they become serious. You make test calls and check the **Message Log Report** screen and the **Display Equipment** screen for information on system conditions. You also can use the **sysmon** command to observe call handling operations.

Managing IR system performance

Your IR system is configured to support the business operations required of it. If you continue to add capabilities, you may start experiencing performance problems that are caused by overloading the IR system. By checking system resources and reducing load, you can avoid overload situations that may affect voice operations.

Performing preventative maintenance

Maintaining backups and system records will speed up and simplify troubleshooting any problems with your IR system. Performing preventative maintenance on page 12 explains what you need to do and includes an *Avaya IR System Data Form* on page 18 for record keeping.

Investigating problems

If you notice problems when monitoring your IR system, you may use a variety of information resources and tools to investigate them. Avaya support representatives help you troubleshoot problems and arrange for any necessary repairs. Avaya maintenance support on page 8 explains the services they provide.

Updating Sun Solaris patches

To help ensure that you are taking advantage of the latest Sun operating system (OS) patches and their capabilities, Avaya provides the following services to help you:

- Any security patches that Sun releases will be tested and verified for Avaya IR system compatibility as soon as possible after their release by Sun. As soon as they have been tested and verified, they will be listed on the Avaya customer support website (support.avaya.com (<http://support.avaya.com>)). If you become aware of a new Sun security patch and you want to check on its status with respect to the Avaya IR system, please feel free to contact your field support representative.

Note:

Avaya only lists the patches that are available. To obtain the patches, you must go to the Sun download site (<http://www.sun.com/software/download/patches.html> (<http://www.sun.com/software/download/patches.html>)).

- Solaris patch clusters are released on a quarterly basis and will be listed on the Avaya customer support website (support.avaya.com (<http://support.avaya.com>)) as soon as it is verified that they are compatible with the Avaya IR system.

Note:

Avaya only lists the patches that are available. To obtain the patches, you must go to the Sun download site (<http://www.sun.com/software/download/patches.html> (<http://www.sun.com/software/download/patches.html>)).

- If you become aware of other Sun patches for your system, and you want to check on its status with respect to your system, please feel free to contact your field support representative.

Solaris system event monitoring

The Solaris operating system monitors critical hardware events. These include temperatures outside of range (too high or too low) and fan malfunctions. On the IR system, the **Message Log Report** screen of the Web Administration interface displays messages about these events.

Avaya maintenance support

After your IR system is installed and the feature licensing is set up, Avaya provides maintenance support to ensure successful operations. Charges for maintenance support may or may not apply, depending on the type of maintenance contract you have, and the type of work that is required.

Troubleshooting support

Avaya support representatives are available by phone to troubleshoot problems on your IR system. Avaya can dial in to check system information and run tests. Avaya may also receive notice of a problem before you are even aware of it. See [Remote access for maintenance](#) on page 9 for details.

In most cases, problems are resolved without the need to dispatch a technician to your site. Avaya support representatives will work with you to help identify the cause of the problem. If the problem is caused by a device, application, or connection that is not part of the IR system, you need to receive help from a resource outside of Avaya to resolve the problem. For instance, you may need to contact your:

- Application vendor for problems caused by application errors or application inefficiency
- LAN administrator for LAN transmission problems
- Local exchange carrier (LEC) for issues with the public switched telephone network (PSTN)
- Third-party vendors for errors in speech programming and problems with third-party software
- Database administrator for database setup and transaction issues

You will want to resolve problems, especially those that affect voice operations, as quickly as possible. [Performing preventative maintenance](#) on page 12 explains how to maintain the information and provides resources that you need to support effective troubleshooting. The Troubleshooting section describes the requirements for successful voice response operations and explains how things can go wrong.

Hardware repair

If a component of your IR system needs repair or replacement, an Avaya support representative will generally arrange to dispatch a technician to your site. Other than failed hard drives in a mirrored system, you should not attempt to remove or repair components yourself.

Upgrades and migrations

Upgrades

When you need to add capacity or activate new features on your IR system, contact your Avaya sales representative. Avaya sales and support representatives will work with you to set up and complete the upgrade.

Migrations

The Remote Services Center (RSC) supports migrations of data from previous versions of the IR system. Contact your Avaya support representative for more information.

System restoration

If your IR system is affected by a disaster or other event that causes data loss, Avaya support representatives will work with you to restore the system. These guidelines apply to system restoration:

- Work done by Avaya to restore systems is billable.
- System restoration is much faster and easier if you have complete system backups and records. See [System recovery plan](#) on page 16 for more information.

Remote access for maintenance

Avaya IR systems may be accessed from a remote location. Remote access:

- Is almost always set up for Avaya support representatives
- May also be set up for employees of your organization who work in another location
- Is generally used to perform maintenance and troubleshooting functions

Implementation of remote access means that the Avaya IR system can:

- Dial out to at least two predetermined (user administrable) telephone numbers and provide an alarm status
- Call the INADS contact number (not administrable)
- Send alarm information via e-mail

Access is through a modem, and all commands can be managed via remote console. The ability to add, change, and delete privileges is limited to the Avaya IR system administrator.

Remote access vs. other types of access

For the most part, remote access provides the same capabilities as direct access to the Avaya IR system console and access through the LAN. Users can:

- Monitor system status and functions
- Perform administration, development, configuration, OS tuning, and maintenance functions
- Work with the operating system, boot PROM levels, and CMOS setup levels
- Check and change settings and configuration of the Sun Validation Test Suite (VTS) software
- Connect to the system via the external modem to manage the configuration, initialization, and operation of the modem by setting the modem's operating parameters, setting the modem initialization string, and resetting the modem

Additionally, messages can be written to the console (this ability may be disabled or enabled). Writing messages to the console is helpful if someone is at the console assisting with troubleshooting.

Remote access has a few limitations:

- Response time is slower. Using commands is preferable to using the Web Administration interface.
- The platform cannot be rebooted:
 - While the user views system status
 - From a remote connection
- The modem can be reset, but the connection is then dropped

Besides limitations that are caused by modem access, remote users may be constrained in the actions they perform by the state of the Avaya IR system. If the system is experiencing

problems, limited functions, or no functions at all, may be available. See [Effect of system state on system functions](#) on page 11 for more information.

Effect of system state on system functions

Frequently, remote access is used for troubleshooting purposes. If the IR system is experiencing problems, not all system functions may be available. The table that follows summarizes the effects of system states.

System states and causes	System actions	System availability
Normal <ul style="list-style-type: none"> Powered on or reset Passed self-test 	SunVTS software monitors events and executes actions.	Modem is available for platform use, for both placing and receiving calls. SunVTS responds to commands that reach SunVTS from the normal platform operating system.
Panic Dialout Panic Dialout command was received.	SunVTS: <ul style="list-style-type: none"> Takes control of the modem Dials a predetermined number Issues a panic message Disconnects Returns to the state previous to the receipt of the panic dialout command 	Reflects system status before receipt of panic dialout command. Connection to a remote session is maintained.
Built-in self-test Startup or Reset command was received.	SunVTS performs a self-test and goes into the normal, impaired, or disabled state depending on the results.	Reflects the system status after the self-test.
Impaired Non-serious hardware error detected by the built in self-test.	SunVTS operates to the fullest extent possible.	Reflects the functions available in the impaired state.

Disabled Self-test detected serious hardware error (severe or fatal problem with the processor complex or a problem that could degrade the host platform).	SunVTS and its modem are shut down.	No functions are available.
Authentication Remote caller connects to RSC.	SunVTS controls the modem and issues a login and password prompts.	Reflects the current system status.

Note:

Independent state does not apply to SunVTS. SunVTS does not run separately from the Sun Blade 150 operating system.

The platform performs a self-test of events when the platform is started or reset.

Remote users can manage panic dialout. They can:

- Turn off panic dialout during a remote session.

Panic dialout messages queue, and the user is notified that they are being queued. Panic dialout is re-enabled when the remote session ends. Queued panic dialout messages are released at that time.

- Clear panic dialout messages from the queue.

Performing preventative maintenance

To perform preventative maintenance, you check IR system operations and keep backups and system records up-to-date and accessible.

Effective IR system monitoring

The IR system has three resources that display information on system events and alarms. Two are part of the IR system web administration interface. On the Web Administration interface:

- The **Message Log Report** screen lists events and alarms experienced by the system.
- Alarms screens list alarms only.

The source logs that provide input into the Message Log Report screen and alarms screens may be viewed through log commands.

Besides checking information on system events regularly, you may customize the way the information is stored and displayed. Customizing and reviewing regularly are key actions in creating an effective monitoring system that helps you to resolve problems faster.

Viewing the Message Log report

By default, the **Message Log Report** screen (Reports > Message Log Report) lists all events and alarms experienced by the IR system. Over time, especially with large call volume and heavy activity, the information in the Message Log can become overwhelming.

However, you may focus on the information that is important to you at any given time. Modify the report to limit the display to messages and alarms regarding a particular component, timeframe, priority level, and so forth. Receive explanations of messages while viewing the report and update the report to show the latest events. For example, you may limit the display to messages regarding fax operations that were received in the last two days.

Administering messages

By administering messages regarding system events, you create a customized system that works for your organization and meets changing requirements.

Changing destinations

Default destinations for messages are as follows:

- Messages are sent to a message master log file.
- Alarms are sent to an alarm log file.
- Events are sent to an event log file.

Other destinations, such as pipes, send messages to specific file locations.

Changing priority levels

You may increase or decrease the default or current priority level for a system event. By changing priority, you may cause or stop alarms for a particular system event. For instance, assigning an event that normally does not result in an alarm a priority level of Minor results in an alarm for that event that appears in the Alarms screens.

Note:

While changing priority levels is useful, Avaya technical support representatives expect alarms to appear at their default levels. When you change priority levels, do so on a short-term basis. If you have changed priority levels and request support, let your technical support representative know.

Establishing thresholds

Establish thresholds for system events, and associate those thresholds with a threshold message that has a particular criticality level, and goes to selected destinations. For instance, a threshold message might be triggered when a certain number of fax print procedures fail within a specified time period. By establishing thresholds, you alert operations personnel to continued occurrences of events that would not usually result in alarms.

Administering alarms

The **Alarms** screens display only those system events that have alarm status. Changing priority level may cause an event to have or lose alarm status.

Retiring alarms

Alarms are displayed on the active alarms list until you retire them. The default order is time order, with the most recent alarms listed first. Once retired, active alarms move to a separate screen that lists the retired alarms. Retiring alarms that are no longer relevant makes it easier to review active alarms when you are troubleshooting a problem. Also, entering information about why the alarm was retired helps you keep records about system problems.

Establishing and revising dialout parameters

Establish and revise dialout parameters for modem calls placed when alarms occur. Generally, the modem will call INADS when an alarm occurs. You may choose to have no dialout, or dial out only for major and critical alarms. Three dialout locations may be specified, so that the IR system can dial out to remote locations as well as to INADS when alarms are generated.

Managing logs

System logs feed into the **Message Log Report** screen. Use log commands to review these logs directly and administer them.

Interpreting logs

Messages are sent to a number of specific log files. Log files may be lengthy and difficult to read. Log commands make them easier to interpret. *Locants* are parameters you specify to search log files (generally the date and time).

Administering logs

Use log commands to administer the content, format, and activities of logs. The table that follows identifies the functions of log commands.

Command	Function
logCat	Converts a file of compressed logging messages into readable format.
logDstPri	Creates the shared memory containing the dynamic destinations and priorities of logging messages using the logMsg interface
logEvent/logMsg	Allows shell scripts to log a specific message
logFmt	Displays and changes the parameters used to display messages and explanation texts, specifically the messages mnemonics and screen width
logIt	Logs the specified message in the logging files
logTest	Reads a script of logging messages to be sent to the logdaemon and sends the messages at the specified times and as the specified process

A word about the Tomcat server log

In Avaya IR Release 2.0, the Web Administration tool uses Tomcat as both the Web server and servlet engine. Tomcat periodically writes data to a log on the Avaya IR server.

Since the Tomcat server does not provide a method internally to delete old data, it continually adds to this data and will continue to do so unless cleaned up from time to time. We recommend that you check these log files on a regular basis and delete old data files when the size of the log file directory gets too large.

This file can be found at the following location:

/webadm/jakarta-tomcat-5.0.28/logs/localhost_log.<yyyy-mm-dd>.txt

where <yyyy-mm-dd> is the date of the last time the log was written to. For example, if the last date the log was written to was May 7, 2004, then the name of the log file would be:

localhost_log.2004-05-07.txt

System recovery plan

As with any other application running on a server, you should be prepared to do a partial or complete Avaya IR system restoration in the event of a disaster. Developing system documentation and maintaining backups helps you work with Avaya or act on your own to restore operations in the quickest, easiest manner.

Creating Avaya IR system records

Document the components and settings for your Avaya IR system:

- Keep a current list of all software, including versions, installed on your system.
- Store software in a safe and easily accessible location.
- Keep a list of your disk partitioning information, so you can restore applications to the correct location.
- Print and keep a copy of your **Display Equipment** screen.
- If you are using the VoIP feature, print and keep copies of configuration entries made using the **Assign VoIP Card** screen.
- Make sure that you know what to do to restore each application package. Record all values and parameters that must be entered.
- Record changes to system defaults.
- Record Avaya and other contacts and data about your system on the *Avaya IR System Data Form* on page 18.

Maintain backups

- Maintain two complete backups of your Avaya IR system. Identify backups by type, content, and date.
- Store backup copies away from the Avaya IR system (off-site, if possible).
- Keep copies of host configuration files that contain the information required on the Avaya IR system to be able to connect to a specific Host Mainframe System. (These files are sometimes called the host "GEN," because they can be used with an IBM SNA Mainframe NCP GEN system.)

Host configuration files

Save copies of host configuration files in case you need to restore the host connection to the Avaya IR system.

If you have a TN3270 connection, save copies of the following files:

- /etc/opt/tn3270/tn3270*.txt
- /vs/bin/util/tnstart
- /etc/hosts
- /etc/resolv.conf

If you have an SNA connection, save copies of the following files:

- /etc/opt/sna/sna*.txt
- /etc/opt/sna/sdlc.ini
- /etc/opt/sna/sna_node.cfg
- /etc/opt/sna/sna_domn.cfg
- /vs/bin/util/snastart

If you have completed a questionnaire for the vendor of host services, keep that as well.

Preventative maintenance to do list

Daily system monitoring

- Make test calls to the numbers your customers use to see if your system is handling calls as it should.
- Check the **Display Equipment** screen for cards or channels that are not in service (status of *oos).
- Check the **Message Log Report** for critical (C*) or major (**) errors.

Periodic maintenance

- Schedule partial backups to run daily, or at least weekly.
- Schedule full backups to run weekly, or at least monthly.
- Reboot the IR system monthly.
- Change the password associated with the **root** login monthly (If the password expires, cron jobs will not execute)
- Back up voice response applications after revisions have been made to them.
- Check cables on the back of the IR system for secure connections regularly.
- Use the **sysmon** command to observe live operations as needed.

IR System Data Form

Complete this form and provide copies to all IR system administrators.

Avaya resources	Avaya IR system information
Avaya Helpline: 1-800-242-2121	Customer Identification Number (CIN):
Avaya IR website: http://support@avaya.com	Installation Location (IL):
International customers go to the Avaya IR website to find Helpline phone numbers for their countries.	Dial-up number of modem: IP address of Network Interface Card (NIC):
Vendor and Internal Resources	
Names and phone numbers of application vendors:	Server names and IP addresses of IR system servers: Speech servers: Database servers: Application servers:
Names and phone numbers of speech vendors:	Telephone numbers for test calls:
	Sample account numbers for testing:
Names and phone numbers of database vendors:	

Note:

Keep a copy of your sign-on names and passwords in a location that is secure.

Managing IR system performance

When your Avaya IR system is installed, it is configured to support the various transactions that are required of it. As you make changes to your system, you may find that performance problems develop. As with any computer, these problems are the result of too many processes competing for system resources.

Performance management guidelines

To get the most out of your Avaya IR system, you need to:

- Consult with your Avaya sales representative to verify potential changes to system operations due to adding features, particularly the Natural Language Speech Recognition (NLSR) feature.
- Look for symptoms of performance problems before the problems become serious.
- Identify possible causes of performance problems.
- Solve performance problems by reducing the load on the CPU, memory, and hard drive.

Changes that may affect performance

The following types of changes may result in performance problems:

- Adding ports and channels
- Enhancing voice response applications
- Activating and enhancing features

Natural Language Speech Recognition (NLSR), Proxy Text-to-Speech (PTTS), Avaya Recognizer, VoiceXML, TN3270 host (combined with JDBC or TN3270 host, or JDBC alone) place a heavy load on the system. The use of NLSR can dramatically change performance.

When you make changes to your system configuration or to voice response applications, be sure to monitor the system for performance problems.

Recognizing symptoms of performance problems

Most performance-related problems become noticeable in one or more of the following ways:

- Users report poor response times to commands, speech breaks, or slow speech responses.
- Load-related messages and alarms appear in the **Message Log Report** screen.

Typically, if load increases to the point where the system cannot serve voice processing requests in real time, alarms are logged. Solaris interprocess communication (IPC) message queues may also indicate that the system is nearing its load threshold.

Note:

You cannot monitor NMS cards separately. Look for NMS-related alarms and problems with call handling to determine if the NMS cards are overloaded.

- Traffic reports show an increase in hold times and in calls or trunks being blocked.

To spot performance problems early, monitor your Avaya IR system carefully. Make test calls and check the Message Log Report screen every day. When alarms and messages appear, they help you to identify the cause of the problem. The type of alarm and the timing can provide valuable information.

Identifying the causes of problems

Performance problems may be caused by system processes external to voice response applications or by the voice response applications themselves. Before analyzing voice response applications for load liabilities, assess Avaya IR external system processes and check on potential issues with LAN communications. Correcting problems with external processes and with LAN communications is generally less time-consuming than making changes to voice response applications.

Assessing external processes

Poorly-managed external processes can have a negative effect on system resources. When external processes coincide with the appearance of load-related alarms, that is a definite indication of a problem with overloaded resources.

Excessive external processes

System resources may be affected by:

- Excessive use of call data event tracking
- Too many requests to the 3270 host interface
- Reading of large (more than 500 records) database tables that are not indexed
- Reading and writing an excessive number of records to database tables
- Use of the system monitor program with a fast refresh rate (anything less than the default rate of 5 seconds)

Ill-timed external processes

System resources may be affected by:

- Use of the voice response application generator on a production machine during peak load hours
- Requests for call data reports during peak load periods
- Performance of operation, administration, and maintenance functions, such as backups and speech administration
- Text-to-fax conversions
- Unnecessary system **cron** jobs running during operations hours

Note:

Every day at 12:15 a.m. all call data is summarized. If this coincides with voice processing activity, even low activity, alarms may be reported.

Typical causes of performance problems

Typical problems that may affect system performance include:

- Inefficient or large, complex voice response applications

The most common cause of performance problems is inefficient voice response applications. *Verifying the efficiency of voice response applications is a critical step to resolving problems.* The person or team responsible for developing voice response applications is responsible for checking application efficiency.

- Excessive, ill-timed, or unnecessary Avaya IR system processes external to voice response applications

External processes are those required for system operations outside of voice response applications or for providing data to the voice response application. Since processes required for data access are driven by voice response applications, you may need to make changes to the applications to fix these performance problems.

- Voice processing that exceeds the capabilities of the system

If current voice processing exceeds the capabilities of your system, you will need to consider adding another system to handle the increased demand. However, there are actions you can take to reduce the load on your current system. This section explains how to reduce load.

- Bottlenecks or increased CPU usage caused by inadequate LAN access or incorrect LAN configuration

If your Avaya IR system receives voice response functions through the LAN, all speech LAN functions should be on their own LAN segment. If you are using touchtone and recorded speech, a separate segment is not required. You also may benefit from placing the Avaya IR system on a separate LAN segment if voice response applications frequently access remote databases. If CPU usage is high, make sure that all configuration settings are correct.

Unnecessary external processes

Certain external processes can be terminated if they are not providing a service to the voice response application. See the table that follows.

Process	Use
xferdip	Used only in bridging applications
lpsched	Required only if a line printer is being used with the system
network processes	Some may not be needed
sysmon	Provides an active view of call handling

Runaway and system-intensive processes

Check processes in these ways:

- If the **sar (1m)** command consistently shows 0 percent idle time, it is likely that a process is in an infinite loop. You can identify the process with **ps (1m)** by examining the change in its CPU time and run status. If it is a system process, contact a service representative. If it is a user process, repair as required.
- The command **/usr/ucb/ps_-aux | head** identifies the leading CPU-intensive process.
- The **top** command identifies the process currently running.

Testing LAN communications

If you are experiencing delays and interruptions in transferring data across the LAN, take these steps:

- Place the IR system on a separate LAN segment, if necessary.

IR systems that move speech traffic across the LAN by using Proxy Text-to-Speech, VoIP, or VoiceXML should be on a separate LAN segment. A separate LAN segment may also be required if there is heavy traffic between voice response applications and remote databases.

- Check current LAN connections and capacity.

You can check LAN traffic with a number of free sniffers that are available online. Work with your LAN administrator as needed to assess connections and make required changes. The following recommendations apply to LAN bandwidth requirements:

- If the IR system transfers speech data over the LAN, the bandwidth required for speech operations should be less than 70% of total bandwidth.
- If the IR system does not transfer speech data over the LAN, the bandwidth required for speech operations should be less than 20% of total bandwidth.

Assessing voice response applications

To assess voice response applications, check the ways that the application:

- Uses code, sub-applications, and channels
- Manages transactions between the caller and databases
- Manages host interactions
- Receives database records through the LAN
- Plays voice (coding algorithms, phrase length, quantity of speech data required)

Refer to [Modifying voice applications](#) on page 28 for very basic information on resolving performance problems related to voice response applications.

Checking system resources

You check system resources when you suspect performance problems or want to know how close to capacity your Avaya IR system is.

Checking disk resources

To check disk resources enter **sar -c** or **sar -c 5 50**. The system displays the **Disk Resources** screen.

Note:

If the sum of the **rchar/s** and **wchar/s** columns is consistently greater than 320000 during the busy hour, then it is likely that the lack of sufficient disk resources is causing performance problems.

Checking memory resources

To check memory resources:

1. Do one of the following.

- Type **sar -p** and press **Enter**.
- Type **sar -p 5 50** and press **Enter**.

The system displays the **Memory Resources** screen.

2. Check the column labeled **vflt/s**. Note if this value is consistently close to or greater than 50.00.
3. Type **sar -g** or **sar -g 5 50** and press **Enter**.

The system displays the Memory Resources screen with new information.

4. Check the column labeled **pgscan/s**. Note if this value is consistently close to or greater than 100.
5. Type **sar -r** and press **Enter**.

The system displays the Memory Resources screen with new information.

6. Check the column labeled **freemem**. Note whether this value:
 - Is consistently close to or less than 100 *or*
 - Consistently decreases and does not regain memory for multiple days
7. If two or more values consistently follow the pattern that follows, then reduce memory usage.
 - **vflt/s** > 50.00
 - **pgscan/s** > 100
 - **freemem** < 100

Note:

Besides memory overload, processes being created and terminated regularly will also cause **vflt/s** to increase. If this is the case, memory may be sufficient, but the creation of processes is forcing the operating system to page processes

to disk and back into memory. When processes are paged, they respond more slowly, and speech processing may be interrupted.

Checking CPU resources

To check the CPU resources:

1. During the busy hour or when alarms are being logged, type **sar** and press **Enter**.

The system displays the **CPU Resources** screen. The sum of columns 2 and 3, (**usr + sys**) represents the percentage of CPU being used.

2. During the busy hour only, type **sar -u 5 50** and press **Enter**.

The system displays current CPU usage every 5 seconds for 50 seconds.

If either of these tests show CPU utilization consistently over 70 percent, it is likely that CPU overload is causing the performance problem.

Solving performance problems

To solve performance problems you need a thorough understanding of the:

- Configuration of your Avaya IR system, including LAN connections and use of remote servers
- Design of voice response applications running on your system
- Transactions handled by your Avaya IR system

Alarms, user reports, and the information in this section provide the details you need to manage performance. Once you know what is affecting the CPU, memory, and hard drives, you can take steps to reduce load. The approach that you take depends on the likely cause of the problem and on the impact on system resources or the LAN. Once you understand these factors, you can take steps to improve performance.

Tactics for solving performance problems

Depending on the situation, you may:

- Manage external processes to reduce their impact
- Modify voice response applications to improve their efficiency
- Improve LAN connections to reduce bottlenecks

- Add capacity by adding another Avaya IR system

Managing external processes

When external system processes cause performance problems, you may:

- Reduce the occurrence of excessive processes
- Eliminate unnecessary processes
- Reschedule ill-timed processes
- Relocate processes to other servers on the LAN

Besides taking these general actions, you may take specific steps to reduce requirements resulting from DIPs, IRAPI commands, host interactions, and database transactions.

Modifying external processes

You can free up system resources by modifying external processes.

Terminating processes

Terminate unnecessary system processes by taking these steps:

- If you do not bridge applications, enter **xferdip_off** to terminate the **xferdip** process.
- If you are not using a line printer with the system, enter the command **/usr/lib/lpshut** to turn off the lp scheduler. You may also rename the **S80lp** file from the **/etc/rc2.d** directory to **s80lp**. This action prevents the process from executing during startup, but maintains the file on the system should you need the scheduler in the future.
- Eliminate network processes, such as **rwhod** and **routed**, that are not required.
- Do not run **sysmon** in systems with insufficient memory.

Reducing and rescheduling processes

- Cut back on the use of demanding processes, or schedule them for a time when voice activity is low or non-existent. Demanding processes include running call data reports, reviewing **sysmon**, creating backups, administering speech, and so forth.
- If you cannot eliminate processes, be sure that all the packages on your system are being used and are not occupying memory unnecessarily.
- Finally, if the **nbufs** parameter has been specified in the **/vs/data/spchconfig** file and a large number is specified, consider reducing **nbufs**. Reducing **nbufs** may increase the number of times that the hard disk is read for speech. However, the voice system is more tolerant of disk reading for speech than for paging.

Managing database transactions

When you need to reduce load from the local or remote database, keep these guidelines in mind:

- For large tables (over 500 records) that are read by the application, indexing the tables reduces the access time and impact on system performance. However, if tables are not indexed effectively, performance problems may remain.
- The insert (add) record operation is a much faster operation than the update (change) operation. One way to replace a change record with an add record is to add records to a table during the normal call hours and write a shell routine using SQL*PLUS to summarize and delete records during nonpeak hours.
- Encapsulating common database queries (those requiring multiple accesses on a single table or accesses from multiple tables) with SQL*Views reduces the number of transactions.
- Keep in mind that each call data event is a unique record in more than one table. Therefore, every time a call data event is accessed, the database table is updated at the end of the call.

Managing DIPs and IRAPI processes

Since DIPs can vary widely in size and complexity there is little specific information that can be given about DIP performance. However, consolidating DIPs generally improves efficiency. For instance, rather than using multiple DIPs to check the database and transfer data, combine processes into one DIP.

Additionally, DIPs should:

- Avoid using excessive memory (more than 200 pages).
- Avoid creating new processes by using **fork(2)** and **exec(2)** or **system(3)**.
- Reduce message sending by relying on minimal communication with the voice response application.

Managing host interactions

One option for improving host interactions is to increase the speed of the host link to decrease delays in host processing. You can also take the actions described in this section to better manage host interactions.

Reducing the load

Take these steps to reduce the load for the host communications:

- To make the voice system less dependent on host performance, limit the number of screens that must be sent to or retrieved from the host.
- Make sure that time-out periods are long enough for the host to respond, but not so long that callers must wait unnecessarily.

Since the parameters associated with the host can affect system performance, be aware of how the parameters are used and what is typical for the host system. To avoid locking out calls, keep track of how many Licensed Units (LUs) the system has and how many channels are to be used. For example, a situation could arise where a system with access to only 32 host LUs has 48 calls active, and each of those calls needs to access the host. As a result, 16 callers will be locked out of the host if LUs are not shared (reserved).

Hiding pauses

For host systems that are known to be slow at times, one way of hiding the pause from the host is to use an **announce** statement between the **send host screen** and the **get host screen** statements. This activity covers part of the time that the host is processing the user-input card number with an announcement that repeats the number to the caller. By the time the announcement is completed, the host may have responded, and the caller does not experience a lag in response time.

Example:

- Prompt and Collect (get card number)
- Get Host Screen A
- Send Host Screen A (send the card number to the host application)
- Announce (repeat the card number to the caller)
- Get Host Screen (retrieve caller data)

Modifying voice response applications

Voice response application developers may write problematic applications that inherently use system resources inefficiently or are extremely large and complex. Designing and developing voice response applications requires skill and training, and it is not the purpose of this topic to address these issues.

However, here are some key guidelines for making applications efficient:

- Since applications are interpreted, using the code for anything other than basic call flow control may result in unacceptable inefficiencies. Code segments performing complex lexical or arithmetic calculations should be considered as candidates for DIPs.
- Using sub-applications results in modular programs that are more efficient. For example, a main application allows a caller to select a language (that is, a version of an application

in a particular language). The caller input would then cause the main application to execute the language sub-application.

- Application scripts should be shared across channels whenever possible, and redundant code and data should be eliminated. The size of voice response applications, both code and data, affects memory usage.
- Interactions with hosts and databases should be handled efficiently, rather than being executed in a redundant manner. See Managing host interactions on page 27 and Managing database transactions on page 27 for details.

Besides these general guidelines, there are techniques to reduce the load for voice play. These are explained in the *Avaya IVR Designer Help*.

Index

A

- A word about the Tomcat server log • 15
- Administering alarms • 14
- Administering logs • 15
- Administering messages • 13
- Assessing external processes • 20
- Assessing voice response applications • 23
- Avaya maintenance support • 7, 8

C

- Changes that may affect performance • 19
- Changing destinations • 13
- Changing priority levels • 13
- Checking CPU resources • 25
- Checking disk resources • 23
- Checking memory resources • 24
- Checking system resources • 23
- Customer maintenance activities • 6

E

- Effect of system state on system functions • 11
- Effective IR system monitoring • 12
- Establishing and revising dialout parameters • 14
- Establishing thresholds • 14
- Excessive external processes • 20

H

- Hardware repair • 9
- Hiding pauses • 28

I

- Identifying the causes of problems • 20
- Ill-timed external processes • 21
- Interpreting logs • 14
- IR System Data Form • 7, 16, 18

M

- Maintenance • 6
- Managing database transactions • 27, 29
- Managing DIPs and IRAPI processes • 27
- Managing external processes • 26
- Managing host interactions • 27, 29
- Managing IR system performance • 19
- Managing logs • 14
- Modifying external processes • 26
- Modifying voice response applications • 23, 28

P

- Performance management guidelines • 19
- Performing preventative maintenance • 7, 8, 12
- Preventative maintenance to do list • 17

R

- Recognizing symptoms of performance problems • 20
- Reducing and rescheduling processes • 26
- Reducing the load • 27
- Remote access for maintenance • 8, 9
- Remote access vs. other types of access • 10
- Retiring alarms • 14
- Runaway and system-intensive processes • 22

S

- Security • 16
- Solaris system event monitoring • 8
- Solving performance problems • 25
- System recovery plan • 9, 16
- System restoration • 9

T

- Tactics for solving performance problems • 25
- Terminating processes • 26
- Testing LAN communications • 22
- Troubleshooting support • 8
- Typical causes of performance problems • 21

U

- Unnecessary external processes • 22
- Upgrades and migrations • 9

V

- Viewing the Message Log report • 13