Avaya™ Interactive Response

Release 1.0

Install and Troubleshooting Guide

Issue 3
Publication Date: March 2003
Document Number: 585-313-168
Comcode: 700250608

Notice
Every effort was made to ensure that the information in this document was complete and accurate at the time of printing. However, information is subject to change.

Preventing Toll Fraud
"Toll fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or 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, 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 Web site:

http://www.avaya.com

Select **Support**, then select **Escalation Lists.** This Web site includes telephone numbers for escalation within the United States. For escalation telephone numbers outside the United States, select **International Services Contacts.**

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 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).

Your Responsibility for Your Company's Telecommunications Security

The final responsibility for securing both this system and its networked equipment rests with you - an Avaya customer's system administrator, your telecommunications peers, and your managers. Base the fulfillment of your responsibility on acquired knowledge and resources from a variety of sources including but not limited to:

- Installation documents
- System administration documents
- Security documents
- Hardware-/software-based security tools
- Shared information between you and your peers
- Telecommunications security experts

To prevent intrusions to your telecommunications equipment, you and your peers should carefully program and configure:

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

Federal Communications Commission Statements

Part 15: Class A Statement
Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his own expense.

Part 68: Answer-Supervision Signaling. Allowing this equipment to be operated in a manner that does not provide proper answer-supervision signaling is in violation of Part 68 rules. This equipment returns answer-supervision signals to the public switched network when:

- answered by the called station,
- answered by the attendant, or
- routed to a recorded announcement that can be administered by the CPE user.

This equipment returns answer-supervision signals on all direct inward dialed (DID) calls forwarded back to the public switched telephone network. Permissible exceptions are:

- A call is unanswered.
- A busy tone is received.
- A reorder tone is received.

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.

European Union Declarations of Conformity

CE

Avaya Inc. declares that the switch equipment specified in this document bearing the "CE" (Conformité Europeénne) mark conforms to the European Union Radio and Telecommunications Terminal Equipment Directive (1999/5/EC), including the Electromagnetic Compatibility Directive (89/336/EEC) and Low Voltage Directive (73/23/EEC). This equipment has been certified to meet CTR3 Basic Rate Interface (BRI) and CTR4 Primary Rate Interface (PRI) and subsets thereof in CTR12 and CTR13, as applicable.

Copies of these Declarations of Conformity (DoCs) signed by the Vice President of R&D, Avaya Inc., can be obtained by contacting your local sales representative and are available on the following Web site:

http://support.avaya.com

Trademarks
Avaya, CONVERSANT, and Intuity are registered trademarks of Avaya, Inc.

Adobe and Adobe Acrobat are trademarks or registered trademarks of Adobe Systems, Inc. in the United States and in other countries.

U.S. Robotics and Sportster are registered trademarks of 3Com Corporation or its subsidiaries.

Alliance Generation is a registered trademark and NMS Communications, Natural MicroSystems, AG, Natural Access, NaturalFax are trademarks or service marks of NMS Communications Corporation or its subsidiaries.

Informix, DB2 are registered trademarks of IBM Corporation.

Microsoft, Windows, and Windows NT are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Nuance and Nuance Vocalizer are trademarks of of Nuance Communications, Inc.

Oracle is a registered trademark, and Oracle8i, and Oracle9i are trademarks or registered trademarks of Oracle Corporation

Sybase is a trademark of Sybase, Inc.

Speechify, OpenSpeech Server, OpenSpeech Recognizer, and OpenVXI are registered trademarks of SpeechWorks International, Inc.

Sun, Sun Microsystems, docs.sun.com, Java, Solaris, Sun Blade are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and in other countries.

Technical Support
To report problems or to request assistance setting up and using your system, contact the Avaya Technical Services Organization (TSO). The telephone number for support in the United States is 1-800-242-2121.

For additional support telephone numbers:

- Visit the Avaya Support Centre Web site.
- Select **Escalation Lists**. This Web site includes telephone numbers for escalation within the United States. For escalation telephone numbers outside the United States, click **International Services Contacts**.

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 Centre Web site http://support.avaya.com.

Ordering Information: Avaya Publications Center

Voice:	+1 207 866 6701 +1 800 457 1764 (Toll-free, U.S. and Canada only)
Fax:	+1 207 626 7269 +1 800 457 1764 (Toll-free, U.S. and Canada only)
Write:	Globalware Solutions 200 Ward Hill Avenue Haverhill, MA 01835 USA Attention: Avaya Account Manager
Web:	http://www.avayadocs.com
E-mail:	totalware@gwsmail.com

Acknowledgment
This document was written by the CRM Information Development group.

Contents

Installation overview

Installation of the Avaya IR system involves the following steps:

Hardware installation on page 9	Explains on-site setup of the hardware components.
Installing the system base software on page 15	Explains how to install the system base software from CD media.
Site-specific setup on page 23	Explains how to set up an Avaya IR system that includes both hardware and software components purchased from Avaya. These steps are not required if you purchased only Avaya IR software.
Installing packages and setting up features on page 29	Explains the process for installing optional and password-protected software, provisioning feature channels, and installing database software.
Working with service packs on page 37	Explains how to determine the current software release, verify which service pack is installed, obtain a service pack, and install service packs.
Backing up the system for the first time on page 41	Explains how to back up the system for the first time.
Restoring the system on page 43	Explains how to restore all the system software, applications, and data, if you have a recent full backup of your system.
Application and data migration on page 45	Explains how to bring voice response applications and data from previous versions of the Avaya IR system (such as CONVERSANT® Version 8).

Hardware installation

If you purchased an Avaya IR system that includes hardware and software, the hardware components are usually installed by an Avaya service technician or third-party service provider as part of the product maintenance agreement.

If you purchased a software-only system, you are responsible for obtaining the hardware components and either installing the hardware platform or arranging for installation by an Avaya service technician or third-party service provider. For information about the recommended hardware platform, see Hardware requirements on page 9.

The Avaya IR platform (Sun Blade 150) must be installed on a local area network (LAN) and have connectivity to a telephony network with which the system will interact. Telephony connectivity can be provided by digital trunks (either T1 or E1) from a telecommunications switch. If the Avaya IR solution uses Voice over IP (VoIP), the LAN provides the telephony connectivity to the switch.

Required documents for hardware installation

The following documents are required for installing the hardware. These documents are available on the *Avaya IR Documentation CD*, the *Avaya IR System Help*, and from the Sun and Natural Microsystems Web sites.

Document	**Web site**
Sun Blade 150 Getting Started	http://www.sun.com
Sun Blade 150 Service Manual	http://www.sun.com
AG4000 Installation and Developer's Manual	http://www.nmscommunications.com
US Robotics Sportster Manual	http://www.usr.com/support/s-main-menu.asp
System Administration Guide, Volume 3 – Managing and monitoring network services for Solaris 8	http://www.sun.com

Hardware requirements

If you purchased only the Avaya IR system software, the following hardware is required.

Sun Blade 150 platform

The hardware platform for the Avaya IR system is a Sun Blade 150 with the following features:

- Solaris 8 Update
- 650-MHz UltraSPARC-IIi processor
- 256-KB Ecache
- 512 MB memory
- One 40 gigabyte hard drive with ATA66 interface
- 1.44-MB diskette drive
- CD-ROM drive
- Three PCI connectors
- ATI Rage XL on-board graphics, 8 Mbyte RAM
- One serial port
- One parallel port
- 10/100 Ethernet network interface card (NIC)
- Two IEEE 1394 ports (Firewire)
- Four USB ports (two are required for keyboard and mouse)
- Country Kit with power cord, keyboard, and mouse

Telephony cards

Telephony cards provide the telephony interface to the system. The telephony card required for the Avaya IR system is the Natural Microsystems (NMS) AG 4000/1600. The Sun Blade 150 platform can have a maximum of two telephony cards.

External modem

A modem is required for remote maintenance and administration functions. The recommended modem is an external U.S. Robotics Sportster 33.6 kB faxmodem.

Modem cable

An RS-232 cable is required to connect the external modem to the serial port of the Sun Blade 150.

Installing the Sun Blade 150

To install the Sun Blade 150 computer:

- Select a physical location – must be on a local area network (LAN) and have telephony connectivity to a switch.
- Connect to power
- Connect the peripherals (such as monitor, keyboard, and mouse)

See Sun Blade 150 Getting Started for complete information on how to perform these tasks.

Installing telephony cards

If you purchased an Avaya IR system that includes hardware and software components, the system arrives from the factory with the purchased telephony cards pre-installed and tested. You should not need to install telephony cards for initial setup of the system.

If you purchased a software-only system, see the following documents for information about how to install the PCI telephony cards required for the Avaya IR system:

Sun Blade 150 Service Manual	This document describes the proper procedure for opening the chassis and installing cards in the PCI card slots.
AG4000 Installation and Developer's Manual	This document describes specific procedures for installing the AG4000 cards in the PCI slots and connecting the cards to the telephone network.

Connecting the platform

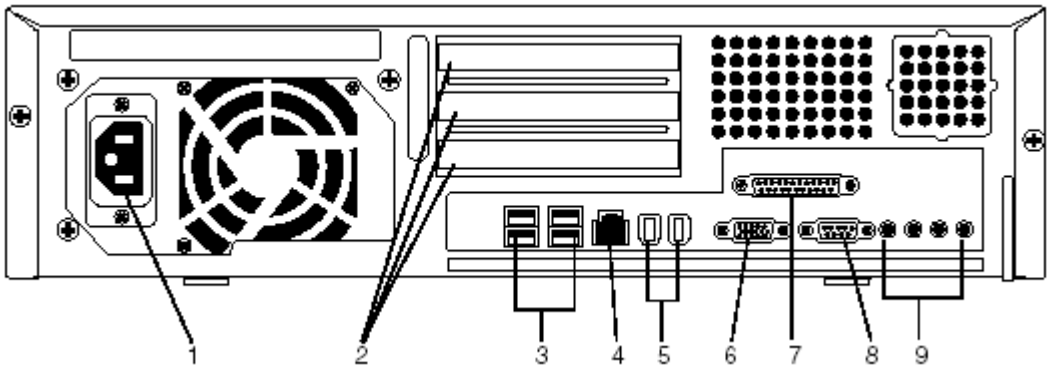
An Avaya IR platform must be connected to a local area network (LAN). It also must be connected directly to:

- The Public Switched Telephone Network (PSTN)
- An Avaya MultiVantage system, or
- A non-Avaya PBX that supports the required digital protocols

Connecting a Avaya IR to the LAN

The Avaya IR platform contains a network interface card (NIC) to communicate with the LAN.

A Category 5 (UTP-5 "data grade") cable from a LAN switch or hub is connected to the twisted-pair Ethernet (TPE) connector on the back panel of the Sun Blade 150 platform (location 4 in the diagram below).



For information about signals at the TPE connector, see the "Twisted-Pair Ethernet Connector" section in the "Signal Descriptions" chapter of the *Sun Blade 150 Service Manual*.

The Sun Blade 150 is set to auto-detect network speed and duplex. Avaya recommends setting the LAN switch or hub to auto-detect for optimal performance. If the LAN switch or hub is set to a specific speed, administer the NIC on the Sun Blade 150 to match that speed. For information on how to administer the NIC, see *System Administration Guide, Volume 3* from Sun.

Connecting trunks to a Avaya IR system

Up to two trunks may be connected directly to each NMS card installed on the Avaya IR system. Trunks may receive calls directly from the PSTN or they may connect to an Avaya MultiVantage system or to a non-Avaya PBX. Trunks connect to the back of the Sun Blade 150 platform (location 2 in the diagram above). See the *AG 4000 Developer's Manual* for more information on connecting trunks. See the appropriate MultiVantage or PBX documentation for information on connecting trunks to a MultiVantage system or non-Avaya PBX.

Installing the modem

To install the U.S. Robotics Sportster 33.6 Kb faxmodem:

1. Verify that the modem power is off.

2. Connect the modem cable.

   Connect the 9-pin connector to the Sun Blade 150 modem port, and connect the 29-pin connector to the modem.

3. Verify that the DIP switch, which is on the rear of the modem chassis, has the following settings:

Switch	1	2	3	4	5	6	7	8
Setting	Up	Up	Down	Down	Up	Up	Up	Down

   If necessary, set the switches.

1. Turn on the modem.

The modem will initialize when the Avaya IR system boots up.

See also

- *U.S Robotics Sportster Manual*

Configuring the modem

The modem is automatically configured by a script that runs at startup.

The following commands are run by the script:

Command	**Description**
set ProductID *product_id*	Sets the product ID.
set AlarmDest *telno*	Sets the telephone number (*telno*) to INADS alarming.
set Alarming [on | off]	Turns dial-out alarming on or off.
send Test Alarm	Sends a test alarm to INADS.
set-ppp-options *tsc_ppp local_IP remote_ID*	Sets up PPP for login account *tsc_ppp.*

Note:

If you want to modify the modem configuration after installation, use the Avaya IR Web Administration interface after the system is set up and running. See Starting the Web Administration interface on page 33.

Installing the system base software

This section explains how to install the system base software from CD media. You may need to install the system software from CD for the following reasons:

- You purchased a software-only system
- You need to rebuild your system from CD media

  Note:
  Another method of rebuilding your system is to restore the system from backup, which may be preferable if you have applications, data, and feature administration that also needs to be restored. See Restoring the system from backup on page 43 for more information.

Preinstallation

You will need the following information to respond to system prompts when you install the system from CDs:

General information:

- Language
- Locale

To configure the system on the IP network:

- Networked? (yes/no)
- DHCP? (yes/no)
- Host names
- IP addresses
- System part of a subnet? (yes/no)
- Network mask
- IPv6 enabled? (yes/no). Note that IPv6 is not supported.

To specify security option:

- Configure Kerberos security? (yes/no). Note that Kerberos is not supported.

To configure the system for the default router:

- Set default network router IP address? (yes/no)
- Default router IP address

To configure the system for name service:

- Name service type (DNS/NIS)
- DNS name service requires:
  - DNS server's IP addresses
  - DNS search domains
- NIS name service requires:
  - Server's host name
  - Server's IP address

To configure the system for date and time:

- Geographic region
- Time zone for region
- Date and time

To configure administrative passwords:

- Root password

Installing system software

Follow the steps below to install the system software from the Avaya IR CD media, which includes the Solaris 8 operating system and all the Avaya IR software. You will need the following CDs:

- Avaya IR R1.0 System Media and Drivers
- Avaya IR Recognizer Media R1.0
- Avaya IR R1.0 Server and Proxy Media R1.0

Note:
Many of the system prompts in this procedure require the use of function keys. Typically, if the function keys do not work, you can use them by pressing **Ctrl**+**F** then pressing **#** where **#** is the function key number. If the terminal type is **xterm**, then use the following procedure so the function keys will work properly:

1. Type **export TERM=xterm** and press **Enter.**
2. Type **export SMTERM=xterm** and press **Enter**.

Step	System prompt	Action
1.	After powering the system up, it displays messages indicating that it is attempting to boot the operating system from the hard disk.	At any point during or after the attempted boot process, display the open boot (ok) prompt by either: • Pressing Stop-A from the Sun console • Pressing Ctrl-Break from a serial port console
2.	ok	Open the CD-ROM drive bay and insert the CD labeled Avaya IR R1.0 System Media and Drivers. Close the CD-ROM drive bay.
3.	ok	Type boot cdrom - install and press Enter. The system displays messages indicating that it is resetting itself and initializing memory.
4.	Select a Language 0. English 1. French 2. German 3. Italian 4. Spanish 5. Swedish Please make a choice (0 - 5), or press h or ? for help:	Type the number of the language you want to use and press Enter.

5.	Select a Locale 0. English (C - 7-bit ASCII) 1. Albania (ISO8859-2) 2. Australia (ISO8859-1) 3. Belgium-Flemish (ISO8859-1) 4. Belgium-Flemish (ISO8859-15 - Euro) 5. Bosnia (ISO8859-2) 6. Brazil (ISO8859-1) 7. Bulgaria (ISO8859-5) 8. Canada-English (ISO8859-1) 9. Catalan,Spain (ISO8859-1) 10. Catalan,Spain (ISO8859-15 - Euro) 11. Croatia (ISO8859-2) 12. Czech Republic (ISO8859-2) 13. Denmark (ISO8859-1) 14. Denmark (ISO8859-15 - Euro) 15. Egypt (ISO8859-8) 16. Estonia (ISO8859-15) 17. Finland (ISO8859-1) 18. Finland (ISO8859-15 - Euro) Press Return to show more choices. Please make a choice (0 - 50), or press h or ? for help:	Type the number of the locale you want to use, which determines the format of screen text, and press Enter. **Note:** If the Sun keyboard is not connected to the computer's USB port, the system prompts you to specify the terminal type for the session. In this case, choose the terminal type you want to use and press Enter.
6.	Configuring default router Enter default router IP address (ex. 192.1.7.254) or 'none':	Type the IP address of the default router and press Enter. The system verifies the default router. This activity takes a few minutes to complete.
7.	The next two screens describe the installation program.	Press F2 to acknowledge the screens. If the system is attached to a network, it assumes that you want to configure the system for network usage. Go to Step 10. If the system is not attached ot the network, it displays the following prompt:
8.	Networked [ ] Yes [ ] No	If you plan to connect your system to a network, position the cursor between the Yes brackets using the arrow keys. Press Enter. An X appears in the brackets to indicate your selection. Press F2.
9.	Use DHCP [ ] Yes [ ] No	Select whether DHCP is to be used on your LAN. Press F2. If you choose No (the preferred option), the system uses static IP address for proxy connections.
10.	Host name:	Type your host name (the name of your computer on the network) and press F2.

11.	IP address:	Type the IP address of the computer and press F2.
12.	System part of a subnet [ ] Yes [ ] No	Choose whether your system is part of a subnet and press F2 If you choose Yes, the system prompts you for the subnet mask. In this case, enter the subnet mask and press F2.
13.	Netmask:	Type the subnet mask and press F2.
14.	Enable IPv6 [ ] Yes [ ] No	Choose No and press F2. IPv6 is not supported. After a short wait (approximately 30 seconds), the system displays the network information you entered similar to the following example:
15.	Host name: host IP address: IP address System part of a subnet: Yes Netmask: subnet mask Enable IPv6: No	Review the information to make sure it is accurate and press F2 to continue. If the information is not correct, press F4 and correct the information starting with the Networked question.
16.	Configure Kerberos Security [ ] Yes [ ] No	Choose No and press F2. Kerberos Security is not supported.
17.	The system displays a confirmation screen.	Press F2 to acknowledge.
18.	Name service [ ] NIS+ [ ] NIS [ ] DNS [ ] LDAP [ ] None	Select your name service and press F2. Although this is specific to your site, the most common selection is DNS. If you selected DNS, the system displays the following series of messages to set up the DNS name service.
18a.	Domain name:	Type your domain name and press F2.
18b.	Server's IP address: Server's IP address: Server's IP address:	You can enter up to three IP addresses for DNS servers. Type the IP address and press Enter to move to the next field. When done, press F2.
18c.	Search domain: Search domain: Search domain: Search domain: Search domain: Search domain:	You can enter up to six search domains. Type the search domain and press Enter to move to the next field. When done, press F2. The system displays the information you entered, similar to the following:

18d.	Name service: DNS Domain name: domain.com Server address(es): 127.0.0.1 Search domain(s): search.domain.com	Review the information to make sure it is accurate and Press F2 to continue. If the list is not correct, press F4 and correct the information starting with the domain name prompt. After the system accepts your name service information, it displays a series of messages requesting information about the time zone for the system.
19.	Regions [ ] Asia, Western [ ] Australia / New Zealand [ ] Canada [ ] Europe [ ] Mexico [ ] South America [ ] United States [ ] other - offset from GMT [ ] other - specify time zone file	Select the region for the system and press F2. The system displays a menu for selecting the time zone for the region you selected. The following example shows the time zones for the United States:
20.	Time zones [ ] Eastern [ ] Central [ ] Mountain [ ] Pacific [ ] East-Indiana [ ] Arizona [ ] Michigan [ ] Samoa [ ] Alaska [ ] Aleutian [ ] Hawaii	Select your time zone and press F2.
21.	Date and time: date time Year (4 digits): year Month (1-12) : month Day (1-31) : day Hour (0-23) : hour Minute (0-59) : minute	Verify that these values for year, month, day, hour, and minute are correct. If any values need to be changed, position the cursor in the appropriate field and type the correct value. Press Enter to move between field. When done, press F2. The system displays the time zone information you entered, similar to the following:

22.	Time zone: US/Mountain Date and time: 2002-07-03 10:38:00	Review the information to make sure it is accurate and press F2 to continue. If the information is not correct, press F4 and correct the information starting with the region prompt. The system installs the system software and configures the network. This takes a few minutes. When completed, the system displays the following prompt:
23.	Welcome To Avaya Interactive Response R1 Installation and Recovery. Please select one of the choices below. I to Install or R for Restore	To begin installing the base packages for the Avaya IR system, type I and press Enter. **Note:** To restore the system from backup at this prompt, see Restoring the system from backup on page 43. The system begins installing the base packages. After several minutes the system reboots and displays the following prompt:
24.	Root password:	Type the root password to be used on the system and press Enter.
25.	Re-enter your root password.	Type the root password again and press Enter. Lines similar to the following will appear:
26.	System identification is completed. Setting netmask of eri0 to XXX.XXX.XXX.X Setting default IPv4 interface for multicast: add net 224.0/4: gateway XXXXX syslog service starting. Print services started. volume management starting. Jul 3 10:48:56 XXXXX sendmail[293]: My unqualified host name (XXXXX) unknown; sleeping for retry The system is ready.	The system reboots and returns to the console login prompt. However, you may need to press Enter to display it.
27.	Console login:	Type root and press Enter.
28.	Password:	Type your root password and press Enter. The system logs you in and automatically opens the CD-ROM drive.

29.	The installation process will now continue. Put the CD labeled Avaya IR Recognizer Media R1.0 into the drive. Press enter when ready.	Remove the Avaya IR R1.0 System Media and Drivers CD and insert the Avaya IR Recognizer Media R1.0 CD into the CD-ROM drive. Press Enter. The system copies files from the CD. This takes a few minutes. When it is complete, the system automatically opens the CD-ROM drive and displays the following message:
30.	The contents of the Avaya IR Recognizer Media R1.0 CD have been installed. Put the CD labeled Avaya IR R1.0 Server and Proxy Media R1.0 into the drive. Press enter when ready.	Remove the Avaya IR Recognizer Media R1.0 CD and insert the Avaya IR R1.0 Server and Proxy Media R1.0 CD into the CD-ROM drive. Press Enter. The installation process continues for several minutes. When it is complete, the system displays the following message:
31.	Software installation is complete. Please reboot the system.	Type shutdown -y -g0 -i6 and press Enter. The system reboots and displays the login prompt for Solaris 8. You must now login and install individual packages required for your particular site. See Installing individual packages on page 29 for more information.

Site-specific setup

The information in *Site-specific setup* applies only if you purchased a system that includes hardware and software components. Site-specific setup is usually performed by an Avaya service technician or certified third-party service provider.

Information required

The following site-specific information is required to respond to system prompts when the system boots up for the first time:

General information:

- Language
- Locale

To configure the system on the IP network:

- Networked? (yes/no)
- DHCP? (yes/no)
- Host names
- IP addresses
- System part of a subnet? (yes/no)
- Network mask
- IPv6 enabled? (yes/no). Note that IPv6 is not supported.

To specify security option:

- Configure Kerberos security? (yes/no). Note that Kerberos is not supported.

To configure the system for the default router:

- Set default network router IP address? (yes/no)
- Default router IP address

To configure the system for name service:

- Name service type (DNS/NIS)
- DNS name service requires:

  - DNS server's IP addresses
  - DNS search domains
- NIS name service requires:
  - Server's host name
  - Server's IP address

To configure the system for date and time:

- Geographic region
- Time zone for region
- Date and time

To configure administrative passwords:

- Root password

Setting up site-specific configuration

The first time you turn on the power to the Avaya IR system, the system prompts you for information that sets up site-specific parameters.

Note:
Many of the system prompts in this procedure require the use of function keys. Typically, if the function keys do not work, you can use them by pressing **Ctrl**+**F** then pressing **#** where **#** is the function key number. If the terminal type is **xterm**, then use the following procedure so the function keys will work properly:

1. Type **export TERM=xterm** and press **Enter.**
2. Type **export SMTERM=xterm** and press **Enter**.

Follow the steps below to configure the system:

Step	System prompt	Action
1.	Select a Language 0. English 1. Fr Please make a choice (0 - 1), or press h or ? for help:	Type 0 and press Enter.

2.	Select a Locale 0. English (C - 7-bit ASCII) 1. Canada-English (ISO8859-1) 2. Thai 3. U.S.A. (en_US.ISO 8859-1) 4. U.S.A. (en_US.ISO 8859-15) 5. Go Back to Previous Screen Please make a choice (0 - 5), or press h or ? for help:	Type 0 and press Enter.
3.	The next two screens describe the installation program and what you will need to answer the prompts.	Press F2 to acknowledge the screens. If the system is attached to a network, it assumes that you want to configure the system for network usage. Go to Step 6. If the system is not attached ot the network, it displays the following prompt:
4.	Networked [ ]Yes [ ] No	If you plan to connect your system to a network, position the cursor between the Yes brackets using the arrow keys. Press Enter. An X appears in the brackets to indicate your selection. Press F2.
5.	Use DHCP [ ] Yes [ ] No	Select whether DHCP is to be used on your LAN. Press F2. If you choose No (the preferred option), the system uses static IP addresses for proxy connections.
6.	Host name:	Type your host name (the name of your computer on the network) and press F2.
7.	IP address:	Type the IP address of the computer and press F2.
8.	System part of a subnet [ ] Yes [ ] No	Choose whether your system is part of a subnet and press F2. If you choose Yes, the system prompts you for the subnet mask. In this case, enter the subnet mask and press F2.
9.	Netmask:	Type the subnet mask and press F2.
10.	Enable IPv6 [ ] Yes [ ] No	Choose **No** and press **F2**. IPv6 is not supported. After a short wait (approximately 30 seconds), the system displays the network information you entered similar to the following example:

11.	Host name: host IP address: IP address System part of a subnet: Yes Netmask: subnet mask Enable IPv6: No	Review the information to make sure it is accurate and press F2 to continue. If the information is not correct, press F4 and correct the information starting with the Networked question.
12.	Configure Kerberos Security [ ] Yes [ ] No F2_Continue F6_Help	Choose **No** and press **F2**. Kerberos Security is not supported.
13.	The system displays a confirmation screen.	Press F2 to acknowledge.
14.	Configuring default router Set default network router IP address [y,n,?]	To configure the default network router IP address, type y then press Enter.
15.	Set Router IP Address (ex. 192.1.7.254):	Type the router IP address then press Enter.
16.	The system asks if the address you entered is correct.	If it is, type y then press Enter.
17.	Name service [ ] NIS+ [ ] NIS [ ] DNS [ ] LDAP [ ] None	Select your name service and press F2. This choice and the prompts that follow are specific to your site. If you selected DNS, the system displays the following series of messages to set up the name server:
17a.	Domain name:	Type your domain name and press F2.
17b.	Server's IP address: Server's IP address: Server's IP address:	You can enter up to three IP addresses for DNS servers. Type the IP address and press Enter to move to the next field. When done, press F2.
17c.	Search domain: Search domain: Search domain: Search domain: Search domain: Search domain:	You can enter up to six search domains. Type the search domain and press Enter to move to the next field. When done, press F2. The system displays the information your entered, similar to the following:
17d.	Name service: DNS Domain name: domain.com Server address(es): 127.0.0.1 Search domain(s): search.domain.com	Review the information to make sure it is accurate and Press F2 to continue. If the list is not correct, press F4 and correct the information starting with the domain name prompt. After the system accepts your name service information, it displays a series of messages requesting information about the time zone for the system.

18.	Regions [ ] Asia, Western [ ] Australia / New Zealand [ ] Canada [ ] Europe [ ] Mexico [ ] South America [ ] United States [ ] other - offset from GMT [ ] other - specify time zone file	Select the region for the system and press F2. The system displays a menu for selecting the time zone for the region you selected. The following example shows the time zones for the United States:
19.	Time zones [ ] Eastern [ ] Central [ ] Mountain [ ] Pacific [ ] East-Indiana [ ] Arizona [ ] Michigan [ ] Samoa [ ] Alaska [ ] Aleutian [ ] Hawaii	Select your time zone and press F2.
20.	Date and time: date time Year (4 digits): year Month (1-12) : month Day (1-31) : day Hour (0-23) : hour Minute (0-59) : minute	Verify that these values for year, month, day, hour, and minute are correct. If any values need to be changed, position the cursor in the appropriate field and type the correct value. Press Enter to move between field. When done, press F2. The system displays the time zone information you entered, similar to the following:
21.	Time zone: US/Mountain Date and time: 2002-07-03 10:38:00	Review the information to make sure it is accurate and press F2 to continue. If the information is not correct, press F4 and correct the information starting with the region prompt.
22.	Root password:	Type the root password to be used on the system and press Enter.
23.	Re-enter your root password.	Type the root password again and press Enter.

24.	System identification is completed. Setting netmask of eri0 to XXX.XXX.XXX.X Setting default IPv4 interface for multicast: add net 224.0/4: gateway XXXXX syslog service starting. Print services started. volume management starting. Jul 3 10:48:56 XXXXX sendmail[293]: My unqualified host name (XXXXX) unknown; sleeping for retry The system is ready.	The system reboots and displays the login prompt for Solaris 8. You must now login and install individual packages required for your particular site. See Installing individual packages on page 29 for more information.

Installing packages and setting up features

After you have installed the system software from CD media or configured a system that includes hardware and software with site-specific information, you must install additional software packages, provision feature channels, and set up the features.

Installing individual packages

A system that includes hardware and software or a system with software installed from CD does not have the following optional packages installed:

- NMS package (AVnms)
- Proxy Text-to-Speech package (AVttsprxy)
- Speech Proxy package (AVsproxy)
- Speech Proxy - Speech Recognition package (AVsrproxy)
- TBCT package (AVtbct)
- Voice over IP package (AVvoip)
- Third-party packages (such as Vonetix)

These packages need to be individually installed using the **pkgadd** command. Once the packages have been installed, an Avaya service technician provisions the feature channels for each package as appropriate. See Provisioning feature channels on page 31 for more information.

Important:
You must install either the NMS package or the Voice over IP (VoIP) package to achieve voice communication and call processing with the Avaya IR system. The NMS package contains the software for interfacing with the telephony cards. The VoIP package contains the software for telephony communications using VoIP with a DEFINITY switch.

To install individual packages:

1. If you are not logged in, log in as root.
2. At the command prompt, type **cd /export/optional_features** and press **Enter**.

   This directory contains all of the optional and licensed packages.
3. Type **pkgadd -d . *package_name*** where *package_name* is the short name for the package you want to install. Press **Enter**.

The package installation starts. Depending on the package you are installing, the system displays various messages. In most cases, the system requires you to confirm some messages by pressing **Enter** (to choose the default **Yes** response).

Note:
If you do not confirm the package installation messages, the process will exit and the package will not be installed.

After a short time, the system displays a message indicating that the installation is complete.

4. If you are installing the AVnms package, type **/vs/bin/nms.install** and press **Enter**. Otherwise, skip this step.
5. Repeat Step 3 for additional packages you need to install.
6. When you have completed installing packages you must reboot the system. Type **shutdown -y -g0 -i6** and press **Enter** to reboot the system.

Installing optional packages

Some software packages are password-protected and must be installed by an Avaya service technician or certified third-party service provider.

Contact the Avaya Technical Services Organization (TSO) to have the following packages installed.

- WholeWord Recognition Base package (Avaya Recognizer)
- WholeWord speech recognition language packages
- VoiceXML package
- ASAI package
- CTI DIP package
- Enhanced Basic Speech packages
- Fax Actions package
- NG FAX package
- IC Integration package
- PDS Integration package

Provisioning feature channels

Once installed, some features must be provisioned by an Avaya service technician or certified third-party service provider to allow the system to use the feature. Provisioning is based on the number of channels of the feature purchased by the customer.

Contact the Avaya Technical Services Organization (TSO) to have the following features provisioned:

- Digital protocol - loop start
- Digital protocol - PRI
- Digital protocol - wink start
- NMS NaturalFax
- Avaya Recognizer (WholeWord speech recognition)
- Natural Language Speech Recognition (NLSR)
- Proxy Text-To-Speech (PTTS)
- Voice over IP (VoIP)

After feature channels are provisioned, a service pack may have to be installed. For information about service packs, see Working with service packs on page 37.

Setting up user accounts

To use the Web Administration tool to set up features on Avaya IR, you can use the root login and password, or you can set up one or more additional user accounts with the correct administrative privileges.

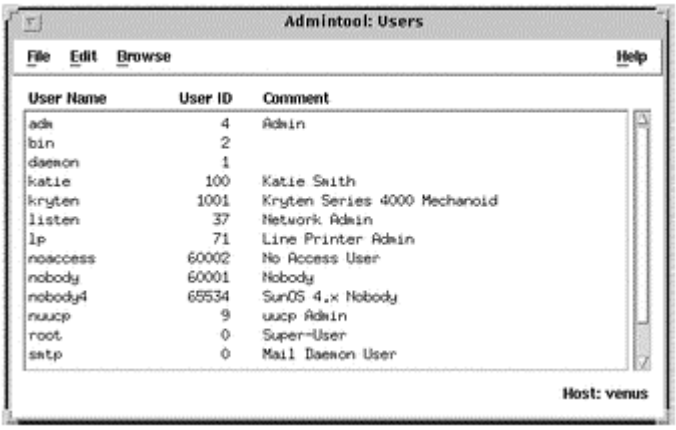
Setting up user accounts for administering Avaya IR includes:

1. Establishing the user account with **admintool**
2. Assigning administration privileges with the **assign_permissions** command.

To establish user accounts:

1. Log in as root.
2. At the command prompt, type **admintool &** and press **Enter**.

   The **Admintool** interface starts, as shown in the following figure.



3. On the Edit menu, choose **Add**.

   The system displays the **Add User** window.

4. Complete the Add User window with information about the new user and click **OK**.

   Consider the following points when entering data about the new user:

   — User ID numbers must be a whole number less than or equal to 2147483647. They are required for both regular user accounts and special system accounts. Although User ID numbers 0 through 99 are reserved, you can add a user with one of these numbers. However, do not use them for regular user accounts. By definition, root always has User ID 0, daemon has User ID 1, and pseudo-user bin has User ID 2.

   — When adding a user account, you must assign a primary group for a user or accept the default group, staff (group 10). The primary group should already exist (if it does not exist, specify the group by a GID number).

   For more information, see the Sun Solaris 8 System Administration Guide, Volume 1.

A user account other than root must me set up with an Avaya IR privilege of Administration or Operations in order to log in to Web Administration. The Operations privilege allows access to fewer Web Administration menu items than the Administration privilege. For example, a user with an Operations privilege cannot administer Backup and Restore.

To assign administrative privileges:

1. At the command prompt, type **assign_permissions *username* Administration** where *username* is the user you added using the admintool. Press **Enter**.

   The system displays:

   ```
   Assigning VIS permissions:      Administration
             for user login:      username
   ```

```
Confirm (Y/N)
```

2. Type **y** and press **Enter**.

   The system displays:

   ```
   login:  username has been assigned VIS permissions level:
   Administration
   ```

   You can now access the Web Administration interface using the new user name.

Starting the Web Administration interface

To set up the features on Avaya IR, you can use the Web Administration interface or the command-line interface.

Note:
Avaya recommends using the Web Administration interface until you are familiar with the administration commands.

To start the Web Administration interface:

1. Start a Web browser.

   To run Netscape locally on the Avaya IR platform, type **/usr/dt/bin/netscape &** at the command prompt and press **Enter**.

   If you are accessing Avaya IR from another computer, start the browser as you normally do on that system. This computer must be on the same data network as the Avaya IR system.

2. In the browser address field, type **http://*domain*** where *domain* is the domain name of the Avaya IR system and press **Enter**.

   The domain name is specified when the system is installed and set up for the first time.

   If you are running the browser locally, you can use **http://127.0.0.1** in the address field.

   The browser displays the **Web Administration entry** screen.

3. Click **Web Administration** from the menu.

   The browser displays the **Login** screen.

4. Log in to the system using an account with root or administration privileges.

   The browser displays the **Web Adminstration** screen, the entry point for the Web Administration interface.

Setting up features

Once packages have been installed, Avaya IR features must be configured to provide the required functionality. You use the Web Administration interface or the command-line interface to administer features on the Avaya IR system.

Common administration tasks in *Avaya IR System Help* provides step-by-step instructions for administering and setting up features.

To set up features:

1. Configure switch interfaces (such as T1/E1 or Voice over IP).
2. Configure JDBC interface for database access.
3. Configure Call Data Handling settings.
4. Configure UCID settings.
5. Configure speech features (such as PTTS, NLSR, or Avaya Recognizer), if required.
6. Configure CTI DIP settings, if required.
7. Configure the ASAI settings, if required.
8. Configure the fax settings, if required.
9. Configure the system for backups.

To access *Avaya IR System Help*, select **Help** in the Web Administration interface.

Installing database software

Database software is typically installed on the LAN or locally on the Avaya IR system. Follow the instructions given by your software provider for installing the database, keeping in mind the network port usage by the system on page 35.

Important:
Of the certified databases, only Oracle may be installed locally on the Avaya IR platform. When installing Oracle do *not* start the Oracle Apache Web Server. The Oracle Apache Web Server conflicts with the Apache Web Server that is installed as part of the Web administration package and is not required for using Oracle on Avaya IR.

Local Oracle configuration guidelines

Avaya recommends using a specific memory usage configuration for local installations of Oracle. The default configuration that is generated by the installation process causes Oracle to consume too much system memory.

The Avaya-provided **/vs/data/init.ora** file contains the recommended configuration for running Oracle on the Avaya IR system. Use this file in place of the default init.ora file (usually located in the **$ORACLE_HOME/dbs** directory) or modify the file using the following values as guidelines:

```
#db_cache_size=67108864
db_block_buffers=500
hash_area_size=262144
#dispatchers=       - disable MTS
#java_pool_size=67108864
#large_pool_size=1048576
shared_pool_size=5000000
```

Network port usage

The following table shows which network ports are used by features. If you are installing new software, be sure not to use any of these ports.

Feature	Network Ports	Protocol
Avaya Recognizer (WholeWord)	2345 to 2345+N-1 where N is the number of ASR ports. The default is 60.	TCP
Web Administration	80 for Apache Web Server, 8081 for Tomcat Servlet Engine	HTTP
Web Administration	8007 for Tomcat Servlet Engine	ajpv12

Working with service packs

Service packs are required to update the Avaya IR system with the most current software available.

Service packs are numbered in ascending order and each subsequent service pack contains the contents of all previous service packs. Also, each software release of the system contains the service packs from the previous software release. For example, release 2.0 contains all the service packs for release 1.0.

You need to install service packs in the following situations:

- After a system arrives from Avaya that does not have the service pack pre-installed.
- After a system has been installed from CD.
- After a system has been recovered using a full-backup image that did not have the service pack installed.
- After new features have been added and activated on a system. This is necessary to ensure service pack materials for the newly activated feature get installed, since the service pack package does not install fixes for features that are not present on the system.

In all of these situations, the basic process of working with service packs is

1. Determining the software release on page 37
2. Verifying the service pack on page 38
3. Obtaining service packs on page 39
4. Installing service packs on page 39

Determining the software release

To determine the current software release:

1. If necessary, log in as root.
2. At the command prompt, type **pkginfo -l AVvs** and press **Enter**.

   The system displays a message similar to the following:

```
PKGINST: AVvs
NAME: Runtime Processing Package
CATEGORY: IVR
ARCH: sparc.sun4u
```

```
VERSION: 1.0.026
VENDOR: Avaya Inc.
PSTAMP: mav220021112110202
INSTDATE: Nov 18 2002 11:59
STATUS: completely installed
FILES: 568 installed pathnames
28 shared pathnames
13 linked files
58 directories
150 executables
4 setuid/setgid executables
71869 blocks used (approx)
```

The first two numbers of the VERSION show the major release number, in this case 1.0.

Verifying the service packs

The service pack package is named after the release number, using the following naming convention:

AV*major-minor*qp

where *major* is the major release number and *minor* is the minor or point release number. For example, the name of the service pack package for release 1.0 is *AV1-0qp*. The service pack package for release 1.2 would be *AV1-2qp* and so on.

To check the service pack package for a given release:

1. If necessary, log in as root.
2. At the command prompt, type **pkginfo -l *sp_package*** and press **Enter** where *sp_package* is the name of the service pack for the release you want to check. The service pack is indicated in the following ways:

   — The system displays an error message, such as:

   ```
   ERROR: information for "sp_package" was not found
   ```

   In this case, make sure you used the correct name for the service pack package. If so, the error indicates that no service pack package has been loaded for the release.

   — The system displays package information. The version of the service pack is indicated at the end of the **VERSION** number. For example, VERSION number *1.0.26.003* indicates that the third service pack for version 1.0 is currently installed.

If this is not the service pack that should be on the system, use the **pkgrm** command to remove the package. To install the correct service pack package, you may need to download

it from the Avaya Support Centre Web site. See Obtaining service packs on page 39 for more information.

Obtaining service packs

If you installed the Avaya IR software from CD, the service pack package may already be loaded on your system.

To determine if you need to obtain a service pack, type **ls /export/patch** and press **Enter.** If the system displays a service pack file, you can install the package using the steps described in Installing service packs on page 39. If there is no service pack file, follow the steps below to obtain the file from Avaya.

To obtain a service pack:

1. From a Web browser, go to http://support.avaya.com.
2. From the navigation menu (the area on the left of the browser window, under **Technical Database**), select **Call Center/CRM**.
3. From the navigation menu, select **Interactive Voice Response**.
4. From the navigation menu, select **Interactive Response**.
5. From the main display area of the browser window, select **Software Downloads**.

   The browser displays a table listing the current software downloads.
6. In the **Software Downloads** table, click the link for the service pack you want to download.

   The browser displays information about the service pack, including instructions for downloading, installing, and uninstalling the service pack.
7. Follow the download instructions, to copy the service pack file from the Web site.

To install the service pack, see Installing service packs on page 39.

Installing service packs

To install a service pack:

1. If necessary, log in as root.
2. At the command prompt, type **cd /export/patch** to change to the directory containing the current service pack package (in compressed form).
3. Type **stop_vs** and press **Enter** to stop the voice system.

4. Type **uncompress *sp_package.ds.Z*** where *sp_package.ds.Z* is the name of the compressed service pack file in the /export/patch directory. Press **Enter.**

   The service pack uncompresses in the current directory.

5. Type **pkgadd -d ./*sp_package.ds sp_package*** where *sp_package.ds* is the name of the uncompressed service pack package and *sp_package* is the name of the service pack you want to install. Press **Enter.**

   For example, to install service pack **AV1-0qp**, type

   pgkadd -d ./AV1-0qp.ds AV1-0qp

   and press **Enter**.

   The package installation starts. The system displays various messages. In most cases, you must confirm these message by pressing **Enter** (to choose the default **Yes** response).

   Note:
   If you do not confirm the package installation messages, the process will exit and the package will not be installed.

   After a short time, the system displays a message indicating that the installation is complete. You must reboot your system for the changes to take effect.

6. Type **shutdown -y -i6 -g0** and press **Enter** to reboot your system.

Backing up the system for the first time

Avaya strongly recommends that you create a full backup of the system after you have completed administering the features for the first time. By doing so, you will preserve your setup and minimize the amount of work you will need to do if the system becomes disabled and has to be restored.

See Creating backups in the *Avaya IR System Help* for more information.

Restoring the system from backup

If a full backup of the Avaya IR system exists, the system can be completely restored without needing to install software from CD media or re-administration of features.

To restore the system from full backup:

Step	System prompt	Action
1.	—	Perform Steps 1 through 21 of Install system software on page 16. After Step 21, the system displays the following prompt:

2.	`Welcome To Avaya Interactive Response R1 Installation and Recovery.`
	`Please select one of the choices below.`
	`I to Install or R for Restore`
		Type **r** and press **Enter**, to begin restoring the system from backup.

3.	The system prompts you to make sure the LAN cable is plugged in before proceeding.	If necessary, see Connecting the platform to the LAN on page 11 for more information.

4.	`You will next have to enter the nfs pathname to the backup image.`
	`The format is backuphostip:/path/systemname.DddmmyyThh:mm:ss`
	`Where:`
	`backuphostip is the ip address of the system where the backup file is located.`
	`path is the pathname to the directory on the backuphost where backup file is located.`
	`systemname is the host name of the system that back up was created from.`
	`There should be two files on the backuphost: systemname.DddmmyyThh:mm:ss.full and systemname.DddmmyyThh:mm:ss.diskinfo.`
	`Enter the nfs pathname to the backup image now.`
		Type the NFS pathname to the backup file and press **Enter**.
		Caution: You must use the IP address of the system where the backup is located (*backuphostip*). If you use a URL instead, the restore operation will fail.
		The system extracts the data from the backup file, install the data, then reboots. This process takes several minutes.

5.	Configuring default router Set default network router IP address [y,n,?]	Type **y** the press **Enter**.
6.	Set Router IP Address (ex. 192.1.7.254):	Type the router IP address then press **Enter**.
7.	Is router address <192.1.7.254> correct [y,n,?]	Type **y** then press **Enter** if the router address is correct.
8.	On this screen you can create a root password. A root password can contain any number of characters, but only the first eight characters in the password are significant. (For example, if you create `a1b2c3d4e5f6' as your rootpassword, you can use `a1b2c3d4' to gain root access.) You will be prompted to type the root password twice; for security, the password will not be displayed on the screen as you type it. > If you do not want a root password, press RETURN twice. Root password:	Type the root password then press **Enter**.
9.	Press Return to continue.	Press **Enter**.
10.	Re-enter your root password.	Type the root password and press **Enter**.
11.	Press Return to continue.	Press **Enter**.
12.	System identification is completed. The system boots and displays the console login prompt.	Log in as you normally do. If incremental backups were made after the full backup, restore them using the Web Administration interface. For more information, see Creating and restoring backups in *Avaya IR System Help*.

Migration

This section defines the processes and tools needed to successfully migrate data from V 6.1, V7, V8, or R9 CONVERSANT platforms (MAP40, MAP40P, MAP100 or MAP100P) to the Avaya IR platform using a LAN connection.

The migration process is a one time process that occurs in three phases:

- **Pre-migration**. Evaluate existing applications to help plan migration activities.
- **Migration/update**. Perform actual migration or movement of data using automated and manual procedures.
- **Post-migration**. Verify the state of the migrated information and update migrated applications.

Note:
To ensure a complete migration, each phase must be completed successfully before proceeding to the next phase. Avaya technical services support customers through all phases of migration.

Migration overview

Pre-migration phase

The pre-migration phase includes the use of the evaluation tool (Scanit), resulting in a log of the evaluation results and a plan of action for each possible result. The evaluation does the following:

- Scans the customer's data, including the following:
  - Core Applications (Voice@Work, IVR Designer, Script Builder, IRAPI)
  - Data files and database tables
  - Utilities and tools
  - Pre-packaged speech files (EBS)
  - Grammar files
  - Custom external functions
  - Recorded speech (prompts)

  - — Call Data Handler (CDH) data (flat files and database tables)
  - — User logins
  - — Host screen files
- Identifies any features or commands on the pre-migration platform that are not supported on the Avaya IR platform and logs the results.
- Includes a plan of action for each item identified by the evaluation tool. The plan of action for unsupported features or commands varies based on the items identified by the evaluation tool.

These activities prepare the customer data for the migration to the targeted platform. For example:

- If speech files are found, they must be converted.
- If an application has unsupported features, (for example, Brook Trout external functions), manual intervention is required.

Unsupported features or commands identified by the Scanit tool can be addressed by:

- Manual changes made to the application
- Execution of a process to update the application
- Exclusion of the application from the data to be migrated to the Avaya IR platform.

After reviewing the action plans, the customer may update the applications to change or remove the unsupported features or may contact Avaya or their ISV to assist with this process.

Migration phase

The migration phase includes data conversion and data transport activities. Data must be transported between platforms using a LAN connection. Upgrade procedures and activities for pre-migration and migration occur on the originating platform.

Post-migration phase

In the post-migration phase, verify that migrated components have reached the targeted platform successfully, without any errors. Update custom speech files and migrated Voice@Work and IRAPI applications.

If a Script Builder application requires updates, update the application on the originating platform and then move it to the Avaya IR platform. The Script Builder development tool is not supported on the Avaya IR platform.

Avaya supplied Enhance Basic Speech (EBS), IRAPI commands, DIPs, TAS scripts, and standard external functions are not migrated because they are a part of the base Avaya IR software.

Unpacking the migration tools

The migration tools and all related files are delivered to the customer system as a **tar** file named **mavscan.tar**.

To unpack the tools on the CONVERSANT system to be scanned:

1. Copy the **mavscan.tar** file to a directory where the tool will run.
2. On the command line, enter **`tar -xvf`** to unpack the tool in the current working directory.

   Unpacking the tool populates the current directory with the scripts and supporting utilities needed to run the migration tools.

Pre-migration phase

The purpose of the pre-migration phase is to determine the scope of the migration (the data and application changes that will be moved from a current CONVERSANT platform to Avaya IR). The pre-migration scripts, including the Scanit tool, are packaged together in a pre-migration package. You install and execute the pre-migration package on the source CONVERSANT system.

Pre-migration scanning tool (Scanit)

Scanit is the primary data gathering tool used to quantify the data and applications on source CONVERSANT platform. The log files from Scanit are a primary input to determining the work effort involved in the migration to an Avaya IR platform. Actual effort estimates require analysis of the log files created from the pre-migration tool and are expected to be made by an experienced development organization such as an ISV or Avaya professional services.

Note:
Scanit should not be confused with the existing SCAN tool that is run by Avaya services. The existing SCAN tool captures an entire CONVERSANT configuration (boards, RTU licenses, etc). Scanit is dedicated to applications and data and complements the existing SCAN tool.

Scanit looks at application source files for occurrences of code that are out of compliance with the new Avaya IR release. These occurrences are referred to as tokens. The Scanit tool allows the user to configure the extensions for which to scan. The default extension types are:

- **.c** for C source files including IRAPI and header files
- **.sh** for shell files, including Oracle SQL commands
- **.t** for TAS scripts and external functions
- **.prg** for Script Builder program files

Scanit searches for files from a root directory by the above extensions. It searches in one pass starting from the specified root directory and continuing downward into all subordinate subdirectories for all source files.

In addition to searching for files by extension type, Scanit can also be configured to specifically look at particular files, regardless of extension type. The input list of files can be a set of files residing anywhere on the system. The user-supplied file list provides an option for the user to specify an explicit *file type* for each file. This allows the user the flexibility to input files to the tool that may not be readily identifiable by their extension type, and therefore would not be found in a standard search.

An example of an unsupported token would be **IRD_FLEXWORD**, which is a value supplied to the irSettParams functions in IRAPI. If this token is found in a source file on a system being migrated to the Avaya IR system, the tool flags the parameter, identifies the file and line number, and logs this information into the log file.

Scanit generates a report identifying where unsupported tokens are found in the customer source code. The tool also provides a set of summary reports which include a list of files with specific token locations and total summaries of individual tokens found.

Scanit provides the ability to assign a weighted value for each token type. This weighted value, is used to symbolize the complexity of the work required to replace the token. The complexity values may be used to determine hours of work. As with all other parameters in the scanning tool these values can be edited and changed in a configuration file.

Data and speech scanning tool

The following describes how the data and speech scanning tool evaluates recorded speech and Oracle data:

- **Recorded Speech**. The data and speech scanning tool discovers and classifies all speech files, by type (ADPCM16, ADPCM32, CELP, etc.), starting from a root directory provided by the user. It builds a log file of all recorded speech files and their types, and totals their sizes to get an estimate of the amount of data to migrate.

  Compound speech files, where multiple types are concatenated into one file, are not flagged and identified as compound by the scanning tool.

  Note:
  Actual speech conversion does not take place in this phase.

- **Oracle Data**. The data and speech scanning tool finds data files located under a user-specified root directory. They are summed into the total data count to get an estimate on the amount of data to migrate. This summary is included in the log file.

Running the Scanit tool

Scanit, is the interactive script that leads the user through the scanning process. Scanit's main purpose is to scan for tokens in the application source. The tool is designed to scan the source code of custom user-written applications and look for things not supported in Avaya IR.

Scanit does not take any command line parameters. It prompts interactively for the user to enter a directory from which to search for source files. It also allows the user to supply an input file (described below). The user must provide an input file or directory to search to proceed.

Setting up an input file for Scanit

The following example shows the format of an input file for the Scanit tool. The input file includes a list of specific files the tool should scan.

```
TYPE t
/test/your.t
/tools/my.t
TYPE c
/tools/test/my.c
TYPE sh
/tools/test/hirunner
```

Note:
You must list all files of the same type after the TYPE declaration, valid types are c, t, sh, nam, and prg. These types correspond to C source/IRAPI, TAS, shell, screen capture, and Script Builder program file, respectively.

Listing specific files has an advantage over searching directories for files in that the tool is explicitly told each file's type. With the directory search option, the tool can only determine the file type through the file extension. For example, if the tool is given only a directory to search and this directory contains extensionless shell files, those shell files without the *.sh* extension, will not be discovered and will be ignored by the tool. If the specific shell files are listed in an input file, the shell files will be examined by the tool.

Running the Scanit tool

1. Type **`scanit`** at the command prompt to start the tool.

   Make sure you are in the directory where the tool was loaded.

Note:
The tool outputs a large amount of information that can scroll by quickly. To capture the output in a file for future reference, use the **tee** or **script** utilities to capture the output. (For example, **|tee *file_name***)

The system responds with:

```
Scan Script Builder applications on this system?
[y or n, default y]
```

2. Press **Enter** to accept the default.

   Accepting the default causes the tool to find all the Script Builder program files to be scanned.

   The system displays the following prompt:

   ```
   Enter file name of source file list.
   <h for help, or CR to continue>
   ```

3. Enter the name of the input file that specifies the files to be scanned.

   You can enter a file of files to scan. As the tool reads these files, it checks to see if the listed source files exist. It then captures the list of files to scan and displays the following prompt:

   ```
   You may also enter directories to search.
   You will be reprompted for each directory

   Enter a directory name
   <h for help, or CR to continue>
   ```

4. Enter the name of the directory where the scan should begin.

   The response to this prompt should be the root directory of the application path. You do not need to supply a directory if all of the applications to be scanned are specified in the input file.

   This prompt repeats after the system searches for files in the given directory and sub directories. You can scan additional source trees if all applications are not in the same directory tree.

5. Enter more directories, or press **Enter** to continue.

   The system displays the following message:

   ```
   The following source files will be scanned
   press return to continue

   [List of files found ……]

   Press return to begin scanning.
   ```

   The tool displays a summary of all the files to be scanned. This is the list of files discovered as a result of all the previous queries.

6. Press **Enter**.

   The tool displays a series of processing messages, as it begins scanning. When the scanning process is complete it displays the following message.

   ```
   Application scanning now complete.
   Results can be found in the directory /current_directory/results
   ```

7. Press **Enter**.

   The results of the application scanning are put into a **results** directory created from the current working directory where the tool is running.

Scanning Results

The Scanit tool creates a directory named **results** with the following log information:

- **source_outages.timestamp.*file_type***

  For every source file type (c, h, sh, t, nam, and prg), the scanning tool lists the files where obsolete tokens were found. The file has the following form:

  ```
  /vs/examples/IRAPI/util_fcns.c
   token name vsprintf found at line 79     vsprintf(mbuf, fmt, args);
   token name getpid found at line 148     srand(getpid());
   token name srand found at line 148     srand(getpid());
   token name rand found at line 401     reg[1] = rand();
   token name ctime found at line 463     strcpy(tbuf,
  ctime(&reg[1]));
   token name ctime found at line 466     irQTraceP(chan, TEE, TAREA,
  vfmtstr( "%s: ctime = %s", fnName, tbuf ));
  /vs/examples/IRAPI/test.c
   token name signal found at line 22 #include <signal.h>
   token name printf found at line 56 if (sgno == SIGTERM) {
  printf("caught sigterm \n"); }
  ```

- **tokensummary.timestamp.*file_type***

For every source file type (c, h, sh, t, nam, and prg), the scanning tool creates a summary file of the following form:

```
Token Name            Occurrences      Rate      Cost
I_ENOOP                     1          2          2
ctime                       2          0          0
exit                       23          1         23
fprintf                    90          1         90
getpid                      1          0          0
printf                      5          1          5
rand                        1          0          0
send                        1          5          5
srand                       1          0          0
vsprintf                    1          5          5
irFlash                     1          1          1
-------------------------------------------------------------
Totals                    127                   131
```

The **Rate** field is an educated guess at how much work will be involved in fixing the application. The **Cost** field is the number of **occurrences** times the **Rate**.

- **token_information.*file_type***

  This is a static file, copied into the results area when the tool is installed. It gives a short textual explanation for every token and describes the Avaya IR issue.

- **speechlog.*timestamp***

  This file contains a listing of all converted speech files, their type prior to conversion (ADPCM16 or ADPCM32), and the number of bytes created by the conversion.

Customizing Scanit

Scanit can be customized by adding tokens to the existing types or by adding new token types.

Adding tokens

Every token type has a file that lists all the tokens for which to scan. The default token files delivered with the tool are:

- **tokens_c** for IRAPI and C language tokens
- **tokens_t** for TAS language and external function tokens
- **tokens_sh** for anything that can appear in a shell script
- **tokens_prg** for Script Builder text files before they are converted into .t files

To add a new token for which to scan:

1. Add a new line with the new token to the end of the file corresponding to its type.

For example, if IRAPI function **irFPlay** were found to have a problem, and needed to be flagged by the scanning tool, you would update the **tokens_c** file (IRAPI calls are found in C programs). The format of **tokens_c** files is a simple three column file that has the following format:

`NAME: token weight`

where NAME is fixed text and *token* and *weight* must be provided.

2. Update the **token_information** file (the file that contains a problem description for every token) for that file type.

Note:
When adding new tokens do not leave any blank lines at the bottom of the **token_*type*** file.

Adding new types of tokens

To add a new type:

1. Identify a new type identifier.

   For example, if you needed to scan java source files, **java** might be a logical new type identifier.

2. Add the new type to the ext_type file in the installed tool directory.
3. Create a **tokens_*new type*** file, and populate it with tokens.

   Use the same format as the other token type files.

4. Create a **token_information.*type*** file with resolutions and descriptions for each new token in the **tokens_*new type*** file.

Migration phase

The migration package prepares data for migration and migrates the data to the new platform. The migration scripts are packaged together in a migration package that is installed and executed on the source CONVERSANT system.

Migrating data

Archiving data to prepare for the move

The **tar_it** utility is delivered with the migration scanning tools to assist with the movement of custom files and data to the target Avaya IR platform. To archive files:

1. Run **`tar_it`** from the command prompt.

The tool prompts for a default file containing a listing of directories and files to be put into a tar archive.

Note:
To capture a list of the files being archived, substitute the command **tar_it | tee *file_name***.

2. Press **Enter** to use the default directories.

   If you choose the default the following directories are used:

   /att/trans/sb
   /vs/bin/ag/lib
   /speech/talk
   /user/add-on

   The tool displays the directories to be archived and asks for confirmation prior to creating the archive.

3. Press **Enter** to confirm.

   The tool lists all files discovered and puts them into an archive. As files are added they are displayed rapidly on the screen.

   When all files are archived the tool responds with the following message:

   `You may now transfer` **/voice1/*file_identifier*.tar** `to target machine. Execute` **tar –xvf *file_identifier*.tar** `to unpack on the target machine. Please note there is no protection from overwriting existing files.`

4. Transfer the files across the network using an **ftp** command of the archive from one system to the other.

   If you need to move individual files, an NFS mount between platforms might be more appropriate. For instructions on setting up NFS, see File sharing with Solaris Systems on page 54.

5. Run the command **tar -xvf *file_identifier*.tar** on the target platform to copy all the files in the archive onto the target system.

   The system creates new directories if needed, and overwrites files on the target system if they are duplicated in the archive.

File sharing with Solaris Systems

The following set of commands can be used to set up file sharing between legacy SCO platforms and Solaris platforms.

1. On the Solaris platform, enter the following command:

   share -F nfs /cat share -F nfs /export >> /etc/dfs/dfstab

   The system responds with the following messages:

```
etc/init.d/etc/init.d/nfs.server stop
/etc/init.d/nfs.server start
```

2. Enter the following command:

   share -F nfs /

3. Mount the Solaris shared directory from the legacy platform.
4. After files are moved, run **unshare**.

Migrating speech files

The Avaya IR platform supports only the G.711 protocol for speech files. To support this, the migration process converts currently supported speech formats on CONVERSANT platforms to PCM64 which follows the G.711 protocol. The G.711 protocol is the international standard for encoding telephone audio on a 64 kbps channel. It is an ITU-T compliant, pulse code modulation (PCM) scheme operating at a 8 kHz sample rate, with 8 bits per sample.

Avaya pre-recorded speech packages have been converted and ported into the Avaya IR base software. They are not part of the migration process.

To migrate speech files to the Avaya IR platform:

1. Ensure that the source ADPCM speech files are placed on a CONVERSANT system.
2. On the CONVERSANT system, run

   /mtce/bin/vis2wav -l –e 16 1036 1036.wav

   Where /mtce/bin/vis2wav is a standard utility found on all V8 systems, 1036 is the source ADPCM CONVERSANT speech file, and 1036.wav is an intermediate file created as output from the **vis2wav**.

3. Transfer or ftp the intermediate **1036.wav** file to the new Avaya IR platform that is loaded with NMS software and utilities.
4. On the Avaya IR platform, run

   vcecopy 1036.wav temp.wav -c10

   Where *1036.wav* is the intermediate file generated on the V8 platform, *temp.wav* is output from the **vcecopy** command and is in final G.711 format suitable for the Avaya IR system.

   Note:
   The **vcecopy** command keys off the **.wav** extensions so make sure to include this file extension.

5. Remove the **.wav** extension from the file name and rename the file back to its original name or a new name.

Migrating host screen files

The Avaya IR platform supports host screen files. During the migration phase, you move all **.sc** and **.nam** supported host screen files from CONVERSANT platforms to the Avaya IR platform. After you transfer the files to the Avaya IR platform, you run a conversion file to correct a byte ordering difference between the Conversant and the Avaya IR platforms. Additional information regarding this change is located in the Host documentation provided by Cleo Communications.

To migrate host screen files to the Avaya IR platform:

1. Transfer or ftp the **.sc** files and **.nam** files located in the **/lt/trans/sc/host_sc/appl.nam** directory to the Avaya IR platform.
2. Place the transferred files in the **/vs/data/host** directory.
3. On the Avaya IR system, run **`cleo_conv`**. This program updates the .sc and .nam files.

Post-migration phase

The post-migration process involves validating and updating data and applications that were migrated to the Avaya IR platform.

The bulk of post-migration work includes:

- Updating custom speech files
- Compiling, debugging, and fixing applications
- Designing and implementing workarounds for obsolete features
- Resolving database connectivity issues
- Testing applications

Most of these tasks cannot readily be automated or even captured in a repeatable process. This phase of migration involves mostly custom work, which can be performed by Avaya professional services, an ISV, or the customer.

Converting custom speech

Speech conversion to G.711 takes place after all the speech files are moved and located on the Avaya IR platform as described in the Migrating speech files on page 55 topic. An automated speech conversion tool (**do_speech**) locates the speech files that were moved and partially converted during the migration phase, and completes the conversion to G.711 format. The tool determines the location of the speech files, using a log file placed on the Avaya IR system during the migration phase.

The speech conversion tool generates a report on converted files, and reports any errors.

To convert the speech files:

1. Transfer the **do_speech** utility, provided with the migration scanning tool, to the target Avaya IR system.

   The do_speech utility is located in the same directory where the migration tools were installed on the source system.

2. Run the command: **do_speech**.

   The do_speech utility prompts for a directory where the speech files are located.

3. Enter the directory where the speech files are located.

   When it is done running, the utility creates a log file in the current directory (for example, **speechlog.06-19-02:133205).**

   The log file contains data in the following format:

   ```
   TYPE: pcm64 File Name: /voice1/vfs/talkfiles/619/41 Bytes: 31304
   TYPE: pcm64 File Name: /voice1/vfs/talkfiles/619/42 Bytes: 40512
   TYPE: pcm64 File Name: /voice1/vfs/talkfiles/619/43 Bytes: 29760
   TYPE: pcm64 File Name: /voice1/vfs/talkfiles/619/44 Bytes: 34368
   TYPE: pcm64 File Name: /voice1/vfs/talkfiles/619/45 Bytes: 26184
   TYPE: pcm64 File Name: /voice1/vfs/talkfiles/619/46 Bytes: 25672
   TYPE: pcm64 File Name: /voice1/vfs/talkfiles/619/47 Bytes: 28232
   TYPE: pcm64 File Name: /voice1/vfs/talkfiles/619/48 Bytes: 88168
   TYPE: pcm64 File Name: /voice1/vfs/talkfiles/619/49 Bytes: 13368
   Total Bytes Converted = 4192200
   ```

   Every converted file is reported and logged. The utility overwrites the legacy Conversant ADPCM files with Avaya IR G7.11 format.

   Note:
   Non-speech files are generally ignored, but it is good practice to make sure that only custom legacy speech files are in the directory.

Migrating applications

You can migrate Script Builder or IVR Designer applications as follows:

Script Builder

Script Builder applications from CONVERSANT systems can be migrated to Avaya IR systems.

To migrate Script Builder applications to the Avaya IR system:

1. Transfer (ftp) the applications from the source CONVERSANT system to the target Avaya IR system.
2. Run the **Script Builder Install** script to compile the application.
3. Execute the Script Builder application.

   Modifications to the Script Builder applications must be made while they are located on the CONVERSANT system. Script Builder applications can be executed but not modified on the Avaya IR system.

The **vesp_dip.t** external function no longer requires applications to define the **vespbuf** variable that was required in previous Script Builder applications. For this reason, the following steps must be performed for Script Builder applications that are currently running on the Avaya IR system using the **vesp_dip.t** external function and the **vespbuf** variable:

1. Transfer (ftp) the **vesp_dip.t** external function from the **vs/bin/ag/lib** directory on the Avaya IR system to the **vs/bin/ag/lib** directory on the V8 or R9 CONVERSANT system. If this directory does not exist, it must be created.
2. Transfer (ftp) the **vesp_dip.h** and **vespdipi.h** header files from the **vs/bin/ag/lib/dip** directory on the Avaya IR system to the **vs/bin/ag/lib/dip** directory on the V8 or R9 CONVERSANT system. If this directory does not exist, it must be created.
3. Run **`verify`** ***`application name`*** on the V8 or R9 CONVERSANT system.
4. Transfer (ftp) the application to the Avaya IR system.
5. Run **`/vs/bin/ag/install`** ***`application name`*** on the Avaya IR system.

IVR Designer

Voice@Work or IVR Designer applications from CONVERSANT systems can be migrated to Avaya IR systems.

To update applications to IVR Designer and migrate them to the Avaya IR platform:

1. Download the IVR Designer software to the PC.
2. Open the R4.x application to be migrated.

   The software automatically updates the application.
3. Compile the application using the **Code Generation** process. Select the Avaya IR platform as the target platform.

   This compiles the application to execute on the Avaya IR platform.
4. Transfer the updated application to the target Avaya IR platform by completing the following steps:

   a) Select **Application Transfer**.

b) Set the Application Transfer options to identify the type of transfer and the correct target platform.

c) Select the files to move to the target platform and click **Transfer**.

5. Install the application on the target Avaya IR platform and assign the application to a channel or channels.

   The application now resides on the Avaya IR platform.

Migrating host interface screen capture files

When you migrate an existing IVR Designer, Voice@Work, or Script Builder application that uses the Cleo host interface, to the Avaya IR platform, you must convert the screen capture files for the application before they can be used within the Avaya IR environment.

This conversion is required before the host application is used on the Avaya IR platform by any of the following programs:

- IVR Designer
- Cleo **screen_capture** utility for capturing host screens on the Avaya IR system
- Cleo **hispy** utility that provides interactive navigation and screen capture of IVR Designer or Script Builder host screens on the Avaya IR platform

Running the conversion utility

To run the Conversion utility:

1. Run the following command at the command prompt:

   cleo_conv *application*

   where *application* is the name of the IVR Designer or Script Builder application.

   The **cleo_conv** utility creates the following files:

   IVR Designer files:

/vs/data/host/appl.sc	V8 formatted screen capture file
/vs/data/host/appl.nam	V8 formatted screen capture name file
/vs/data/host/appl.sc.mav	Avaya IR formatted screen capture file
/vs/data/host/appl.nam.mav	Avaya IR formatted screen capture name file
/vs/data/host/appl.sc.org	Original screen capture file
/vs/data/host/appl.nam.org	Original screen capture name file

   Script Builder files:

/att/trans/sb/appl/appl.sc	V8 formatted screen capture file
/att/trans/sb/appl/appl.sc.mav	Avaya IR formatted screen capture file
/att/trans/sb/appl/appl.sc.org	Original screen capture file

Note:
The **appl.sc** and **appl.nam** files are converted to V8 format on the Avaya IR system, even if they are being migrated from a V6 or V7 system.

Returning files to original version

Cleo also provides the utility **cleo_convback** to return screen capture files that have been updated or created on an Avaya IR system, back to their original V6, V7, or V8 system.

To return screen capture files to V6, V7, or V8 format:

1. Use the following command at the command prompt:

   cleo_convback *`application n`*

   where *application* is the name of the IVR Designer or Script Builder application and *n* is the destination CONVERSANT system version (6, 7, or 8)

   The **cleo_convback** utility converts the current Avaya IR capture files and creates the following files:

   IVR Designer files:

/vs/data/host/appl.sc.V*n*	V*n* (where n is 6, 7, or 8) formatted screen capture file
/vs/data/host/appl.nam.V*n*	V*n* (where n is 6, 7, or 8) formatted screen capture name file

   Script Builder files:

/att/trans/sb/appl/appl.sc.V*n*	V*n* (where n is 6, 7, or 8) formatted screen capture file

Using other Cleo utilities

Once you migrate screen capture files from an existing CONVERSANT platform (V6, V7, or V8) and convert them with the **cleo_conv** utility, the Cleo **screen_capture** and **hispy** utility programs use the Avaya IR formatted files (suffix of .sc).

These Cleo utilities also update the V8 formatted screen capture files (no suffix), whenever a change is made to the Avaya IR formatted files. IVR Designer always has access to the latest screen capture files on the Avaya IR platform.

When you use the Cleo **screen_capture** utility to create new screen capture files or update screen capture files on the Avaya IR platform, the screen capture files have the **.sc** suffix.

The Cleo **screen_capture** utility creates or updates the V8 formatted screen capture files (no suffix) when it exits, so the IVR Designer system has access to the latest screen capture files in the V8 format.

Troubleshooting

Troubleshooting an IR system can be a complex process. The purpose of this section is to provide basic troubleshooting information for customers and for Avaya support representatives who are new to the platform.

The Maintenance section of this online help system describes actions customers can take to keep their IR systems running optimally, and provides detailed information on how Avaya supports maintenance and troubleshooting activities.

Troubleshooting overview

This section explains the requirements for successful operation of the IR system and identifies potential problem areas.

Requirements for successful operations

Interactions between the IR system and other systems and applications can become complex. Understanding the requirements for successful operations helps you to prevent problems and identify them more quickly when they occur.

MultiVantage systems

IR systems may be linked to MultiVantage (DEFINITY) systems that route calls to and from the IR system and perform call handling functions. For successful operations, the MultiVantage system must be free of hardware problems and administered correctly. Additionally, connections between the MultiVantage system and the IR system must be operating properly and free from overload.

The public switched telephone network (PSTN)

Calls come into the IR system from the public switched telephone network (PSTN). Telephony connections may go first to a MultiVantage (DEFINITY) system, or directly to the IR system. For successful voice response operations, these lines, and the telephony network that supports them – including central offices – must be working and free from errors.

Voice response applications

Voice response applications manage the interactions between callers and play the information that callers hear. For successful operations, voice response applications must perform a variety of tasks, such as:

- Interpreting caller input and taking appropriate action
- Communicating with hosts, databases, and proxy speech servers
- Transferring values entered by callers to other applications
- Providing information to callers in the form of recorded speech or speech generated through the Proxy Text-to-Speech feature

As you can see, voice response applications are central to the successful operation of an IR system.

Speech

The IR system provides information to callers through recorded or generated speech. For successful operations:

- Recorded speech must exist, be of acceptable quality, and be accessible to voice response applications.
- Generated speech must be constructed properly by the Proxy Text-to-Speech feature and the voice response application.
- Recorded speech must be transferred from a server, so that the application can play it for the caller.

Communcations between the IR system and the server or host must be adequate to deliver speech in a timely manner.

Connections and communications

Connections to other systems, and the communications that take place across them, are critical to smooth voice operations. Major connections and communications are as follows:

- Lines, PBXs, and other connections that bring calls in from and send calls out to the public switched telephone network (PSTN)
- Connections between any MultiVantage systems and the IR system
- Connections from the back of the IR system to other devices, and to the LAN
- LAN connections between the IR system and servers that provide speech functions, database information, or both

A breakdown in any of these connections can affect voice response operations.

System and LAN capacity

Like any computer, the IR system has a certain amount of memory, drive space, and CPU capacity to support system operations. Additionally, the IR system requires LAN capacity to communicate with servers that provide critical functions. For successful operations, both IR system capacity and LAN capacity must be adequate. Managing IR system performance explains how to check system and LAN resources.

How things go wrong

The IR system is complex. Avaya support representatives who are experienced with this and previous releases find that there is no list of typical problems. However, understanding the ways in which things can go wrong helps you to direct your troubleshooting efforts.

Hardware malfunctions and failures

Hardware malfunctions and failures may stop or interfere with voice operations. These include problems in:

- The IR system itself
- Servers providing speech functions, database information, or both
- Connected MultiVantage (DEFINITY) systems

Hardware malfunctions and failures are not difficult to identify, but they are not a top cause of problems, either.

Incorrect system administration

Errors in IR system administration may cause problems with voice operations. For example, a service may not be assigned to a channel, or TCIP connections between the IR system and a server may be set up incorrectly.

Application errors

Voice response applications manage voice response functions, so errors can be devastating to operations. For instance, an application may call for the playing of recorded speech that does not exist, or try to access the wrong server for speech. Applications that are not sufficiently tested, or not tested under realistic conditions, can cause problems. Voice response applications that are large and complex, or are inefficient, are the most common cause of performance problems.

Connection and communication problems

When any connection that supports voice response applications experiences a problem, operations may be affected. Disruptions may occur in the public switched telephone network (PSTN), MultiVantage (DEFINITY) system, servers that support operations, or in the LAN.

Overloading

Overloading may occur in these ways:

- The IR system may become overloaded by large, complex, or inefficient applications or by excessive external processes. The result of such overloading is performance problems. See Managing IR system performance for more information on reducing load.
- LAN overloading may result from competition with other processes for LAN capacity. The result can be delays and breaks in the availability of required data and functions.

If the call load increases beyond the capacity of the IR system, call handling problems are likely to crop up. A new system, or re-routing of calls, is generally required.

Troubleshooting guidelines

There is no standard troubleshooting process. With experience, individuals develop their own style and approaches. The guidelines presented here identify key actions and areas of information related to the IR system.

Checking IR system information

When problems appear, you can check on system operations and events in a variety of ways. If you check on system operations regularly, you are much more likely to spot problems before they become serious.

Display Equipment screen

The Display Equipment screen lists the NMS or VoIP card or cards, the services and numbers assigned to them, and their service state. The following table shows state descriptions and their meanings.

State	Meanings
INSERV	In service
MANOOS	Manually out of service
FOOS	Forced out of service
BROKEN	Not functioning, possibly needing replacement

System monitoring

The sysmon command provides a live display of system operations. It shows channel activity and conditions, as well as caller input.

Message Log report

The Message Log report lists messages, alarms, and errors. The type and time of the event are identified, and you can see explanations by highlighting an entry and requesting more information.

For more information, see the following topics:

- Effective IR system monitoring explains how to customize the tracking of events and alarms for your organization
- Monitoring the system contains a brief example of checking system operations

Reviewing the IR system history

Researching the history of your IR system helps you to identify the current problem. Find out about:

- Previous problems and support calls
- Recent changes to the system, including upgrades and repairs
- Changes to the LAN setup in your organization
- Previous intermittent problems that may indicate a pattern

Using troubleshooting tools

You can use a variety of troubleshooting tools to learn more about a problem. You may do this on your own, or under the direction of an Avaya support representative.

IR system configuration information

Checking system information on page 69 explains how the **Message Log** report, **Display Equipment** screen, and **sysmon** command contain information about the IR system configuration and processes. Execute administrative commands to receive more detailed information, such as:

- The allocation of resources for all devices
- Resources and space available in the database
- Feature packages installed on your IR system
- A report of all active fax jobs

Command line commands lists and defines all administrative commands.

IR system commands

Use administrative commands to check IR system components and processes. Since the Solaris operating system is UNIX-based, you also can run UNIX commands that check devices, processes, and files.

Sun diagnostic tests

Three types of diagnostic tests are available through Sun applications. Use the Sun:

- Validation Test System (VTS) to test and validate major hardware components.
- OpenBoot Diagnostics system to perform root cause failure analysis on various IR devices.
- PROM Diagnostics to check system processes, such as the error rate and type for Ethernet packets

The *Sun Blade Service Manual* explains how to run these diagnostic tests.

Identifying possible causes of problems

Generally, you will work with Avaya support representatives to identify the cause of the problem and correct it. However, you may find that some problems are easy to identify and resolve on your own.

The following table describes some of these problems and suggests actions you can take to identify them:

Problems	Description	Suggested action
Cable issues	Disconnection or poor connection of cables to the back of the IR system	Check the cable connections. Checking cable connections on page 87 explains the location and function of these cables.
Feature licensing problems	Problems include: expired licensing, incorrect assumptions about features licensed, or, renaming of the IR system that may cause loss of feature licensing	Determine the features you can use. The Feature Licensing screen identifies the features you are entitled to use.
Changes to or problems with your organization's LAN system	These may result in poor communications or no communication with required servers.	Check with your LAN administrator if you suspect problems in this area.
Incorrect system administration	If changes were made recently, there may be errors in channel assignments, server assignments, and other such configuration information.	System administration errors may degrade or stop the affected voice response services.

Inadequate system resources	If your IR system is experiencing delays and speech breaks, it may be overloaded.	Managing IR system performance explains how to check the load on your system and how to reduce load.
Voice response application errors	If new applications were recently implemented, or existing applications were revised, there may be problems with the code. Additionally, large, complex voice response applications may affect system resources.	Modifying voice response applications lists key guidelines for making applications efficient. If you suspect application problems, contact the vendor or internal staff who develop your applications.

Investigating operations problems

Problems central to voice response functions can affect business operations and may result in missed calls and caller frustration. Most of the problems described in this section require prompt attention. To investigate these problems, you should have a good understanding of the Requirements for successful operations on page 65.

Investigating call handling problems

Call handling problems include issues related to responding to and transferring calls, both voice calls and faxes.

Voice system not answering

The voice system will not take calls. The voice system rings but does not answer, or the voice system is busy.

Note:
If host interaction is involved, refer to Host interaction not working right on page 75.

Investigating the problem

To check on possible causes of the problem:

1. Do either of the following:

   — Enter **display card all** and press **Enter**.

   — Go to the **Display Equipment** screen to check the status of cards.

   All NMS cards should be in the in service (INSERV) state.

2. If cards are not in service, you may try to restore them or contact your Avaya support representative.

   See Restoring cards and channels on page 89 for procedures that may bring cards back into service.

3. Make sure PLAY/CODE, TTS, or both, are assigned to an INSERV NMS card.

4. Make sure that the voice response application is properly assigned to the channel or channels.

5. Make sure the voice response application contains an action to answer the phone.

6. Check the **Message Log** report for messages indicating that Transaction State Machine process (TSM) is respawning because there are too many channels in the system.
7. If TSM is respawning, change NCHANNELS and NCALLS.

Changing NCHANNELS and NCALLS, if necessary.

To tune the NCHANNELS parameter:

1. Use **/etc/conf/bin/idtune NCHANNELS value** to increase the NCHANNELS tunable parameter to the value you require.

   The maximum value of NCHANNELS is 448.
2. To rebuild the kernel, type **/etc/conf/bin/idbuild -B** and press **Enter**.
3. Reboot the system.

To set NCALLS:

1. Execute **/etc/conf/bin/idtune NCALLS 400**
2. To rebuild the kernel, type **/etc/conf/bin/idbuild -B** and press **Enter**.
3. Reboot the system.

Calls dropped

Calls dropped at initial prompt

The IR system may drop calls when the initial prompt is playing if the prompt was recorded over background noise, such as a fan or ventilation system. The background noise may be detected as dial tone following disconnection by the caller. If this happens, the call is dropped by the IR system. To fix the problem, re-record the prompt without the background noise.

All calls dropped

Take these actions when all calls are dropped:

Note:
If host interaction is involved, refer to Host interaction not working right on page 75.

1. Scan the **Message Log** report for messages related to the trouble.
2. Type **who -rpb** and press **Enter**.
3. Search for different time stamps on the processes.

   A recent date different from most of the others may indicate the process respawned.

4. If you find different time stamps, record the situation that caused the problem.

Calls not transferred properly

To check and correct dialed digits:

1. Use the **sysmon command**.
2. Observe transfer operations to determine if the correct digits are being dialed.
3. If the wrong digits are being dialed, make the required correction in the voice response application.

Touchtone not interpreted correctly

If touchtone is not working properly:

- Verify that the action to collect data from the caller matches the intended use in the voice response application.
- If the problem only appears on a particular channel and you have another NMS card, determine whether the problem occurs on the other NMS card. If the problem does not occur on the other NMS card, contact your Avaya support representative for assistance.

Host interaction not working right

Host sessions recover repeatedly

1. Check the **Message Log** report for messages related to the trouble.

   Alarms related to host interaction begin with the letters **HOST**, and range in severity from **none** to **critical**.
2. Make sure that a **Transaction Base** screen has been specified.
3. Make sure the Login and Recovery sequences both leave the host session at a Transaction Base screen.

Ring no answer for application with host interface

1. Check the Message Log report for messages related to the trouble.
2. Check the host timeout value and verify that the host response time is not exceeded.

All calls dropped

To check the status of the host, type **hstatus all** and press **Enter**. If all sessions are recovering or logging in, this could explain the trouble.

Speeding up connections between the IR system and the host may resolve host interaction problems.

Investigating fax problems

When you investigate fax problems, you will find it helpful to know what usually goes wrong and what type of information about fax operations the Avaya IR system provides.

Typical fax problems

The most common reasons that a fax is not sent are:

- The remote fax machine is busy or out of paper.
- There is no fax machine at the remote number.

Once you have checked these two possibilities, troubleshoot fax problems using the procedures that follow.

Locating fax errors

For internal errors:

- Check the **Message Log** report for FAX001 and FAX002 *or*
- Type **trace FAXOOC sbFaxProc chan all area all level all** and press **Enter**. Provide output to technical support.

You may also learn of errors through negative return values on a FAX action. Refer to Interpreting negative fax values on page 77 for explanations of negative errors

Reviewing fax troubleshooting procedures

When problems arise with fax operations, the Message Log report may display various error messages. The help topics for these messages include suggested repair procedures.

- See information on FAX alarms for repair procedures to use when the fax print or the fax operation fails.
- FXMON alarms and messages report FAX maintenance events.
- VXMDI alarms and log messages report problems with fax operations.
- If you are using an Audix system, also check FAX AUDIX alarms and errors.

Execute UNIX command failed

Most likely, the problem is with the command or shell script. Make sure that the command or shell script that was attempted works when executed manually. If it does, make sure that its full path name is provided to the script.

Fax file or text file not found

Take action depending on whether the problem occurred in transmission or receipt of the fax:

- If the request to *transmit* a fax file to the caller failed, verify that the fax file exists either in the **Fax Loading and Printing** screen or at the full path specified in the voice response application.
- The caller did not *receive* the fax requested, consider manually transmitting the fax message requested by the caller using the delivery number contained in the error message.

Out-of-call fax transmission failed

You learn of this problem through the fax report. Follow the repair procedure provided for the FAX001 message.

Interpreting negative fax values

When a negative return value of a FAX action indicates that an error has occurred, use the following list of return values to determine the cause of the error. These values are found in the **fax_tool.h** file.

Value	Meaning
-1	Another **faxit** command is executing.
-2	Fax transmission failed (internal).
-3	Channel was denied (internal).
-4	File cannot be opened or does not exist
-5	There are no previous queued faxes.
-6	No background file was found (obsolete).
-7	No foreground file was found (obsolete).
-8	**faxit** command timed out (internal).
-9	File linking failed (obsolete).
-10	File opening failed (obsolete).
-11	File queued before fax (obsolete).

-12	Cannot set timer (internal).
-13	File was not specified.
-14	Unix call failed (internal).
-15	Destination was not supplied.
-16	Mode, for FAX_CNG, not supplied (obsolete).
-17	Command was not supplied.
-18	Return string was not supplied.
-19	Cover page merging failed (internal).
-20	Subprog to sbFaxHpr failed (internal).
-21	IRAPI call failed (internal).
-22	**faxmastr** file open error occurred (internal).
-23	Wrong subprog message was received (internal).
-24	Max. sbFaxHpr instances was reached (internal).
-25	Fax file is a big endian fax file.

Investigating speech problems

Speech problems include all malfunctions related to playing and processing speech.

Speech not playing

Speech may not play for a variety of reasons, including the following:

- An NMS card or a channel is out of service.
- The voice response application does not contain, or fails to find, the required phrase.
- The required voice response application is not assigned to the channel.
- A proxy server providing Text-to-Speech service is disconnected or experiencing intermittent problems.

Checking the card and channel service state

To check card and channel state:

1. Do one of the following to check the status of the NMS card or cards:

   — Go to the **Display Equipment** screen.

— Type **display card *(card number)*** and press **Enter**.

The status should be in service (INSERV).

2. If the card or cards are not in service, try to restore the card or contact your Avaya support representative.

   See Restoring cards and channels on page 89 for procedures that may bring NMS cards back into service.

3. If the card is in service, place test calls to determine if the problem is occurring on every channel.

   If the problem occurs only on certain channels, it could be a hardware problem.

4. If the problem occurs only on certain channels, take one of the following actions:

   a) Go to the **Change State of Voice Equipment** screen (Configuration Management > Voice Equipment > Equipment State) and place the channels in a MANOOS state.

   b) Try to restore the card or contact your Avaya support representative.

      See Restoring cards and channels on page 89 for procedures that may bring a MANOOS channel back into service.

Checking the voice response application and system administration

To check the application and the administration settings:

1. If a particular phrase of recorded speech is not playing, check to see that it is recorded and record it, if necessary.
2. Go to the **Display Equipment** screen (Configuration Management > Display Equipment) and check to see if the correct service is assigned to the channel or channels.
3. If the correct service is not assigned, go to the **Assign Services to Channels** screen and make the required changes.

   See Assigning services to channels for more information.

Checking the server connection

If speech is supplied through a server on the LAN, check the connection: type **sproxyadm -r ALL -d** and press **Enter**.

See Troubleshooting speech server disconnections on page 97 for a complete procedure on checking and testing the connection.

Checking for errors

To check for errors:

1. Scan the **Message Log** report for messages related to the trouble.

2. Enter **trace tsm chan all | tee /tmp/trace.out** and press **Enter**.

   The trace output is sent to the console and to the file **/tmp/trace.out**

3. Review the trace output for failure indications or error messages.

Speech recognition not working

If Avaya **speech recognition** is not working, the cause may be:

- Incorrect or incomplete administration of the Natural Language Speech Recognition feature or proxy speech server on the IR system
- Disconnection or malfunction of the proxy speech server

The procedures in this section explain what to do when speech recognition is not working at all. See **PROXY alarms and messages** for information and repair procedures for a variety of speech recognition problems.

Speech recognition not available as resource

If the drop-down list in the **Speech Resource Status Display** screen does not display any type of speech recognition, the recognition type is not administered. See **Speech administration** for more information.

Cannot configure speech recognition

If the Speech Recognition Configuration option is not available on the **Speech Proxy Administration** screen, the Natural LanguageSpeech Recognition packages are *not* installed. The AVSproxy and AVsrproxy packages are required for the Natural Language Speech Recognition feature. If the Avaya Recognizer will be used for WholeWord support, Avasr, Avwwasr, and one or more of the language packages (AVwwau, AVwwbp, AVwwcf, AVwwcs, AVwwfr, AVwwgr, AVwwit, AVwwjn, AVwwms, AVwwnl, AVwwuk, Avwwus) are also needed.

All ports BROKEN on speech server

If all ports for a proxy speech server are in the BROKEN state when viewed either by recognition type or by server type, the speech recognition proxy is not able to connect to the specified server with the configured port.

To correct the problem:

1. Make sure that the speech recognition server is up and running.

   See Troubleshooting speech server disconnections on page 97 for more information.

2. Run the **netstat –a** on page 101 command on the recognition server to verify that the recognition server is listening on the configured port.

Speech resource bad or non-configured

If you see the following system message when you try to display a speech configuration resource, there is no server administered for the specified recognition type.

```
Error: Bad or Non-configured Resource type
```

See Speech administration for information on configuring proxy speech servers.

Speech response delayed

Delays in speech response may be caused by:

- Inadequate IR system or LAN resources. See Managing IR system performance for more information.
- Limited recognition resources in a speech recognition application. All remote application resources may be busy and not available for allocation to other calls. You must wait for resources to become available or increase the number of resources the system can use.
- Overloaded host communications. See Managing host interactions for more information.

Messages cut off

When messages are cut off, try making the following changes in the voice response application to correct the problem:

- Add a few seconds of initial silence (0.2 to 0.5 seconds) to the beginning of the message to be played.
- Construct a phrase consisting of a few seconds of silence and play that phrase first.
- Make sure that the prompt does not allow voice barge-in. If it does, any background noise or talk by the caller will interrupt the prompt.

Investigating system process problems

Problems with system processes affect you as the system administrator, and may also affect callers. Many system processes can cause speech breaks. CPU overload causes delays that result in a multitude of symptoms. Host interaction problems also may cause delays or breaks in calls.

Note:
The system process problems described in this section are *not* related to IR

system overload. For information about performance problems, refer to Managing IR system performance.

Call data reports inaccurate or incomplete

The CDH feature supports call data handling for reports.

If call data reports are not accurate or they are not complete, take these steps to correct the problem:

1. Type **dbfrag** and press **Enter**.

   This will determine if there is any additional free space in the database.

2. Review the **Message Log** report.

   — Message **DB001** may appear if an attempt to write a record into the database failed.

   — CDH messages identify problems with Call Handling reports.

3. Contact your Avaya support representative for assistance.

UNIX commands failing or disk errors

If UNIX commands are failing, or the system reports disk failures, scan the **Message Log** report.

vi editor causes core dump

If the vi editor causes a core dump, split the file into multiple segments.

Type **split - *n filename name*** and press **Enter**, where *n* is the number of lines in each piece (1000 is the default), *filename* is the name of the files you want to split, and *name* is the new segment you are creating.

ccasum does not finish cron job

To correct unfinished cron jobs:

1. Determine if the system is transferring to more than 100 numbers.
2. If more than 100 numbers are being transferred, kill the cron job:

   a) Type **ps -ef | grep ccasum** and press **Enter**.

b) Search for the parent process id (PID) for **ccasum** (located in the second column from the left).

c) For PID number *pid#*, type **kill *pid#*** and press **Enter**.

3. Create an index for **ccasum** by doing the following:

a) Log in to SQL*Plus as **sti/sti**.

b) Type **create index cca_idx on cca(phone_num);** and press **Enter**.

c) To exit the SQL*Plus Utility, type **:quit** and press **Enter**.

d) When the call traffic is light, type **/vs/bin/util/ccasum** and press **Enter**.

e) When **ccasum** is finished, type **/vs/bin/util/ccadel** and press **Enter**.

Card diagnostics fail

If card diagnostics fail, check for ESD sources, such as:

- Florescent lights
- Power supplies

If ESD is not an issue, contact your Avaya support representative. A technician may need to come to your site to check connections to the cards for kinks or pin problems.

Investigating database problems

If you are using databases on the LAN, communications problems with those databases may affect voice operations. Troubleshooting database server disconnections on page 98 covers what to do when the IR system is not communicating with the database server at all. The following topics explain how to check on less serious problems with databases.

Checking JDBC operations

Use the following commands to check JDBC function:

- **netstat *-a*** lists port usage.
- **trace chan all DBDIP3** traces DIP activity.

Review the following system processes related to JDBC operations:

- /vs/bin/vrs/idbcint *DIP num*
- /vs/bin/vrs/jdbcdip dipnumber
- /use/bin/../java/bin/../bin/SPARC/routine_threads/java -Dpname=ais3 -cp /webadm
- /user/bin/../java/bin/../bin/SPARC/routine_threads/java -Dpname=ais(dip number) -cp /webadm

Checking Oracle free space

To check the Oracle database free space:

1. Type **dbfrag** and press **Enter**.

   The system displays the **System Tablespace** screen.

2. If the number in the **%FREE** field is less than 20 in any of the tablespaces, add more space to that tablespace.

   Note:
   Contact your internal database administrator or your database vendor for help with this and other database tasks.

Checking Oracle object size limits

An extent is an user defined unit of storage in the Oracle **storage** clause when defining an Oracle object. It is used as MINEXTENTS or MAXEXTENTS in the storage clause. An Oracle object (that is, a table, an index, a rollback segment) grows one extent in size each time the object needs to be expanded.

When the maximum allowed number of extents is reached, the object will not be able to grow further. The object needs to be redefined so that either the size of each extent is increased or the initial object size is increased, to reduce the number of extents required for the storage of this object. The maximum allowed number of extents in an system is 2,147,483,645.

To check the number of extents:

1. Type **dbused** and press **Enter**.

   The system displays the **Space Allocated** screen.

2. Compare the value in the **EXTENTS** column to the value in the **MAX_EXTENTS** column.

   If the value in the **EXTENTS** column is greater than or equal to the value in the **MAX_EXTENTS** column, the table has reached its maximum size.

3. Redefine the database table storage, if necessary.

   Note:
   Contact your internal database administrator or your database vendor for help with this and other database tasks.

Tracing a service

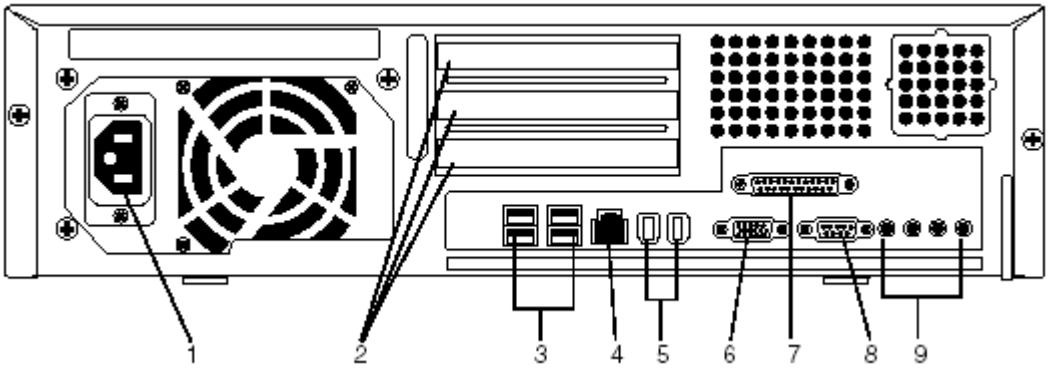
A trace is a record of the events that have occurred on a voice channel, the voice system, or a host system. Tracing tells you what events are occurring as the IR system completes tasks in the voice response application. Use the trace command to trace a service.

Checking hardware

Hardware failures and malfunctions can stop or interfere with voice system operations. This section explains how to check various types of hardware connections and components.

Checking cable connections

Make sure that the cables that connect your IR system to other devices and systems are firmly in place and functioning properly. The diagram below shows where cables connect to the back of the back of the Sun Blade 150 platform.



Label	Function and Troubleshooting Considerations
1	Power connector - Cable here provides power to the IR system. Disconnection from the plug results in loss of power and function.
2	PCI card slots - Cables here connect NMS cards to the MultiVantage (DEFINITY) system or to digital telephony lines. Problems here may interfere with receiving and handling calls.
3	USB connectors (four) - Two of these connectors are reserved for the keyboard and mouse that are part of the country kit. If a keyboard is not connected, and the IR system is rebooted, you may not be able to log into the IR system. Your organization may use the remaining USB connectors for other purposes.
4	Twisted-pair Ethernet connector - Cable here connects the IR system to the LAN. Problems here may interfere with access to voice response applications, databases, proxy speech servers, and other IR system components that reside on servers on the LAN. If VoIP is in use, a loose connection here may cause problems with call processing.
5	IEEE 1394 (Fireware) connectors (two).

6	VGA video connector - The cable connects the video monitor to the IR system. Problems here may cause the video monitor to appear blank, even though the IRsystem is still processing calls.
7	Parallel connector
8	Serial connector (RS-232) - Cables here connect the IR system to the external modem, which controls dial up access to the system for Avaya support technicians. Problems here may mean that Avaya support technicians are unable to acccess the IR system for troubleshooting purposes.
9	Audio module connectors

You can also test port function. The Sun OpenBoot Diagnostics system performs root cause failure analysis on the ports. The *Sun Blade 150 Service Manual* explains how to run OpenBoot Diagnostic tests.

Testing platform hardware

When hardware problems occur with the IR system, you can use the Sun Validation Test System (VTS) to test and validate the hardware. You use Sun VTS in the event of failures in:

- Powering on
- Video output
- The hard drive, CD-ROM, or DVD ROM drives
- Dual in-line memory module (DIMM) function

The *Sun Blade 150 Service Manual* explains how to run the tests.

Checking NMS card configuration

Check the configuration of the NMS card or cards with the commands described in the table that follows.

Commands	**Functions**
nmsboards	Identifies boards and their types (E1 or T1)
pcidev	Identifies board type and communicates with PCI files

boardinfor	Provides detailed information on the board, communicates with board and provides real-time memory display
trunkmon	Identifies trunk protocols
showcx95	Provides board timeslot information
ctavers	Identifies version of NMS software

Checking card and channel states

If you think a problem is caused by the failure or malfunction of an Avaya IR system channel, NMS card, or VoIP card, you can check the state of the component. To check card and channel states, go to the **Display Equipment** screen (Configuration Management > Voice Equipment > Display Equipment). The IR system displays information about cards and channels, which should show an in service (INSERV) state. If cards and channels are not in the INSERV state, you may be able to restore them. See Restoring cards and channels on page 89.

Restoring cards and channels

Channels and voice operations cards on the IR system can go out of service for a variety of reasons. When that happens, following the procedures presented in this section may restore channels, NMS cards, or VOIP cards to service. Most out-of-service conditions are the result of administration errors or intermittent problems, rather than actual hardware failures. By taking the time to troubleshoot, you may be able to resolve the problem yourself. If not, you will gain valuable information about the situation.

When you troubleshoot problems with cards and channels, bear in mind that as long as even one channel on a card is operating, the card will be in the in service (INSERV) state. If a card is out of service, *all* channels connected to the card are not operating.

Restoring MANOOS cards and channels

The MANOOS (manually out of service) state is the result of one of the following events:

- A user requested that the card or channel be taken out of service.
- An internal error put the card or channel in this state to allow for an attempted recovery.

To restore a channel or card in the MANOOS state:

1. Type **restore channel *channel #*** or **restore card *card#*** and press **Enter**.
2. Check the **Display Equipment** screen to determine if the card or channel has returned to the INSERV state. From the main menu: Configuration Management > Voice Equipment > Display Equipment.

   The card of channel may remain in the MANOOS state or go to another out-of-service state.
3. If the card or channel has not returned to the INSERV state, contact your Avaya support representative.

Restoring FOOS cards and channels

The FOOS state indicates that the card or channel was taken out of service by some physical channel error. Only to channels that are defined with LOOP or WINK start protocols go into the FOOS state.

To restore a card or channel in the FOOS state:

1. Go to the **Message Log Report** (Reports > Message Log Report) and review any messages related to the particular card or channel.
2. Check connections and indicators on the back of the IR system and reseat the connection, if necessary:

   a) Check the physical connection to the NMS or VoIP card and determine if it is seated correctly.

      The card should not have worked its way out of the connection. See Checking cable connections on page 87 for more information.

   b) If the connection is loose, re-seat it.

   c) Make note of other information about the card, such as lit LEDs, connection to the telephony switch for T1/E1 connections, LAN status for VoIP connections, and so forth.
3. If you have reseated the connection, go to the **Display Equipment** screen (Configuration Management > Voice Equipment > Display Equipment) to see if the card or channel is now in the INSERV state.
4. If the card or channel is still not in service, contact your Avaya support representative about the problem and share the information you have gathered.

Restoring NETOOS cards and channels

The NETOOS state indicates that the card or channel was taken out of service by some network or physical channel error. This state refers only to channels that are defined as PRI protocol.

To restore a card in the NETOOS state:

1. Go to the **Message Log Report** (Reports > Message Log Report) and review any messages related to the particular card or channel.
2. Check connections and indicators on the back of the IR system and reseat the connection, if necessary:
   a) Check the physical connection to the card and determine if it is seated correctly.

      The card should not have worked its way out of the connection. See Checking cable connections on page 87 for more information.

   b) If the connection is loose, re-seat it.
3. If you have reseated the connection, go to the **Display Equipment** screen (Configuration Management > Voice Equipment > Display Equipment) to see if the card or channel is now in the INSERV state.
4. If the card or channel is still not in service, take the following actions:
   a) Check the status of the card or channel on the switch system administration interface.
   b) Run diagnostics from the switch system administration interface to identify any errors there.
   c) If errors are identified, correct them.
   d) Busy out and release the card or channel on the switch to try to clear the problem.
   e) Re-check the status of the card or channel on the Display Equipment screen, if necessary.
5. If the card or channel is still not in service, contact your Avaya support representative about the problem and share the information you have gathered.

Restoring BROKEN NMS and VoIP cards

The BROKEN state can result from conditions other than actual malfunction of the card or channel. For example, the card or channel may:

- Be unconfigured, or configured incorrectly

- Have an inadequate number of Right-to-Use licenses (RTUs)

Note:
Individual channels do not come up in the BROKEN state, so the procedures in this section apply only to NMS and VoIP cards.

Inspecting the IR system platform

When an NMS or VoIP card is in the BROKEN state, inspect the IR system platform:

1. If the BROKEN card is an NMS card, determine whether there is a card in the identified slot.

   VoIP function is provided through the Ethernet connection, so there will be a card in the slot.

2. If there is no NMS card in the slot, take one of the following actions:

   — Install an NMS card.

   — Disregard the BROKEN state if no card is required in the slot.

   An IR system may operate using one or two NMS cards. If the system is configured for two NMS cards, but has only one, system messages and screens report a BROKEN card for the empty slot.

3. Check the connection for the BROKEN card or channel on the back of the IR system.

   The card or channel should not have worked its way out of the connection. See Checking cable connections on page 87 for more information.

4. If the connection is loose, re-seat it.

5. If you have reseated the connection, go to the **Display Equipment** screen (Configuration Management > Voice Equipment > Display Equipment) to see if the card or channel is now in the INSERV state.

If the card is still not in service, it may be administered incorrectly. See Checking card administration on page 92 for more information.

Checking card administration

If a card is present in the slot and securely connected, the next step is to check the IR system administration settings for the card.

To check administration settings:

1. Check configuration settings for the BROKEN card:

   — For the NMS card, go to the **Display Digital Interface Card** screen (Configuration Management > Switch Interfaces > Digital Interfaces > Protocols > Display Parameters > Display Digital Interface Card) to view the card parameters.

— For the VoIP card, go to the **Display VoIP Parameters** screen (Configuration Management > Switch Interfaces > Voiceover IP > Display Parameters > Display VoIP Parameters) to view parameters.

Configuration settings should match the type of card installed. VoIP cards should be enabled.

2. If the card is configured incorrectly, make the required corrections:

— For the NMS card, go to the **Change Card** screen for the appropriate type of digital interface (Configuration Management > Switch Interfaces > Digital Interfaces > Protocols > Digital Interfaces Protocols > Change Parameters - Change Card - Digital Interfaces, and choose subsequent screens based on card type).

See Checking NMS card configuration on page 88 for useful commands related to NMS cards.

— For the VoIP card, go to the **Change VoIP Card** screen (Configuration Management > Switch Interfaces > Voiceover IP > Change Parameters > Change VoIP Parameters > Change VoIP Card) and change parameters.

3. If you have corrected the card configuration, go to the **Display Equipment** screen (Configuration Management > Voice Equipment > Display Equipment) to verify the card state.
4. If the card is still not in service, type **display card *card _number*** and press **Enter**. See if the card is found.

Note:
If there are problems with licensing, there may be no usable channels on the card, and the card will not be found when the **display card** command is run.

5. If the card is not found, go to the **Feature Licensing** screen (Configuration Management > Feature Licensing) and verify that there are enough Right-to-Use licenses (RTUs) for the channels supported by the card.
6. If you do not have an adequate number of RTUs for channels in operation, contact your Avaya support representative to arrange to acquire more RTUs.

If RTUs are not an issue, and the card is still not in service, you may be able to bring it back into service by removing and restoring it. See Removing and restoring cards on page 93 for more information.

Removing and restoring cards

If the connection to a card is seated properly, and the card is configured correctly, try removing and restoring the card. Repeat the remove and restore process anytime that you change a configuration parameter or reseat a cable. Removing and restoring causes the IR system to attempt re-initialization of the card.

To remove and restore a card:

1. To remove the card, type **remove card *card number*** and press **Enter**.
2. To restore the card, type **restore card *card number*** and press **Enter**.

   The IR system attempts to configure the card again. The reconfiguration process may bring the card back into service.
3. If the card remains in the BROKEN state, check the card configuration in the switch and make any required corrections.
4. Remove and restore the card again on the IR system.

   Even if you have made no changes to the card configuration on the switch, removing and restoring the card at this point may clear the problem.
5. If the card is still BROKEN, busy out and release the card on the switch.
6. Remove and restore the card once more on the IR system.

If the card remains in the BROKEN state, you need to find out more and then contact your Avaya support representative. See Gathering data on card operations on page 94 for more information.

Gathering data on card operations

Display required information as described in the following procedure, then contact your Avaya support representative for assistance in troubleshooting the card.

Displaying information about NMS cards

1. Type **trunkmon-b *card_number*** and press **Enter** to display information about a specific card.

   The **alarms** column should show a steadily-displayed entry of **NONE**, and the **Frame sync** column should show a steadily-displayed entry of **OK**. If either of these entries is fluctuating between the identified values and another value, note the other value for discussion with your Avaya support representative.
2. Press **Esc** to return to the command-line interface.

Displaying information about VoIP cards

1. Run the following diagnostics:

   — SunVTS OpenBoot diagnostics for the network connection

   — Watch-Net and Watch Net-All diagnostics

   All of these diagnostics monitor Ethernet packets and identify both good packets and packets with errors. The *Sun Blade Service Manual* explains how to use these diagnostics.

2. Note the results for discussion with your Avaya support representative.

Performing root cause failure analysis

The Sun OpenBoot Diagnostics system performs root cause failure analysis on various IR devices by testing internal registers, confirming subsystem integrity, and verifying device functionality. The *Sun Blade 150 Service Manual* explains how to run OpenBoot Diagnostic tests.

Checking communications

Because voice system functions may be reliant on servers, checking LAN communications is an important aspect of troubleshooting. You may need to work with your LAN administrator to completely investigate LAN problems.

Checking LAN communications

To support voice response operations, an Avaya IR system may communicate with remote servers that store databases, with proxy servers for text-to-speech and speech recognition, or both. Using servers outside the Avaya Interactive Response system provides flexibility and increased storage capacity. However, problems with the LAN and with servers themselves can interrupt or cut off access to required functions.

Understanding how to check LAN connections and communications helps you to identify the cause of voice response problems faster when servers are part of the picture. The following are typical causes of problems with server communications over the LAN:

- Incorrect administration of server communication settings, such as IP addresses
- Breakdowns in the LAN system or malfunction of the server itself
- Overloading the Avaya IR system or the LAN

You can receive help with troubleshooting server problems from your LAN administrator and from Avaya. Before seeking assistance, be sure to:

- Research the situation
- Make sure that servers are administered correctly in the Avaya IR system

Troubleshooting speech server disconnections

To investigate the problem when a speech proxy server is not responding:

1. Go to the **Speech Server Status** screen (Feature Packages > Speech Administration > Display Status > Display Speech Proxy Status > Speech Server Status) to check server status and settings.
2. Select the desired speech server from the list and click **Submit**.

   The system displays setting and status information for the server.
3. Verify that the correct ports, server name, and IP address are in use.

   If you have recorded the server name and IP address on the Avaya IR system Data Form, refer to it now.
4. If there are errors in the configuration of the server, take the following actions:

   a) Go to the appropriate proxy configuration screen and make the required corrections.

      To correct speech recognition configuration errors, go to the **Change Speech Recognition Server** screen (Feature Packages > Speech Administration >

Administration > Speech Recognition Configuration > Change Speech Recognition > Change Speech Recognition Server).

To correct text-to-speech configuration errors, go to the **Change Text-to-Speech Server** screen (Feature Packages > Speech Administration > Administration > Text-to-Speech Configuration > Change Text to Speech > Change Text-to-Speech Server).

b) Return to the Speech Server Status screen to see if the server status is INSERV (in service).

5. If the server status is not INSERV, go to the Solaris operating system and execute the **ping** on page 100 command to test the connection.
6. If the **ping** command fails, take the following actions:

   a) Check the **/etc/hosts** file to make sure that it has the correct IP address and name for the server.

   b) Verify that the LAN cables are correctly connected between the Avaya IR, the server, and the LAN hub (where applicable).

   c) Make sure that the voice response application is referring to the correct server.

   d) Contact your LAN administrator to determine whether there are problems with the server or with network connections.

7. If the **/etc/hosts** file is correct and no network problems exist, check license administration on the remote server to ensure that the maximum number of licenses has not been exceeded.
8. If the server remains disconnected, contact your Avaya technical support representative for assistance.

Troubleshooting database server disconnections

To investigate the problem when a database server is not responding:

1. Go to the JDBC Administration screen (Configuration Management > JDBC Administration) to check server status and settings.
2. Select the database data interface process (DIP) that interacts with the server in question.

   The system displays the **JDBC Administration - Edit** screen.
3. Check the DIP settings, particularly those for ports, hostname and DB name, and make any required corrections.

   If multiple DIPs interact with the server, you will need to check them separately.

4. Click **Test** to check communications between the Avaya IR system and the database server.

   Once the Avaya IR system is configured, you can check the network connection to *any* database through the JDBC Administration - Edit screen.

5. Continue checking settings, testing connections, and making corrections for all DIPs that communicate with the database server.
6. If the database server is still not responding, take the following actions:

   a) Check the **/etc/hosts** file to make sure that it has the correct IP address and name for the server.

   b) Verify that the LAN cables are correctly connected between the Sun Blade 150, the server, and the LAN hub (where applicable).

   c) Make sure that the voice response application is referring to the correct server.

   d) Contact your LAN administrator to determine whether there are problems with the server or with network connections.

7. If the **/etc/hosts** file is correct and no network problems exist, check license administration on the remote server to ensure that the maximum number of licenses has not been exceeded.
8. If the server remains disconnected, contact your Avaya technical support representative for assistance.

Troubleshooting intermittent LAN problems

Slow or interrupted LAN communications may result in failed processes for speech recognition, Text-to-Speech, or database checking. The cause is generally overloading of the Avaya IR system or the LAN.

See Managing Avaya IR system performance for:

- Guidelines on LAN requirements for voice response operations
- Information on assessing and reducing load on the IR system

Troubleshooting persistent server problems

If you experience persistent problems with a server, you may want to reconfigure and retest:

1. Put all systems used in the application that is experiencing problems on a dedicated LAN hub, completely isolated from the rest of the LAN.

2. Configure the systems to communicate with each other over the dedicated LAN hub.
3. Use the **ping** on page 100 command to verify that the server responds.
4. If none of these solutions work, contact your field support representative.

Pinging server connections

The **ping** command indicates whether a remote host can be reached. It can also display statistics about packet loss and delivery time.

The ping command is available through the Solaris operating system. Use it with the attributes shown in the following table:

Attribute	Function
-d	Set the SO_DEBUG socket option.
-l	Send the packet to the given host and back again.
-L	Turn off loopback of multicast packets.
-n	Display the network addresses as numbers.
-r	Bypass the normal routing tables and send directly to a host on an attached network.
-R	Set the IP record route option and store the route of the packet inside the IP header.
-v	List any ICMP packets, other than ECHO_RESPONSE, that are received.
-i	Specify the outgoing interface to use for multicast packets.
-I	Specify the interval between successive transmissions.
-t *ttl*	Specify the IP time to live for multicast packets.

Monitoring Ethernet packets

The Sun Solaris operating system provides Watch-Net and Watch Net-All diagnostics that monitor Ethernet packets and identify good packets, and packets with errors. The *Sun Blade Service Manual* explains how to use these diagnostics.

Tracing LAN activities

LAN trace utilities help you see how LAN communications are operating and identify problems. The LAN trace utilities have a few disadvantages:

- Only traffic on the subnet to which the IR system is attached can be traced.
- When traffic on the LAN is very heavy, some packets may be lost because the server cannot keep up with the flow.

Nevertheless, these utilities are very helpful. You may want to seek support from your Avaya support representative when running them.

Detecting incorrect IP addresses (arp)

The **arp** command provides information about Ethernet/IP address translation. The command can be used to detect systems on the LAN that are configured with an incorrect IP address. The table that follows identifes options for the **arp** command and their functions.

Command	Function
arp -a [unix[kmem]]	Display all of the current ARP entries by reading the table from the file **kmem** (**default /dev/kmem**), based on the kernel file **unix** (**default /kernel/unix**)
arp -d *hostname*	Delete an entry for the host called *hostname*. **Note:** This option may only be used by the super-user.
arp -s *hostname ether_address* [temp] [pub] [trail]	Create an ARP entry for the host called *hostname* with the Ethernet address *ether_address*
arp -f *filename*	Read the file named *filename* and set multiple entries in the ARP tables

Displaying network statistics (netstat)

The **netstat** command is used to display statistics about each network interface and socket, and statistics about the network routing table. Use the **netstat** command with the attributes shown in the table that follows.

Attribute	Function
-a	Display the state of all sockets and all routing table entries.
-f *address_family*	Limit the statistics or address control block reports to those of the specified family. (The address family can be inet for the AF_INET family or UNIX for the AF_UNIX family.)
-g	Display the multicast group memberships for all interfaces.

-i	Display the state of the interfaces that are used for TCP/IP traffic.
-m	Display the STREAMS statistics.
-n	Displays the network addresses as numbers.
-p	Display the address resolution tables, using the **-p** option.
-r	Display the routing tables.
-s	Display the per-protocol statistics.
-v	Display additional information for the sockets and the routing table.
-I *interface*	Display the state of a particular interface.
-M	Display the multicast routing tables.
-P *protocol*	Limit the display of statistics or state of all sockets to those applicable to protocol.

Displaying packet route (traceroute)

The **traceroute** command displays the route packets take going to a remote system. Information about the route is printed. Use the **traceroute** command with the attributes shown in the table that follows.

Attribute	**Function**
-f	Set the initial time-to-live used in the first outgoing probe packet
-F	Set the **don't fragment** bit
-d	Enable socket level debugging
-g	Specify a loose source route gateway
-i	Specify a network interface to obtain the source IP address for outgoing probe packets
-I	Use the ICMP ECHO instead of UDP datagrams
-m	Set the max time-to-live (max number of hops) used in outgoing probe packets
-n	Print hop address numerically rather than symbolically
-p	Set the base UDP port number used in probes. (Default is 33434.)
-r	Bypass the normal routing tables and send directly to a host on an attached network
-s	Use the following IP address (which usually is given as an IP number) as the source address in outgoing probe packets

-t	Set the type of service in probe packets to the following value
-v	List the ICMP packets other than TIME_EXCEEDED and UNREACHABLE
-w	Set the time (in seconds) to wait for a response to a probe
-x	Toggle checksums

Obtaining release notes

Release notes for Avaya IR are available at Avaya Support Centre Web site.

To obtain release notes:

1. From a Web browser, go to http://support.avaya.com.
2. From the navigation menu (the area on the left of the browser window, under **Technical Database**), click **Call Center/CRM**.
3. From the navigation menu, click **Interactive Voice Response**.
4. From the navigation menu, click **Interactive Response**.
5. Click **Release Notes**.

   The browser displays a table listing the current Release Notes.
6. In the **Release Notes** table, click **Avaya IR R1.0 Release Notes**.

   The browser displays information about the Release Notes, and links for different file formats.
7. Click the appropriate link in the **Download File** table.

   The file downloads to your computer.

Index

R

S

T

U

V

W