Avaya™ Interactive Response

Release 1.0

Common administration tasks

Issue 1
Publication Date: December 2002

© 2002, Avaya Inc.
All Rights Reserved

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 US and Internationa**l. This Web site includes telephone numbers for escalation within the United States. For escalation telephone numbers outside the United States, select **Global Escalation List**.

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

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
Avaya provides a telephone number for you to use to report problems or to ask questions about your contact center. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see 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, select **Global Escalation List**.

Warranty
Avaya Inc. provides a limited warranty on this product. Refer to the Limited use Software License Agreement provided with your package.

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.

About this document

This document is a compilation of help topics from *Avaya IR System Help* that has been formatted for printing. It contains the same information as the *Help* itself.

This document is only available as part of the *Avaya IR System Help* and *Avaya IR Documentation CD.* You cannot order this document separately from Avaya.

About cross-references in this document

The topics in *Help* contain hypertext links to other topics that enable you to jump to the linked topic. In this document, hypertext links appear as cross-references to the pages containing the linked topics. For example, a hypertext link in *Help* to a topic called "Features" would appears in this document as

"See Features on page 54 for more information"

However, not all the linked-to topics are included in the printable documents. This results is some topics that are normally linked in the *Help* content, appearing without page cross-references. Using the example above, if the "Features" topic is not included in this document, the text appears as

"See Features for more information"

Please be aware that this is a limitation of having subsections of *Help* compiled for print. If you see text that looks like a cross-reference without a page number, the information is available in *Help*.

Contents

Common administration tasks

There are several tasks that most people perform in the administration of a system. In this section you can find procedures for these tasks.

Accessing the system

The system can accessed for administration directly on the hardware platform or over the LAN. Users who perform UNIX administration functions must be a member of the sysadmin group (group 14) or have root-level permissions.

Accessing the system with a direct connection

With a monitor, keyboard, and mouse connected to the hardware platform, you can directly access the system. Typically the command-line interface is already available (as a UNIX prompt), and you can use administration commands after you log in to the system.

To use the Web Administration interface:

1. Run the Netscape browser from the UNIX prompt.

   To do so, type **/usr/dt/bin/netscape** and press **Enter**. (This command may have changed. See "Getting Started With Netscape Communicator" in the latest version of Sun Blade 150 Getting Started.)

2. Type the URL of the system in the address window and press **Enter**.

   The browser displays the Web Administration entry screen.

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

   The browser displays the Login screen.

4. Log in to the system.

Accessing the system with a LAN connection

To use the Web Administration interface:

1. Run a supported browser from a computer that is connected to the LAN.
2. Follow Steps 2 through 4 in "Accessing the system with a direct connection" above.

To use the command-line interface:

1. Start a terminal session, using a terminal or terminal emulator.
2. Log in to the system.

Administering users

You can determine who can have access to the system, and what these users are able to do with the system (by assigning permissions to them).

Changing permissions

Users can have different levels of permissions for Web Administration, as described in the following table:

Permission	Description
Root	Any task on the system can be performed by the user
Administration	The user has full control of the voice system
Operations	The user has access to configuration management, reports administration, and system monitor capabilities, but does not have control of the voice system

Note:
Different Web Administration menu options are displayed for each permission level.

Only a user with root level permission can set a user's permission level. From the command-line interface, the root user does the following:

1. To determine the current permission level of a user whose user name is *username*, type **display_permissions *username*** and press **Enter**. The permission level is displayed on the screen.
2. To change the user's permission level:
   - To administration, type **assign_permissions *username* Administration** and press **Enter**.
   - To operations, type **assign_permissions *username* Operations** and press **Enter**.
3. To remove a user's access to the voice system, type **unassign_permissions *username*** and press **Enter**.

Adding users and changing passwords

To add users or manage passwords, use the relevant Solaris UNIX administration commands. See the Sun Solaris 8 System Administration Guide, Volume 1 for more information.

Administering the system

Administration of the system involves creating the proper associations between voice applications ("services"), channels, speech resources, telephone numbers, switches, and databases.

Administering channels

Channels typically have telephone numbers and services associated with them. Channels can also belong to equipment groups, allowing them to be administered together.

Assigning channels to equipment groups

If more than one channel needs to have the same configuration, an equipment group can be created that has this configuration. If you want a channel to have the configuration of an equipment group, you simply assign the channel to the group. This simplifies the administration process considerably. You can administer the group as a whole rather than administering each channel individually.

Assigning channels to groups from the Web Administration interface

1. Go to the Channels to Groups screen (Configuration Management > Voice Equipment > Channels to Groups).
2. Select **Assign**. The browser displays the **Assign Channels to Equipment Groups** screen.
3. Fill in the fields, and click **Submit**.

Note:
You can reverse this process by *unassigning* a channel from a group. To do so, choose **Unassign** instead of **Assign** in Step 2 above.

Assigning channels to groups from the command-line interface

Use the assign channel command to assign a channel to a group.

Note:
To unassign a channel, use the delete channel command.

Assigning phone numbers to channels

You can associate telephone numbers with specific channels.

Using Web Administration

1. Choose Configuration Management > Voice Equipment > Phone Number from the main menu.

   The browser displays the Phone Number - Channel Assignment screen.

2. Choose **Assign**.

   The browser displays the **Assign Phone Number to a Channel** screen.

3. Type the phone number in the **Phone Number** field.
4. Enter a channel number in the **Channel Number** field.
5. Click **Submit**.

Using the command-line

Use the assign phone command.

Assigning services to channels

Services are voice response applications. You can have one or more channels run a given application by assigning the application to the channels you want to run it.

Using Web Administration

1. Choose Configuration Management > Voice Equipment > Voice Services from the main menu.

   The browser displays the Voice Services screen.

2. Select **Channel Services**.

   The browser displays the Channel Services screen.

3. Select **Assign Service**.

   The browser displays the **Assign Services to Channels** screen.

4. Select a **Service Name** and a **Startup Service**.
5. Fill in the **Channels** field with the channels you want the services assigned to.
6. Click **Submit**.

Using the command-line interface

Use the assign service/startup command.

Administering databases

The system uses database DIPs to communicate with databases (one DIP per database). These DIPs need to be supplied with information regarding where and how to access the databases. The DIP configuration is managed entirely from the Web Administration interface.

You can have call information alternatively stored in a Call Data Handler (CDH) flat file where it can either be read directly or uploaded into a database. The upload to a database can be done at a convenient (low traffic) time using a cron job.

Configuring a database DIP

1. Choose Configuration Management > JDBC Administration from the main menu.

   The browser displays the JDBC Administration - Main screen.

2. To configure a DIP:

   a) Select the hyperlink corresponding to the DIP in the **Dipid** column.

      The browser displays the **JDBC Administration - Edit** screen for the DIP you chose.

   b) Fill in the fields and click **Save**.

3. To activate a DIP:

   a) Select the radio button beside the name of the DIP in the **Dipid** column of the **JDBC Administration - Main** screen.

   b) Click **Start**.

      The browser displays the DIP Start Status screen, which shows whether or not the DIP has started.

4. To deactivate a DIP:

   a) Select the radio button beside the name of the DIP in the **Dipid** column.

   b) Click **Stop**.

      The browser displays the DIP Stop Status screen, which shows whether or not the DIP has stopped.

Configuring CDH

If a flat file is always used, the flat file needs to be configured:

1. Select the **File CDH** hyperlink in the **Dipid** column of the **JDBC Administration - Main** screen.

   The browser displays the **JDBC Administration - Edit** screen.

2. Select the database DIP that is used to upload the flat file to a database.
3. Enter the path to the flat file. Include the file name.
4. Click **Save**.

If you enable File CDH, the information saved in the flat file is always stored in the database accessed by the database DIP you chose.

> **Note:**
> Since enabling File CDH results in heavy LAN traffic, Avaya does not recommend doing this in most cases.

To enable File CDH:

1. From the **JDBC Administration - Main** screen, select the radio button beside **File CDH** in the **Dipid** column.
2. Click **Start**.

   The browser displays the **DIP Start Status** screen, which notifies you if the DIP has successfully started.

To disable File CDH:

1. From the **JDBC Administration - Main** screen, select the radio button beside **File CDH** in the **Dipid** column.
2. Click **Stop**.

   The browser displays the **DIP Stop Status** screen, which notifies you if the DIP has successfully stopped.

In some cases, you may want to create your own customized database DIP to run with a database. This DIP would use the CDH flat file as its source of call data.

To configure the DIP:

1. From the **JDBC Administration - Main** screen, click on the **Database CDH** hyperlink in the **Dipid** column.

   The browser displays the **Database DIP Configuration - Edit** screen.

2. Fill in the fields and click **Save**.

To activate the DIP:

1. From the **JDBC Administration - Main** screen, select the radio button beside the name of the DIP in the **Dipid** column.

2. Click **Start**.

   The browser displays the **DIP Start Status** screen, which notifies you if the DIP has successfully started.

To deactivate a DIP:

1. From the **JDBC Administration - Main** screen, select the radio button beside the name of the DIP in the **Dipid** column.
2. Click **Stop**.

   The browser displays the **DIP Stop Status** screen, which notifies you if the DIP has successfully stopped.

Administering messages

Messages relay information about the status of the system. These messages can be sent to a number of destinations, including a message log, based on priority and on the number of messages generated by the system in a specified period of time.

You can also create a report that extracts information of interest from the message log.

Using the Web Administration interface

The Message Administration screen lets you determine what messages are sent to particular destinations, and under what conditions. To see this screen, choose Configuration Management > Message Administration from the main menu.

The Message Log Report screen provides options for constructing and viewing a summary of messages found in the message log. To see this screen, choose **Reports > Message Administration** from the main menu.

Using the command-line interface

Several commands apply to message administration, display, and reports.

- To explain messages, use the explain command.
- To display messages, use the display messages command.

Administering the voice system

Administering the voice system includes the following tasks:

- Checking voice system status
- Renumbering voice channels
- Stopping and starting the voice system

Checking voice system status

You can find out the following:

- Whether the voice system is operating or not operating (*up* or *down*)
- The number of purchased voice ports
- The number of voice ports in service

Using the Web Administration interface

Choose Configuration Management > System Control > Report Voice System Status from the main menu. The browser displays the Report Voice System Status screen.

Using the command-line interface

Use the vs_status command.

Renumbering voice channels

The Renumber Voice Channels option removes all nonexistent (NONEX) circuit cards from the voice equipment table, and reorders all existing equipment. This reordering changes the channel numbers of some circuit cards. However, user-defined characteristics such as options, attributes, and script assignments, do not change. If a circuit card is found in the system that was not in the voice equipment table, it is added with default settings.

Renumbering voice channels brings down the system immediately and restarts it. When you select this option, a warning is displayed and you are given the option of continuing with the procedure or returning to the **System Control** menu.

Using the Web Administration interface

To renumber the voice channels:

1. Choose Configuration Management > System Control > Renumber Voice Channels from the main menu.

   The browser displays the Renumber Voice Channels screen.

2. Click **Renumber**.

   The browser notifies you that renumbering takes effect after the voice system is restarted.

3. Stop and restart the voice system on page 24.

Using the command-line interface

To renumber the voice channels:

1. Use the renumber command.
2. Stop and restart the voice system on page 24.

Stopping and starting the voice system

If you stop the voice system, no calls are answered by the system. Starting the voice system enables call answering and processing.

Using the Web administration interface

To stop the voice system:

1. Select Configuration Management > System Control > Stop Voice System from the main menu.

   The browser displays the Stop Voice System screen.

2. Click **Submit**.

   The browser displays a screen that tells you whether the voice system has stopped.

To start the voice system:

1. Select Configuration Management > System Control > Start Voice System from the main menu.

   The browser displays the Start Voice System screen.

2. Click **Submit**.

   The browser displays a screen that tells you whether the voice system has started.

Using the command-line interface

- To stop the voice system, use the stop_vs command.
- To start the voice system, use the start_vs command.

Administering fax

Administering the fax feature involves three basic procedures:

1. Enabling fax for the digital protocol you are using
2. Creating a fax header
3. Viewing and modifying the fax transmission queue
4. Printing a fax that has been received

Enabling fax

Enabling fax involves administering the card you are using to recognize fax as being associated with a particular digital protocol.

Using Web administration

To enable fax on a card that has already been administered:

1. From the main menu, select Configuration Management > Switch Interfaces > Digital Interfaces.

   The browser displays the **Digital Interfaces** screen.

2. Choose **Protocols**.

   The browser displays the Digital Interfaces Protocols screen.

3. Choose **Change Parameters**.

   The browser displays the **Change Card - Digital Interfaces** screen.

4. Choose the protocol you are using.

   The browser displays a **Change Parameters** screen appropriate to the protocol.

5. Select a **Card**.
6. Click **Submit**.

   The browser displays a **Change Card** screen for the card.

7. Select *yes* in the **Fax Enabled?** field.
8. Click **Submit**.

Using the command-line interface

To enable fax: Use *y* for the *fax* argument of the nms change command.

See also

- Administering fax on page 26

Creating a fax header

A fax header is text that is automatically placed at the top of every fax page. The following procedures describe how to create a header or use an existing one.

Using Web Administration

1. Go to the Fax Administration screen (Feature Packages > Fax Administration).
2. Select **Fax Header**.

   The browser displays the Fax Header screen, which shows the current fax header.

   Note:
   If you want to use the **Current Fax Header**, navigate to another screen (do so without clicking any of the buttons on this screen).

   The rest of this procedure describes how to change the fax header.
3. Select a **Fax Header**.
4. Click **Submit**.
5. If you chose **none** or **default**, the browser displays the names of the current fax header and the new fax header.
   - To accept the new fax header, click **Submit**.
   - To pick a different header, click **Cancel**. Continue with Step 3.
6. If you chose **custom**, enter the **New Custom Header Text** on the screen that the browser loads.
7. Click **Submit**.

Using the command-line interface

To create a fax header: Use the fax command.

Administering the fax queue

To view the fax queue or remove any fax jobs from the queue:

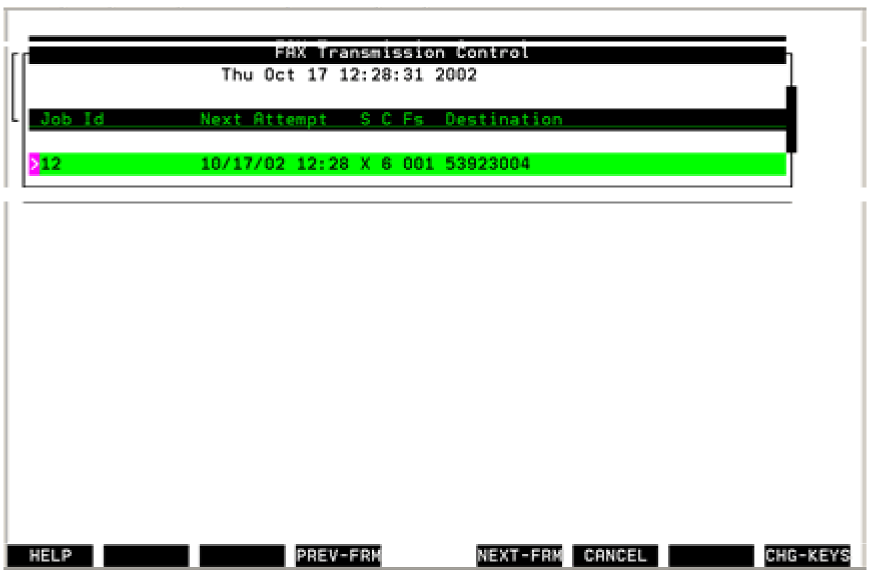
Displaying the fax queue (from the command-line interface)

1. Type **fax_admin** and press **Enter**.

   The **FAX Actions** menu is displayed on the screen.

2. From the **FAX Actions** menu, select **FAX Transmission Control**:

3. The system displays the **FAX Transmission Control** window:



The **FAX Transmission Control** window lists the details (such as time, date, and size) for every fax job in queue. The fax jobs are listed in the order in which they appear in the fax transmission queue.

The following table describes the columns on the **FAX Transmission Control** window.

Column Name	Description
Job ID	The job identification number
Date/Time Submitted	The date and time the fax request was submitted

Column Name	Description
Date/Time Next Attempted	The date and time the fax job is to be processed. This is the time specified by the application if no attempt to send the job has been made, or it is the subsequent retry attempt time if the original attempt failed.
S	The current status of the job: F — Job has failed (final failure). W — Job is waiting for a retry attempt. R — Job is ready to be processed. The outgoing call is in progress. D — Job is delayed by user (scheduled for future delivery). A — Job is waiting for an address. Destination number is not found. X — Job is transmitting the fax. P — Job is being processed. S — Job has sent the fax. f — Job process has failed.
Pgs/Snt	The number of pages submitted and the number of pages transmitted
Destination	The telephone number where the fax is to be delivered

Note:
The system does not automatically update the FAX Transmission **Control window when new entries are added to the fax queue.**

1. Updating the FAX Transmission Control window
2. Fr**om the FAX Transmission** Control window, **p**ress F6 (Cancel) to return **to the FAX** Actions menu. You may need to **p**ress F8 (Chg-Keys) to **access** CANCEL.

   In the FAX actions menu, **select FAX Transmission** Control.

   The system displays the updated fax **queue**.

Note:
It may be necessary to remove a fax from the queue to perform channel diagnostics or to relieve an overburdened system.

1. Removing a fax from the fax job queue
2. **In the FAX Transmission** Control window, select the fax to be removed.

   Press F2 (Remove). You may need to **p**ress F8 (Chg-Keys) to access REMOVE.
3. The system removes the selected fax.

Press F6 (Cancel) repeatedly to return **to the FAX** Actions menu.

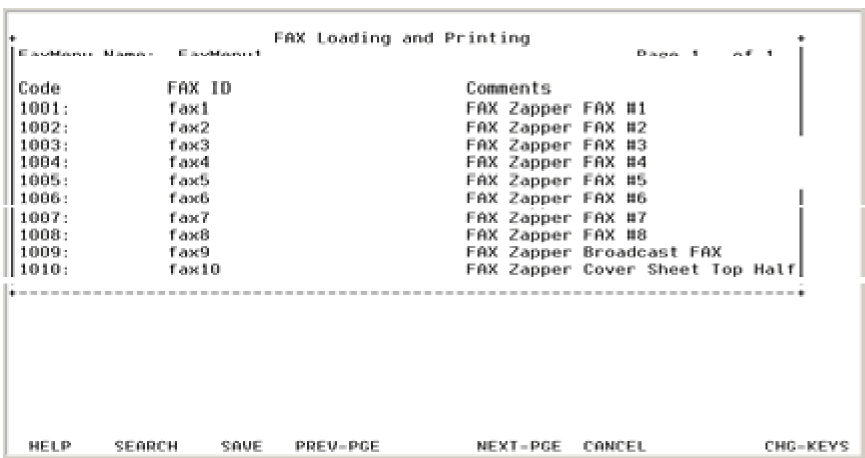
Printing a fax

The **FAX Loading and Printing** window allows you to load a fax in the system, preview a fax, or send a fax to the printer.

To access the **FAX Loading and Printing** window:

1. Start at the **FAX Actions** menu and select **FAX Loading and Printing**:

The system displays the **FAX Loading and Printing** window.



FAX Loading and Printing

Code	FAX ID	Comments
1001:	fax1	FAX Zapper FAX #1
1002:	fax2	FAX Zapper FAX #2
1003:	fax3	FAX Zapper FAX #3
1004:	fax4	FAX Zapper FAX #4
1005:	fax5	FAX Zapper FAX #5
1006:	fax6	FAX Zapper FAX #6
1007:	fax7	FAX Zapper FAX #7
1008:	fax8	FAX Zapper FAX #8
1009:	fax9	FAX Zapper Broadcast FAX
1010:	fax10	FAX Zapper Cover Sheet Top Half

HELP SEARCH SAVE PREV-PGE NEXT-PGE CANCEL CHG-KEYS

Above is a sample of the **FAX Loading and Printing** window. The window in your system may appear differently. The columns and what they represent, however, are the same.

The following table provides a description of the columns in this window.

Column Name	Description
FaxMenu Name	Name of the menu displayed in the window
Page	Number of pages in the menu

Column Name	Description
Code	A 4-digit identifier. The first digit may not be a zero.
FAX ID	An alphanumeric string in the form of faxN where N is a number between 1 and 999
Comments	2. A description of the fax, with 30 or fewer alphanumeric characters

3.

   Press F8 (Chg-Keys).

4. The system displays the alternate set of function keys.

   Press F4 (FAX-ADM).

5. The system displays the fax queue.

   — Select the fax to be loaded or printed, and do one of the following:

   — **Pr**ess F2 (Load-FX) to load the fax onto the system.

6. **Pre**ss F3 (Print-FX) to send the fax to the system printer.

Press F6 (Cancel) repeatedly until you return t**o the FAX A**ctions menu.

Administering speech recognition

Voice response applications access speech recognition resources using speech recognition types. Each speech recognition type is assigned to one or more servers that are running speech recognition engines.

So that an application can use a speech resource, you must do the following administration tasks:

1. If using Proxy Text-to-Speech (PTTS), assign TTS system parameters
2. Assign the type (speech recognition or TTS)
3. Assign the type to a server
4. Stop and restart the voice system

Note:
In some cases (such as during maintenance and troubleshooting) you may want to take a particular resource out of service. In these cases you would change the speech state for the resource.

Administering speech resources

The same basic steps for administering speech resources are followed from whichever interface you use.

Using the Web Administration interface

1. Assign the speech recognition type.

   a) Go to the Speech Proxy Administration screen (Feature Packages > Speech Administration > Administration).

   b) Choose Speech Recognition Configuration.

   c) Choose **Assign Speech Recognition**.

   The browser loads the Assign Speech Recognition Configuration screen.

   d) Choose **Assign Speech Recognition Type**.

   e) Select a **Recognition Type**, and click **Submit**.

   f) Fill in the fields, and click **Submit**.

2. Assign the speech recognition type to a server.

   a) Go to the **Assign Speech Recognition Configuration** screen (see Steps 1a through 1c above, or use the **Back** button on your browser, or click the **Cancel** button on the screen).

   b) Choose **Assign Speech Recognition Server**.

      The browser loads the **Assign Speech Recognition Server** screen.

   c) Select the recognition type you assigned in Step 1, and click **Submit**.

   d) Fill in the fields, and click **Submit**.

3. Stop and restart the voice system (see Stopping and starting the voice system on page 24).

Using the command-line interface

1. Assign the speech recognition type.

   Use the speech assign command.

2. Assign the speech recognition type to a server.

   Use the **speech assign** command.

3. Stop and restart the voice system (see Stopping and starting the voice system on page 24).

Special considerations for speech resources

Administration of speech resources on the Avaya IR system depends on the speech engine you are using. Below are recommendations and information about administration for several of the speech engines that Avaya supports.

The column headings are described in the following table:

Column heading	**Description**
Parameter	The name of a parameter of the speech assign command
Screen field	The field in the Assign Speech Recognition Configuration screens that is equivalent to the parameter
Value	The recommended value for the parameter and the screen field

Column heading	Description
Comments	Additional information and recommendations

Administering SpeechWorks for VoiceXML

Parameter	Screen field	Value	Comments
filter	Speech filter	no	—
configfile	Speech configuration file	default	**/vs/sproxy/cfg/SRproto.cfg**
protocol	Speech protocol	oss	—

Administering speech with Nuance

Parameter	Screen field	Value	Comments
filter	Speech filter	no	Set filter to *y* if Nuance's NPC process is version 3.0 or earlier and does not support -stdmulaw in the **npc** batch file.
configfile	Speech configuration file	default	**/vs/sproxy/cfg/SRproto.cfg**
protocol	Speech protocol	default	—
baseport	Base port	2345	This is an example. The port should be consistent with the *RecClientPort* defined in the Nuance **npc** batch file.
share	Share Base Port?	yes	Value is *yes* if one NPC, *no* if number of NPC is same as number of ports

The following is an example of npc batch file running on the Nuance server:

```
npc -package C:\Nuance\v8.0.0\grammar\stk -httpport 8001 -stdmulaw
audio.Format=8bit-mulaw config.ServerPort=8888  config.ServerHostname=ivrsp11
```

```
client.Behaviors=calllog config.RecClientPort=7783 rm.Addresses=ivrsp10 rm.Port=7777
      lm.Addresses=ivrsp10 -numdisp 12
```

Administering speech with Avaya WholeWord

Parameter	Screen Field	Value	Comments
rectype	Recognition Type	WHOLEWORD	—
filter	Speech filter	no	—
configfile	Speech configuration file	default	**/vs/sproxy/cfg/SRproto.cfg**
protocol	Speech protocol	default	—
baseport	Base port	2345	—
share	Share Base Port?	no	—

Administering Proxy Text-to-Speech

The same basic steps for administering Proxy Text-to-Speech are followed from whatever interface you use.

Using the Web Administration interface

1. Assign TTS system parameters.

   a) Go to the Speech Proxy Administration screen (Feature Packages > Speech Administration > Administration).

   b) Choose Text-to-Speech Configuration.

   c) Choose **Assign Text-to-Speech**.

   The browser displays the Assign Text-to-Speech Configuration screen.

   d) Choose **Assign Text-to-Speech System Parameters**.

   e) Enter a **Default Voice Tag** (as provided by the third-party vendor's TTS software) and click **Submit**.

2. Assign the TTS type.

a) Go to the **Assign Text-to-Speech Configuration** screen (see Steps 1a through 1c above, or use your browser's **Back** button, or click the **Cancel** button on the screen).

b) Choose **Assign Text-to-Speech Type**.

c) Select a **Text-to-Speech Type** and click **Submit**.

d) Enter the **Speech protocol** and **Speech configuration file** for the TTS type you selected in the previous screen.

e) Indicate whether the **Port Supports All Voices**.

f) Click **Submit**.

3. Assign a server to the TTS type.

Note:
See Special considerations for PTTS on page 37 to determine whether or not to administer the ports or Base Port, or to share Base Port fields for the TTS type.

a) Go to the **Assign Text-to-Speech Configuration** screen (see Steps 1a through 1c above, or use your browser's **Back** button, or click the **Cancel** button on the screen).

b) Choose **Assign Text-to-Speech Server**.

c) Select the **Text-to-Speech Type** you assigned in Step 2 or another assigned TTS type and click **Submit**.

d) Fill in the fields for the server and click **Submit**.

Note:
The number of ports entered on this screen must be no greater than the capacity of the server.

4. Assign a voice to the TTS type and server.

Note:
See Special considerations for PTTS on page 37 to determine whether or not to administer the voice for the TTS type.

a) Go to the **Assign Text-to-Speech Configuration** screen (see Steps 1a through 1c above, or use your browser's **Back** button, or click the **Cancel** button on the screen).

b) Choose **Assign Text-to-Speech Voice**.

c) Select the **Text-to-Speech Type** you assigned in Step 2 or another assigned TTS type and click **Submit**.

d) Select the server you assigned in Step 3 or another assigned server and click **Submit**.

e) Fill in the fields for the voice and click **Submit**.

5. Stop and restart the voice system (see Stopping and starting the voice system on page 24).

Using the command-line interface

1. Assign TTS system parameters using the tts assign command.
2. Assign the TTS type using the **tts assign** command.
3. Assign the server to a TTS type using the **tts assign** command.
4. Assign a voice to the server using the **tts assign** command.
5. Stop and restart the voice system (see Stopping and starting the voice system on page 24).

See also

- Proxy Text-to-Speech feature
- Text-to-Speech configuration screens

Special considerations for PTTS

Below are recommended values for command parameters and field values in Web Administration screens.

Administration of Proxy Text-to-Speech (PTTS) on the Avaya IR system depends on the speech engine you are using. Below are recommendations and information about administration for several of the speech engines that Avaya supports.

The column headings are described in the following table:

Column heading	Description
Parameter	The name of a parameter of the tts command
Screen field	The field in the Assign Text-to-Speech Configuration screens that is equivalent to the parameter
Value	The recommended value for the parameter and the screen field
Comments	Additional information and recommendations

Administering TTS with the default configuration

Note:
There are currently no Text-to-Speech vendors that use the default configuration. However, this configuration works for any vendors that supply a Text-to-Speech engine that works with the Avaya Proxy Text-to-Speech software.

Parameter	Screen field	Value	Comments
defaultvoice	Default Voice	—	Depends on the Text-to-Speech software used
configfile	Speech configuration file	default	**/vs/sproxy/cfg/TTSproto.cfg**
protocol	Speech protocol	default	**/vs/sproxy/lib/defaultTTSProxy.so.1**
allvoice	Port Supports All Voices?	yes	—
baseport	Base Port	2222	Hard-coded in Avaya Proxy Text-to-Speech software

Note:
Do not administer voice parameters.

Administering TTS for SpeechWorks Speechify

Parameter	Screen Field	Value	Comments
defaultvoice	Default Voice	mara	For example — or another voice supplied by Speechify
configfile	Speech configuration file	**/vs/sproxy/lib/spcfTTSProxy.so.1**	—
protocol	Speech protocol	**/vs/sproxy/cfg/spcfTTSproto.cfg**	—
allvoice	Port Supports All Voices?	no	—
ports	Ports	—	Applies to server. Do not administer *ports*
baseport	Base Port	—	Applies to server. Do not administer *baseport*

Parameter	Screen Field	Value	Comments
share	Share Base Port?	—	Applies to server. Do not administer
voicebaseport	Base Port	5555	Applies to voice. This is the default port number for mara voice. You can change this number on the server side. The number administered here has to be consistent with the number administered on the server side
voiceshare	Share Base Port?	yes	Applies to voice
language	Language	en-US|en-GB|fr-FR|es-MX|es-ES|it-IT|de-DE|ja-JP	Applies to voice ports

Administering switch interfaces

Calls come into the system through switch interfaces (or "cards"). These calls either use digital telephony signals or Voice over IP (VoIP) signals. The system must be told what kinds of signals are coming into each card.

Administration of the switch interfaces typically involves:

1. Selecting a type of signal (digital or VoIP).
2. Displaying assignments of signals to cards to find out the current configuration.
3. Assigning the signal type to a card. This includes defining the characteristics (parameters) of the particular signal that is coming into the card.
4. Stopping and restarting the voice system.

Administering digital interfaces

Using the Web Administration interface

To administer digital interfaces using Web Administration:

1. Display the current assignments.
   a) Choose Configuration Management > Switch Interfaces > Digital Interfaces from the main menu.

      The browser displays the Digital Interfaces screen.

   b) Choose **Protocols**.

      The browser displays the Digital Interfaces Protocols screen.

   c) Choose **Display Assignments**.

      The browser displays a list of currently assigned cards and their associated protocols.

2. Assign a protocol.
   a) Go back to the **Digital Interfaces Protocols** screen (see Steps 1a and 1b or use the **Back** button on your browser).

   b) Choose **Assign Card**.

c) Choose a digital protocol.

d) Fill in the fields on the **Assign Card** screen and click **Submit**.

These fields include the **Card** you want to assign the protocol to, along with information specific to the protocol.

Note:
If no cards appear in the **Card** field, there are no unassigned cards for the type of card.

3. Stop and restart the voice system (see Stopping and starting the voice system on page 24).

Using the command-line interface

To administer digital interfaces using the command-line interface:

1. Use the nms assign command.
2. Stop and restart the voice system (see Stopping and starting the voice system on page 24).

Switch administration for ISDN

Following are a group of guidelines to direct the configuration of ISDN on a network switch connected to an Avaya IR system already configured for ISDN. These are general guidelines and do not pertain to any particular network switch.

Configuration of ISDN where trunks are attached to an NMS card and each trunk contains its own D-channel

In this case, there is no NFAS (non-facility associated signaling) involved:

- Trunk interface identifiers or NAI (network access identifier) values are assigned the value of the trunk (for example: trunk 0 has NAI or interface identifier of 0, trunk 1 has NAI or interface identifier of 1, and so on).
- The network switch should be configured so that level 3 packets between the Avaya IR system and the network switch which contain a *Channel Identification IE* have the *Interface Identifier Present* field set to *Interface Implicitly Identified*.
- Should the switch not allow implicit interface identification, the *Interface Identifier* field of the *Channel Identification IE* should be set to the number of the trunk over which the

packet travels. From the network switch, this may be “fixing the interface number” to a specific value.

Configuration of ISDN where trunks are attached to an NMS card and one trunk contains the D-channel

In this case, there is NFAS:

- The NFAS group number must be set and matched up on both the network switch and the Avaya IR system.
- The first trunk to the Avaya IR system must contain the D-channel. The second trunk to the Avaya IR system should be included in the NFAS group and contain only B-channels.
- An NFAS group cannot span multiple NMS cards, so verify that the network switch is set up accordingly.
- The first trunk's NAI value is 0, and the second trunk's NAI is 1. The network switch must match these values.

Administering Voice over IP

Using the Web Administration interface

To administer Voice over IP using the Web Administration interface:

1. Display the current assignments.

   a) Go to the Voice over IP screen (Configuration Management > Switch Interfaces > Voice over IP).

   b) Choose **Display Assignments**.

      The browser loads a list of cards and the associated protocols.

2. Decide which card you will assign to a signal.
3. Assign the card to the signal.

   a) Go back to the **Voice over IP** screen (see Step 1a or use the **Back** button on your browser).

   b) Choose **Assign Card**.

   c) Fill in the fields on the **Assign Card** screen, and click **Submit**.

4. Stop and restart the voice system (see Stopping and starting the voice system on page 24).

Using the command line interface

To administer Voice over IP using the command-line interface:

1. Use the voip assign command.
2. Stop and restart the voice system (see Stopping and starting the voice system on page 24).

See also

- Configuring DEFINITY for VoIP
- Voice over IP feature

Administering VoiceXML

VoiceXML administration uses a combination of command-line commands and editing of configuration files, such as defaults.xml and default.cfg.

Assigning AVAYAVXI service to channels or numbers

The AVAYAVXI service acts as the main VoiceXML application that provides the dispatching function for calls coming into the voice system. To enable the AVAYAVXI service, you assign it to the channels or numbers you want to use for VoiceXML applications.

Note:
Make sure that the channels and numbers you use for your applications are the same ones to which you assigned the AVAYAVXI service. Your application fails if you use different channels or numbers.

The procedures below show how do a basic assignment of the AVAYAVXI service to a:

- Channel
- Number, using the Dialed Number Identification Service (DNIS)
- Number, using Automatic Number Identification (ANI) service

For detailed information on the **assign service** command, see assign service/startup command.

Note:
If other services on the Avaya IR system have been (or are) assigned with the **startup** option, Avaya recommends that you assign the AVAYAVXI service with the **startup** option.

Channel assignment

To assign the AVAYAVXI service to a channel:

1. At the command prompt, type **assign service AVAYAVXI to chan *number*** where *number* is the channel you want to assign. Press **Enter**.
2. Test the service assignment by following the test procedure below.

DNIS assignment

To assign the AVAYAVXI service to a DNIS number:

1. At the command prompt, type **assign service *DNIS_SVC to chan *range*** where *range* is the range of channels the DNIS service is assigned to. Press **Enter**.
2. Type **assign service AVAYAVXI to dnis *number*** where *number* is the DNIS you want to assign. Press **Enter**.
3. Test the service assignment by following the test procedure below.

ANI assignment

To assign the AVAYAVXI service to an ANI number:

1. At the command prompt, type **assign service AVAYAVXI to ani *number*** where *number* is the ANI you want to assign. Press **Enter**.
2. Test the service assignment by following the test procedure below.

Testing the service assignment

To test the AVAYAVXI service assignment, call one of the numbers to which you assigned AVAYAVXI.

If no VoiceXML applications have been assigned to the number you called, AVAYAVXI returns an audio message stating that there are no applications assigned to the number. If you hear this message, you have successfully assigned the AVAYAVXI service.

Administration commands for VoiceXML

To manage the assignment of VoiceXML applications to channels and numbers, you use the following command-line commands:

- vxmlassign
- vxmldelete
- vxmldisplay

To assign VoiceXML applications, you specify the starting page of your VoiceXML application and assign it to the appropriate channels or numbers (DNIS or ANI).

Note:
Make sure the channels and numbers you use for your applications are the same ones to which you assigned the AVAYAVXI service. Your application will fail if you use different channels or numbers.

Specifying starting pages

Starting pages can be local files or they can be remote files located on the Web. Local files are referenced using a URI that begins with **file://**. Local files are located in the **/voice1/vxml/apps/*application*** directory where <*application*> is the name of your VoiceXML application. For example, the starting page for the **widget** application would be **file:///voice1/vxml/apps/widget/starting_page.vxml**.

Web files are referenced using a URI that begins with **http://** and can be located on any Web server visible to the Avaya IR VoiceXML Interpreter. For example, the starting page for the **widget** application the Web server **voiceserver.com** would be **http://voiceserver.com/widget/starting_page.vxml**.

Testing VoiceXML with TTS or NLSR

If you are using Proxy Text-to-Speech (PTTS) or Natural Language Speech Recognition (NLSR) with your VoiceXML application, you can test the proxy connection to the TTS or NLSR servers using the test document, **vxmlFeatureTest.vxml,** provided as part of the VoiceXML feature. This document is set up to prompt the caller with a test and provide feedback that indicates the software is working properly.

To test the proxy for PTTS or NLSR:

1. At the command line, enter **vxmlassign uri file:///vs/data/vxml/vxmlFeatureTest.vxml chan *range*** where *range* is the range of channels you want to assign to the test document, such as 0-23.
2. Place a call to phone number in the assigned channel range.

   If the system fails to answer, assign the test document again and make sure the AVAYAVXI service has been assigned to the same channel range.
3. When the system answers, press **1** to test TTS or **2** to test NLSR.
   - If you press 1, the system speaks test that says the PTTS software is working.
   - If you press 2, the system prompts you to speak two digits, such as *4* and *8*. Speak the two digits. If the NLSR software is working correctly, the system speaks the two digits back to you (using PTTS). If you are not using PTTS, the results of the test are written to the as AVB013 message in the Message Log Report.
4. Hang up.

VoiceXML properties and event handling

The property and event handling defaults for VoiceXML applications running on Avaya IR are specified in the **/vs/data/vxml/defaults.xml** file. All applications use the values set in this file unless otherwise specified in a lower-level document. For example, an application document can specify its own property values and override the values set in the **defaults.xml** file.

Property values in defaults.xml

The **property** element is used to specify certain platform behaviors, such as speech recognition parameters. The **defaults.xml** file specifies the following default properties and values:

```
<property name='xml:lang'     value='en-US'/>
<property name='confidencelevel'  value='0.5'/>
<property name='sensitivity'    value='0.5'/>
<property name='speedvsaccuracy'  value='0.5'/>
<property name='termtimeout'    value='0s'/>
<property name='termchar'     value='#'/>
<property name='bargein'      value='true'/>
<property name='caching'      value='fast'/>
<property name='audiofetchhint'  value='prefetch'/>
<property name='documentfetchhint' value='safe'/>
<property name='grammarfetchhint' value='prefetch'/>
<property name='objectfetchhint'  value='prefetch'/>
<property name='scriptfetchhint'  value='prefetch'/>
<property name='inputmodes'    value='dtmf voice'/>
```

See the VoiceXML specification, in the VoiceXML section of the W3C Web site see http://www.w3.org/voice", for information on the purpose of each of these properties and on how the values affect the system.

To change these properties to meet the requirements of your VoiceXML application, edit the **defaults.xml** file or specify the property values in your application documents using the **property** element.

Any changes you make to the defaults.xml file are not effective until the Avaya VXI process has been restarted. The easiest way to restart the Avaya VXI process is to stop the voice system (using the **`stop_vs`** command) and start it again (using the **start_vs** command). For more information on how to use these commands, see start_vs command and stop_vs command.

Event handling in defaults.xml

The **defaults.xml** file specifies how to handle certain types of events that may occur during the course of a VoiceXML application, if the application itself does not specify how to handle them.

The Avaya Voice Browser (AVB) provides default handling for the following types of events:

Type of event	Description of event	By default the system...
Cancel	The user has asked to cancel playing of the current prompt	Does nothing
Exit	The user has asked to exit	Exits the application
Help	The user has asked for help	Plays an audio file informing the user that no help is provided. On the fifth instance, exits the application.
No input	The user has not responded within the timeout interval	In the first four instances, provides a series of escalating responses ranging from reprompting on the first instance to playing an audio file informing the user that the system cannot hear input. On the fifth instance, exits the application.
No match	The user has input something, but it was not recognized	In the first three instances, plays a series of escalating responses requesting the user to provide input again. On the fourth instance, exits the application.
Telephone disconnect	The user has hung up	Exits the application
Error	An application fatal error has occurred	Attempts to log information about the error, plays an audio file informing the user that a serious error has occurred, and exits the application.

If you plan to use the default event handling specified in the **defaults.xml** file, you may want to record your own audio files to use for each type and instance of certain events. Copy the audio files to the **/voice1/vxml/apps** directory and edit the **defaults.xml** file to reference the new audio recordings.

Any changes you make to the **defaults.xml** file are not effective until the Avaya VXI process has been restarted. The easiest way to restart the Avaya VXI process is to stop the voice system (using the **stop_vs** command) and start it again (using the **start_vs** command). For more information on how to use these commands, see start_vs command and stop_vs command.

Using the default.cfg file

The **/vs/data/vxml/default.cfg** file contains configuration data for the AvayaVXI process. Under most circumstances, you do not need to make changes to this file. However, there are a few situations in which you must open this file and edit the value of a configuration setting.

Note:
Any changes you make to the **default.cfg** file are not effective until the Avaya VXI process has been restarted. The easiest way to restart the Avaya VXI process is to stop the voice system (using the **`stop_vs`** command) and start it again (using the **start_vs** command). For more information on how to use these commands, see start_vs command and stop_vs command.

Increasing the loop count

The number of times that a VoiceXML application can loop through different form items is specified by the client.vxi.maxLoopIterations parameter in the **default.cfg** file. The default is **1000**, which should be enough for most applications. However, if an application has a legitimate reason to have more loops, you can increase the value of this parameter.

Transfer configuration requirements

With VoiceXML you cannot do a blind transfer (<transfer bridge="false" ....>) over PRI. The call can come in over PRI, but you must set the outdial signaling group transfer parameter (client.tel.outdialgroup in the **default.cfg** file) to a signaling group that is line-side T1, or loop start. Note that the entire signaling group used for the transfer must be line-side T1 or loop start, since any available resource in the signaling group could be used for the transfer.

For bridge transfer (<transfer bridge="true" ....>), PRI is supported.

When using the <transfer> element, the **destexpr** attribute supports the **tel** URL scheme defined in the Internet standard RFC2806, "URLs for Telephone Calls." For more information, see **http://www.ietf.org/rfc/rfc2806.txt**.

Caching parameters

You can set the **client.inet.cacheEntryExpTimeSec** parameter in the **default.cfg** file to specify the number of seconds used to determine expiration time when no other expiration time is available for a cache entry. For example, this parameter would be used if the VoiceXML document does not provide metadata fields for **Expires** or **Last-Modified** in the header.

The default value for this parameter is **86400**, which means that a page expires after one day.

Recognition timeout parameters

You can set the following recognition timeout parameter in the **default.cfg** file:

- completetimeout
- incompletetimeout
- timeout

The value for each timeout paramenter should be specified in seconds, for example, **timeout=10s**. For more information about these timeout parameters, refer to the VoiceXML Specification see http://www.w3.org/voice".

Avaya VXI log messages

Various levels of logging messages from the Avaya VXI process can be enabled (and disabled) in the **default.cfg** file. Logging levels are specified in the file by the parameter: **client.log.diagTag.*number***, where *number* specifies the type of log messages to generate. There are several logging levels specified in **default.cfg**. The following logging levels are particularly useful for debugging and troubleshooting purposes:

- **client.log.diagTag.3000** shows inet messages.
- **client.log.diagTag.4000** shows ECMAscript messages.
- **client.log.diagTag.5000** shows activity associated with spoken words (using text-to-speech), prompts, announcements, and other audio playback.
- **client.log.diagTag.6000** shows activity associated with grammar loading, activation, and deactivation. Also provides *best* and *value* results, which show what was trying to be matched in the grammar (best) and what the end result was (value).
- **client.log.diagTag.8000** shows errors associated with Avaya VXI activities, such as unsupported mime type.
- **client.log.diagTag.8001** shows standard pre-defined VoiceXML errors thrown by the Avaya VXI process, such as error.badfetch.
- **client.log.diagTag.8002** shows variable settings, fetch information, fetch errors, and parsing errors. This logging level is useful for tracing through application logic and finding any errors in the application syntax.
- **client.log.diagTag.9000** shows object tag messages.

By default, all of the logging parameters are disabled. A disabled logging parameter is indicated by the comment character ("#") at the beginning of the line specifying the parameter.

Enabling logging levels

To enable Avaya VXI logging levels:

1. Type **vi /vs/data/vxml/default.cfg** and press **Enter**.
2. Using the vi editing commands, remove the comment character (#) from the lines that specify the logging levels you want to enable.
3. Save and close the file.

Note:
Any changes you make to the **default.cfg** file are not effective until the Avaya VXI process has been restarted. The easiest way to restart the Avaya VXI

process is to stop the voice system (using the **stop_vs** command) and start it again (using the **start_vs** command). For more information on how to use these commands, see start_vs (command) and stop_vs (command).

Viewing log messages

Log messages are written to the **/voice1/vxml/log.txt** file or the file specified by the **client.log.filename** parameter in the **default.cfg** file.

Using the log tag

You can use the **log** tag in VoiceXML documents to generate logging or debug messages that may be helpful in troubleshooting problems with applications. Logging can also be used to monitor events and take action in applications using asynchronous event nodes.

For example, the command:

```
<log>Error: <value expr='_event'/>, <value expr='_message'/></log>
```

could be used to generate errors based on evaluating the **_event** and **_message** variables in an application.

Complete information on the **log** tag is in the VoiceXML 2.0 draft specification at the W3C Web site http://www.w3.org/TR/voicexml20/".

Messages generated by using the <log> tag are written to the same log file used by Avaya IR. The are viewable using the Message Log Report screen under the Reports Administration menu. All **log** tag messages are written at as AVB013 messages in the Message Log Report.

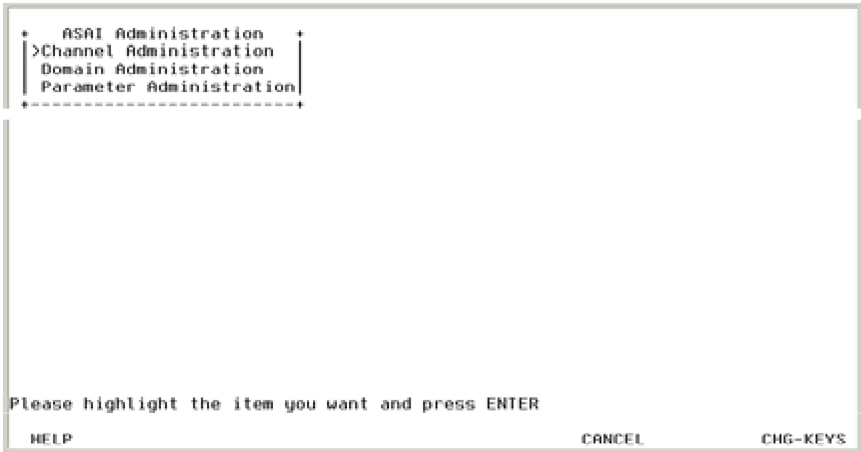
Administering ASAI

ASAI is administered from the command-line interface.

To administer ASAI:

1. At the command prompt, type **asai_adm** then press **Enter**.

The **ASAI Administration** screen is displayed.



2. From this menu, choose one of the following options:

- Channel administration (see ASAI channel administration on page 55)
- Domain administration (see ASAI domain administration on page 60)
- Parameter administration (see ASAI parameter administration on page 66)

ASAI channel administration

Channel Administration maps the voice system channels to the DEFINITY switch extension numbers. The **Channel Administration** window displays one entry for each telephony channel (voice system agent) that is a member of the voice system automatic call distributor (ACD) split.

Use the **Channel Administration** window to do the tasks described in the following table:

Task	Description
Add an ASAI channel	Assigns telephony channel as a voice system agent
Change an ASAI channel	Changes the switch extension assigned to a telephony channel
Remove an ASAI channel	Unassigns a telephony channel as a voice system agent
Log in an ASAI channel	Logs in a channel as an agent of the ACD split, enabling the channel to receive calls from the ACD
Log out an ASAI channel	Unassigns a channel from the ACD split, and prevents the ACD from delivering calls to it

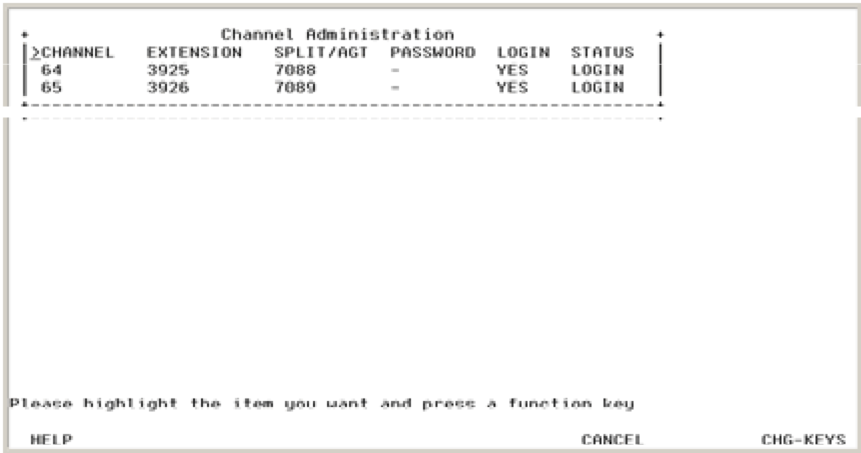
Accessing the Channel Administration window

To access the **Channel Administration** window:

1. Start at the **ASAI Administration** menu and select **Channel Administration**.

```
> Channel Administration
```

The system displays the **Channel Administration** window.



The following table describes the information on this screen:

Column Name	Description
CHANNEL	Telephony channel number on the voice system
EXTENSION	Switch extension number assigned for the channel
SPLIT/AGT	DEFINITY switch login number, either ACD extensions or Agent IDs. Maximum length of 9 characters. If the channel is an ACD split extension, the number represents the split number. If the channel is an Agent ID in an expert agent select (EAS) environment, the number represents the Agent ID.
PASSWORD	Password for the Agent ID. Channel password must match the password for the corresponding Agent ID. Maximum length of 9 characters. Dash indicates no channel password used.
LOGIN	*Yes* represents channel login for ACD split. If *No*, ACD does not deliver any calls to this channel.

Column Name	Description
STATUS	Channel maintenance state, shown as one of the following: • *broken* – A possible malfunction is detected on the line • *foos* (facility out-of-service) – The line is not functional • *hwoos* (hardware out-of-service) – The channel cannot be logged in because ASAI digital link is not operating • *logout* (logged out) – The channel has not been administered to be logged in. • *manoos* (manual out-of-service) – The channel has been taken out of service by the administrator • *netoos* (network out-of-service) – The ASAI link is up, but switch attempts to log into the channel are failing • *nonex* (nonexistent) – The channel does not exist • *login* – The voice channel is ready to receive calls from the ACD

Adding a channel entry

To add a channel entry:

1. Start at the **Channel Administration** window and press **F8** (Chg-Keys).

   The system displays the alternate function keys.

2. Press **F1** (Add).

   The system displays the **Add A Channel Entry** window.

3. Enter the telephony channel number that you want to add in the **Channel** field. The channel number must be unique.
4. Enter the switch extension number assigned to the application in the **Extension** field. The extension number must be unique.
5. If the channel is an extension in an ACD split, enter the split number in the **Split/Agent** field. If the channel is logged in as an Agent ID in an EAS environment, enter the Agent ID in the **Split/Agent** field.
6. If the channel is used for an Agent ID, enter the password of the corresponding Agent ID on the DEFINITY switch in the **Password** field.
7. Press **F3** (Save).

   The system adds the new agent line and returns to the **Channel Administration** window.

8. Complete the procedure in "Logging In a Channel" below.

Changing a channel entry

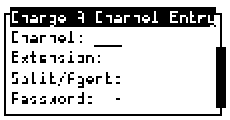
The channel must be logged out before you can change it. If the channel is not logged out, complete the procedure in "Logging Out a Channel" below.

To change the switch extension associated with a channel:

1. Start at the **Channel Administration** window and select the channel you want to change using the ↑ or ↓ keys or by typing the channel number.
2. Press **F8** (Chg-Keys).

   The system displays the alternate set of function keys.
3. Press **F2** (Change).

   The system displays the **Change A Channel Entry Window**.

4. Enter the telephony channel number extension you want to change in the **Channel** field.
5. Enter the new switch extension number in the **Extension** field.

   Note:
   The new extension number must be unique.
6. If the channel is an extension in an ACD split, enter the split number in the **Split/Agent** field. If the channel is logged in as an Agent ID in an EAS environment, enter the Agent ID in the **Split/Agent** field.
7. If the channel is used for an Agent ID, enter the password of the corresponding Agent ID on the DEFINITY switch in the **Password** field.
8. Press **F3** (Save).

   The system changes the switch extension of the selected channel and returns to the **Channel Administration** window.
9. Complete the procedure in "Logging In a Channel" below.

Removing a channel entry

The channel must be logged out before you can remove it. If the channel is not logged out, complete the procedure in "Logging Out a Channel" below.

To remove a channel entry:

1. Start at the **Channel Administration** window and select the channel you want to change using the ↑ or ↓ keys or by typing the channel number.

2. Press **F8** (Chg-Keys).

   The system displays the alternate function keys.

3. Press **F3** (Remove).

   The system displays a confirmation screen asking you if you want to remove the selected item.

4. Press **Enter**.

The system unassigns the selected channel and returns to the **Channel Administration** window.

Logging In a channel

Once the telephony channels are logged in, no manual intervention is required to log the channels back in during recovery (for example, rebooting the switch or voice system) or upon restarting the voice system.

To log in a channel:

1. Start at the **Channel Administration** window and select the channel you want to change using the ↑ or ↓ keys or by typing the channel number.

2. Press **F8** (Chg-Keys).

   The system displays the alternate set of function keys.

3. Press **F4** (Login).

   The system logs in the selected channel to the ACD and returns to the **Channel Administration** window.

Logging Out a Channel

To log out a channel:

1. Start at the **Channel Administration** window and select the channel you want to change using the ↑ or ↓ keys or by typing the channel number.

2. Press **F8** (Chg-Keys).

   The system displays the alternate set of function keys.

3. Press **F5** (Logout).

   The system unassigns the selected channel from the ACD and returns to the **Channel Administration** window.

ASAI domain administration

Use the **Domain Administration** window to:

- Add a domain to the switch domain set
- Change a voice system domain assignment
- Remove a domain from the switch domain set
- Enable a domain (place the domain in service)
- Disable a domain (take a domain out of service)

Once the domain is placed in service, no manual intervention is required to bring the domain back into service during recovery (for example, rebooting the switch or voice system) or upon restarting the voice system.

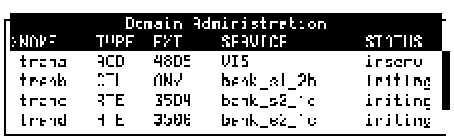
By default, the voice system updates the **Domain Administration** window every two seconds.

Accessing the Domain Administration window

To access the **Domain Administration** window:

Start at the **ASAI Administration Menu** and select **Domain Administration**.

The system displays the **Domain Administration** window.



The following table describes the columns in the **Domain Administration** window:

Column name	Description	Comments
NAME	Domain name	—

Column name	Description	Comments
TYPE	Domain type for the voice system	Must be one of the following: • ACD – Monitors calls to the corresponding split domain on the switch • VDN – Monitors calls to the corresponding VDN domain on the switch • CTL – Monitors calls transferred away from the voice system (by a voice script using the *A_Tran* action) to destinations on the switch that are not monitored by an ACD or VDN domain (for example, monitor calls transferred using *A_Tran* to miscellaneous extensions). CTL domains are defined only by the voice system and do not correspond to any domain on the switch. • RTE – Accepts Route Requests from the switch. RTE domains are defined by only the voice system and do not correspond to any domain on the switch.

Column name	**Description**	**Comments**
EXT	Extension	Must enter *any* for calls transferred to any destination not already monitored by another domain, or one of the following, depending on the domain type: • ACD switch extension – Corresponding ACD split switch extension being monitored. • VDN switch extension – Corresponding VDN switch extension being monitored. • CTL extension – Extension for which calls are being transferred by a voice system channel using the *A_Tran* action and processed by the CTL domain. Extension must correspond to an extension used in the *Destination* field of the *A_Tran* action used by an application assigned to the ASAI channel. • RTE extension – Extension that limits the processing of route requests based on the extension dialed. Only route requests for the specified extension are processed.
SERVICE	Application name that services the domain, and can be assigned to any type of domain (ACD, VDN, and so on)	*SERVICE* can be one of the following, depending on the domain type: • ACD/VDN domains – If the application, ACD or VDN, directs calls to the voice system telephony channel, you must enter the special service *VIS* . VIS service provides the ability to start voice scripts on the tip/ring channels based on the DNIS. It also provides the ability for those voice scripts to use the *A_Callinfo* and *A_Tran* action. The service can be assigned to multiple ACD or VDN domains. All channels that are administered as agents must be members of at least one ACD or VDN domain. • CTL domains – The SERVICE must be monitoring • RTE domains – The SERVICE must be routing

Column name	Description	Comments
STATUS	Domain maintenance state	Shown as one of the following: • *broken* (broken) – A virtual channel could not be allocated for the service assigned to this domain • *foos* (facility out-of-service) – The ASAI digital link is not operating • *initing* (initializing) – The service assigned to the domain is failing initialization • *inserv* (in service) – The domain is ready to receive call information from the switch • *manoos* (manual out-of-service) – The domain has not been placed into service • *netoos* (network out-of-service) – The ASAI link is up, but attempts to receive call information from the switch are failing

Adding a domain

The system supports 64 domains or fewer.

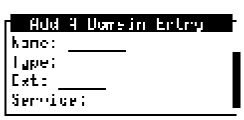
To add a domain:

1. Start at the **Domain Administration** window and press **F8** (Chg-Keys).

   The system displays the alternate function keys.

2. Press **F1** (Add).

   The system displays the **Add A Domain Entry** window.



3. Enter the domain name in the **Name** field. This is the name that has been given to the ACD on the PBX.
4. Enter the domain type in the **Type** field or press **F2** (Choices) to select from a menu. Valid choices are ACD, VDN, CTL, or RTE.
5. Enter the switch extension of the domain in the **Ext** field.

6. Enter the service for the domain in the **Service** field or press **F2** (Choices) to select from a menu. This may be any application designed and developed for use with the ASAI feature.
7. Press **F3** (Save).

   The system adds the new domain and returns to the **Domain Administration** window.
8. Complete the procedure in "Enabling a Domain" below.

Changing a domain

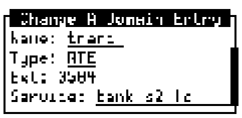
The domain must be disabled before you can change it. If it is not disabled, complete the procedure "Disabling a Domain" below.

To change a domain:

1. Start at the **Domain Administration** window and press **F8** (Chg-Keys).

   The system displays the alternate function keys.
2. Press **F2** (Change).

   The system displays the **Change A Domain Entry Window**.



3. Enter the domain type in the **Type** field or press **F2** (Choices) to select from a menu. Valid entries are ACD, VDN, CTL, or RTE.
4. Enter the switch extension number assigned to the ACD split in the **Ext** field.
5. Enter the service that specifies how the calls offered to the domain are handled by the voice system in the **Service** field or press **F2** (Choices) to select from a menu. This may be any application designed and developed for use with the ASAI feature.
6. Press **F3** (Save).
7. The system makes the specified changes to the domain and returns to the **Domain Administration** window.
8. Complete the procedure in "Enabling a Domain" below.

Removing a domain

The domain must be disabled before you can remove it. If it is not disabled, complete the procedure in "Disabling a Domain" below.

To remove a domain:

1. Start at the **Domain Administration** window and press **F8** (Chg-Keys).

   The system displays the alternate function keys.

2. Press **F3** (Remove).

   The system displays a confirmation screen, asking you if you want to remove the selected item.

3. Press **Enter**.

   The system removes the selected domain and returns to the **Domain Administration** window.

Enabling a domain

To enable a domain:

1. Start at the **Domain Administration** window and press **F8** (Chg-Keys).

   The system displays the alternate function keys.

2. Press **F4** (Enable).

   The system changes the **Status** field to *inserv*.

Disabling a domain

To take a domain out of service:

1. Start at the **Domain Administration** window and press **F8** (Chg-Keys).

   The system displays the alternate function keys.

2. Press **F5** (Disable).

   The system changes the **Status** field to *manoos*.

ASAI parameter administration

Use the **Parameter Administration** menu option to administer:

- *Connect Event* reporting to the *A_Event* variable in an application assigned to an ACD, VDN, or CTL domain
- Details displayed with the **trace dip7** command to monitor messages and events processed by the ASAI feature

Administering Connect Event reporting

To set ASAI parameters regarding connect event reporting and the level of trace detail:

1. Start at the **ASAI Administration** menu and select **Parameter Administration**:

The system displays the **ASAI Parameters** window.

2. Enter either *Connected* or *Alerting* in the **CONNECT Event** field to specify when the Connect event is reported to the A_Event action in a script assigned to an ACD, VDN, or CTL type domain. Or, you may press **F2** (Choices) to select from a menu. The default is *Connected*.
3. Enter *Low*, *Normal*, or *High* in the **Trace Detail** field to specify the amount of trace detail to display. Or, you may press **F2** (Choices) to select from a menu. The following table summarizes the **trace** command settings and the level of detail achieved with each one:

Setting	Display
Low	Information displayed about ASAI error and warning conditions
Normal	All information displayed by the Low setting, plus ASAI script action (that is, A_Callinfo, A_Tran, A_Event, and A_RouteSel)
High	All information displayed by the Low and Normal settings, plus call event descriptions received from the PBX

4. Enter the IP address or host name of the MAPD in the **IP Address** field.

5. Enter the Node ID of the Avaya IR system as administered on the MAPD in the **Node ID** field. This field contain the value from *signal01* to *signal08*.
6. Press **F3** (Save).

   The system displays the level of trace detail specified.
7. Press **F6** (Cancel) repeatedly to return to the **ASAI Administration** menu.

See also

- trace command

Creating and restoring backups

You can do a full backup or a partial backup, and you can restore any backup to the system. (This procedure assumes the system is fully operational. See Restoring the system for disaster recovery.)

Avaya recommends that you perform a full backup after the initial installation.

> ⚠CAUTION**:**
> The transfer of large backup images may slow your network performance.

Using the Web Administration interface

Backups are done using the main menu's Backup/Restore options.

To do a full backup:

1. Choose Backup from the main menu, and choose **Full Backup**.
2. Fill in the fields and click **Submit**.

To do a partial backup:

1. Choose **Backup** from the main menu, and choose **Partial Backup**.
2. Fill in the fields and click **Submit**.

To restore a backup:

1. Choose Restore from the main menu.
2. Choose **Restore** from the screen that the browser displays.

3. Fill in the fields and click **Submit**.

Using the command-line interface

- To do a full or partial backup, use the backup command.
- To restore a backup, use the restback command.

Note:
You can use the schedback command to create a cron job to schedule a backup, and you can use the delbackup command to remove backups from the cron table. Running delbackup removes the Backup entry permanently from cron.

Monitoring system operations

You can learn the current state of the system by using the System Monitor. It tells you, by channel:

- How many calls have been processed today
- What service (application) is assigned to the channel
- The service status
- The caller input
- Dialed digits

To monitor the system, use the sysmon command from the command-line interface.

Tracing a service

A trace is a record of events that have occurred on a voice channel, the voice system, or a host system. You can view this record from the command-line interface using the trace command.

Rebooting the system

Use the command-line interface to reboot the system:

Type **reboot** and press **Enter**.

Viewing licensed features

Optional features are licensed by Avaya or its third-party vendors. You can view which features can used with either the Web Administration interface or the command-line interface.

From the Web Administration interface:

Choose Configuration Management > Feature Licensing from the main menu. The browser displays the Feature Licensing screen.

From the command-line interface:

Use the RTUquery command.

Administering additional software

Any additional software that is part of systems that interact with the Avaya IR system must be administered. The software involved depends upon the features used.

Administering CVCT for CTI

You must administer the Avaya IR and the CVCT servers to make the Avaya IR a CVCT client.

To administer CVCT servers, do the following steps on each CVCT server:

1. Create a new user name for the Avaya IR system.
2. Register the user.
3. Create a device for each port of the Avaya IR system that will use CTI.

See *CentreVu Computer Telephony Release 9.1, Version 1, Telephony Services and CallVisor PC Installation* for details on how to administer the CVCT server.

Administering the system and switch for CTI

You must administer the Avaya IR and the DEFINITY PBX as follows:

1. Administer the MAPD in DLG mode. See *CallVisor PC LAN over MAPD Installation, Administration, and Maintenance*, 555-230-113.
2. Administer the Avaya IR network interface card.
3. Administer the E1 or T1 telephone lines on the PBX.
4. Assign telephone numbers (or extensions) to the ports of the Avaya IR that will use CTI.
5. Administer the DEFINITY for ASAI connectivity with the CVCT server.
6. Administer the E1 and T1 lines on the Avaya IR system.

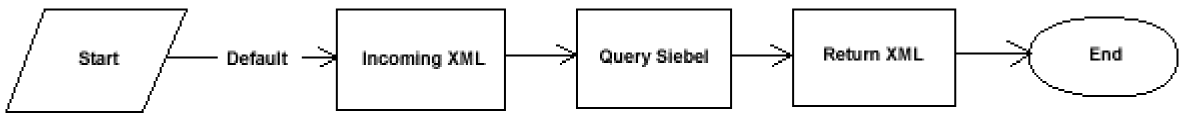
Setting up and administering a Siebel Client for CTI

If a Siebel client will be used, see *CentreVu ® CT Integration for SIEBEL ® eBusiness Applications (Release 1.1, Version 1.2.205) Client Installation Guide*. That guide will provide information about the related setup and administration of both the client and the CVCT server.

Workflows for Siebel transfer

Workflows must be created to enable the proper operations within Siebel eBusiness. One or more workflows may be used, depending on the customer's needs.

A sample workflow for a query is shown below. In this workflow, an XML document is received from the Avaya IR system, a Siebel database is queried, and an XML document is prepared and sent to the Avaya IR system.



Below is a sample workflow for an update. In this case, data is inserted into a Siebel database after Siebel eBusiness receives an XML document from the Avaya IR system. An XML document is prepared and sent to the Avaya IR system.

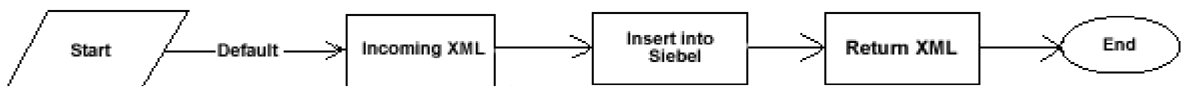


Figure 1: Siebel update workflow

Index

A

C

E

M

P

R

S

T

U

V

W