Cisco Internet Service Node (ISN) Product Description

Internet Service Node (ISN) Release 2.0

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Customer Order Number:
Text Part Number: OL-1250-02

CONTENTS

About This Guide

Purpose

This manual describes the Cisco Internet Service Node (ISN).

Audience

This document is intended for Call Center Managers, ISN System Managers, ICM/NAM System Managers, VoIP Technical Experts, and IVR application developers. Readers of this manual should already have a general understanding of the NAM product, as discussed in the Cisco Network Applications Manager (NAM) Product Description. Readers should be familiar with general ICM installation and setup procedures.

Organization

The manual is divided into the following chapters.

Chapter	Description
Chapter 1, "Introduction"	Provides an overview of Internet Service Node (ISN) features and benefits.
Chapter 2, "ISN Solution Components"	Presents additional information about the ISN solution runtime components first introduced in Chapter 1.
Chapter 3, "Prompt Recording and Distribution"	Provides an overview of ISN media file handling and information about ISN system prompts.
Chapter 4, "VoIP Routing"	Presents information about: • Using ISN and IP Phones with Cisco Call Manager. • Inbound routing and outbound routing.

Conventions

This manual uses the following conventions:

Format	Example
Boldface type is used for user entries, keys, buttons, and folder and submenu names.	Choose **Script > Call Type Manager**.
Italic type indicates one of the following: • A newly introduced term • For emphasis • A generic syntax item that you must replace with a specific value • A title of a publication	• A *skill group* is a collection of agents who share similar skills. • *Do not* use the numerical naming convention that is used in the predefined templates (for example, **persvc01**). • IF (*condition*, *true-value*, *false-value*) • For more information, see the *Cisco ICM Software Database Schema Handbook*.
An arrow (>) indicates an item from a pull-down menu.	The Save command from the File menu is referenced as **File > Save**.

Obtaining Documentation

Cisco provides several ways to obtain documentation, technical assistance, and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation on the World Wide Web at this URL:

http://www.cisco.com/univercd/home/home.htm

You can access the Cisco website at this URL:

http://www.cisco.com

International Cisco web sites can be accessed from this URL:

http://www.cisco.com/public/countries_languages.shtml

Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which may have shipped with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual subscription.

Registered Cisco.com users can order the Documentation CD-ROM (product number DOC-CONDOCCD=) through the online Subscription Store:

http://www.cisco.com/go/subscription

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/en/US/partner/ordering/index.shtml

- Registered Cisco.com users can order the Documentation CD-ROM (Customer Order Number DOC-CONDOCCD=) through the online Subscription Store:

  http://www.cisco.com/go/subscription

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, U.S.A.) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can submit comments electronically on Cisco.com. On the Cisco Documentation home page, click **Feedback** at the top of the page.

You can e-mail your comments to bug-doc@cisco.com.

You can submit your comments by mail by using the response card behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com, which includes the Cisco Technical Assistance Center (TAC) Website, as a starting point for all technical assistance. Customers and partners can obtain online documentation, troubleshooting tips, and sample configurations from the Cisco TAC website. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC website, including TAC tools and utilities.

Cisco.com

Cisco.com offers a suite of interactive, networked services that let you access Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com provides a broad range of features and services to help you with these tasks:

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

To obtain customized information and service, you can self-register on Cisco.com at this URL:

http://www.cisco.com

Technical Assistance Center

The Cisco TAC is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two levels of support are available: the Cisco TAC website and the Cisco TAC Escalation Center. The avenue of support that you choose depends on the priority of the problem and the conditions stated in service contracts, when applicable.

We categorize Cisco TAC inquiries according to urgency:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration.
- Priority level 3 (P3)—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- Priority level 2 (P2)—Your production network is severely degraded, affecting significant aspects of business operations. No workaround is available.
- Priority level 1 (P1)—Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No workaround is available.

Cisco TAC Website

You can use the Cisco TAC website to resolve P3 and P4 issues yourself, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco TAC website, go to this URL:

http://www.cisco.com/tac

All customers, partners, and resellers who have a valid Cisco service contract have complete access to the technical support resources on the Cisco TAC website. Some services on the Cisco TAC website require a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to this URL to register:

http://tools.cisco.com/RPF/register/register.do

If you are a Cisco.com registered user, and you cannot resolve your technical issues by using the Cisco TAC website, you can open a case online at this URL:

http://www.cisco.com/en/US/support/index.html

If you have Internet access, we recommend that you open P3 and P4 cases through the Cisco TAC website so that you can describe the situation in your own words and attach any necessary files.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses priority level 1 or priority level 2 issues. These classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer automatically opens a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to this URL:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

Before calling, please check with your network operations center to determine the level of Cisco support services to which your company is entitled: for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). When you call the center, please have available your service agreement number and your product serial number.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The *Cisco Product Catalog* describes the networking products offered by Cisco Systems as well as ordering and customer support services. Access the *Cisco Product Catalog* at this URL:

  http://www.cisco.com/en/US/products/products_catalog_links_launch.html

- Cisco Press publishes a wide range of networking publications. Cisco suggests these titles for new and experienced users: *Internetworking Terms and Acronyms Dictionary, Internetworking Technology Handbook, Internetworking Troubleshooting Guide,* and the *Internetworking Design Guide.* For current Cisco Press titles and other information, go to Cisco Press online at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco monthly periodical that provides industry professionals with the latest information about the field of networking. You can access *Packet* magazine at this URL:

  http://www.cisco.com/en/US/about/ac123/ac114/about_cisco_packet_magazine.html

- *iQ Magazine* is the Cisco monthly periodical that provides business leaders and decision makers with the latest information about the networking industry. You can access *iQ Magazine* at this URL:

  http://business.cisco.com/prod/tree.taf%3fasset_id=44699&public_view=true&kbns=1.html

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in the design, development, and operation of public and private internets and intranets. You can access the *Internet Protocol Journal* at this URL:

  http://www.cisco.com/en/US/about/ac123/ac147/about_cisco_the_internet_protocol_journal.html

- Training—Cisco offers world-class networking training, with current offerings in network training listed at this URL:

  http://www.cisco.com/en/US/learning/le31/learning_recommended_training_list.html

Introduction

This chapter contains an overview of Internet Service Node (ISN) features and benefits.

What is the ISN?

The ISN is a Web-based, AVVID-compatible platform that provides carrier-class Interactive Voice Response (IVR) and IP switching services over Voice Over IP (VoIP) networks. The ISN feature set includes:

- **IP-based switching.** ISN can transfer calls over an IP network.
- **IP-based Takeback.** ISN can take back a transferred call for further IVR treatment or transfer.
- **IP-based IVR services.** The classic prompt-and-collect functions: "Press 1 for Sales, 2 for service," etc.
- **IP-based queuing.** Calls can be "parked" on the ISN for prompting, music on hold, etc., while waiting for a call center agent to be available.
- **Compatibility with other Cisco Call Routing and VoIP products.** Specifically, the Network Application Manager (NAM) or Intelligent Contact Manager (ICM), Cisco Gatekeeper, Cisco Gateways, and Cisco IP Contact Center (IPCC).
- **Compatibility with the Public Telephone Switch Network (PTSN).** Calls can be moved onto an IP-based network for ISN treatment and then moved back out to a PTSN for further call routing to a call center.
- **Carrier-class platform.** ISN's reliability, redundancy, and scalability allows it to work with Service Provider and large Enterprise networks.

The IVR problem / The ISN Solution

For many years, IVRs were the primary technology base for automated user transactions for businesses. Much of that role has been passed to the Web, but the IVR has remained its own "backwater" of proprietary technology.

The Internet Service Node implements an IVR using Web technology. To the ISN, an IVR is just a Web application with a special browser—called the *Voice Browser*—that delivers Web pages as voice.

Figure 1-1 illustrates the ISN VoIP solution. The ISN components—shown centered in the "cloud"—consist of the following:

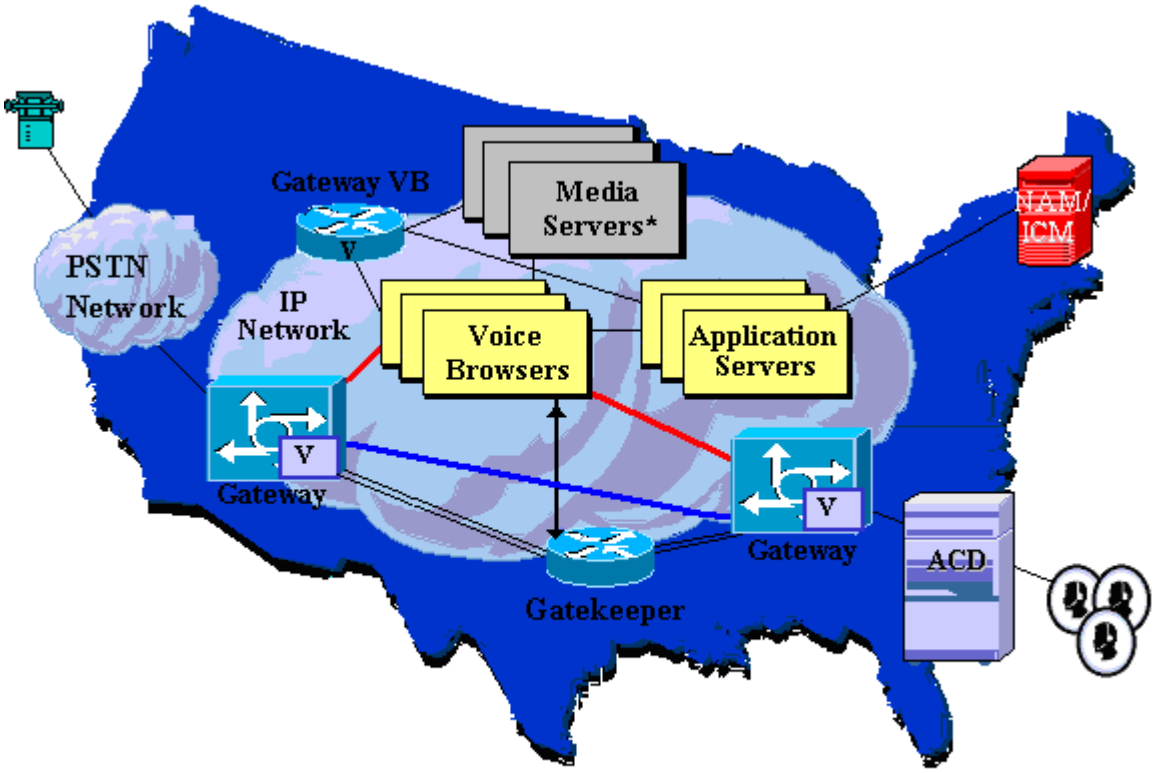
- **Application Server**. A Web Server application which interprets messages from the Cisco ICM software and generates VXML documents that it uses to communicate with the Voice Browser.
- **Voice Browser**. Accepts incoming PSTN and IP telephone calls, makes requests to the Application Server, and acts upon VXML commands received from the Application Server.

The prompt files to be played to the caller reside on the **Media Server**, an off-the-shelf Web Server. The Voice Browser uses HTTP requests to retrieve the prompt files it needs.

Independent of the ISN's components, the **NAM/ICM** is the cornerstone for making call routing decisions as they progress through the network. To the NAM/ICM, the ISN is simply a VRU peripheral; this is true whether the network is classic PSTN, VoIP, or a combination of both.

In the ISN solution, the **Gateway** serves to convert PSTN calls to H.323 VoIP. Those calls are routed to a destination endpoint—the Voice Browser—using a Gatekeeper or another mechanism available to the Gateway. The Gateway passes information such as the called number to the ISN's Voice Browser, so an application can be chosen.

Figure 1-1 The ISN VoIP Solution



* Media Servers: ASR, TTS, HTTP (prerecorded prompts)

The ISN has full control of call routing through the whole VoIP networking cloud. This is shown in Figure 1-1, where the ISN takes a call that enters the IVR from the PSTN on the West Coast and switches it under NAM/ICM direction to an agent on an ACD in Florida. In doing so, it enables the NAM/ICM to direct the IP voice connection (represented by the thick blue line) across a coast-to-coast IP network.

At the same time, the Voice Browser retains call control (represented by the thick red lines) on the two Gateways, so the NAM/ICM system can rearrange the call in the IP network if the agent wants to transfer the call. Specifically, this means that the NAM/ICM's Network Transfer feature (which captures an agent transfer request on an ACD and rearranges the TDM network if the target agent is remote) can migrate directly to the IP world.

ISN Deployment Models

ISN Version 2.0 provides three deployment models, depending on your ASR/TTS, VRU transfer, and queuing needs:

- **Advanced Speech.** For customers who:
  - Do not need to use the ISN to control queued calls
  - Do not need use the ISN to perform subsequent agent transfer
  - Do not need to outpulse digits for Transfer Connect
- **Queue and Transfer.** For customers who:
  - Want to prompt/collect **without** using ASR/TTS
  - Use the ISN to control queued calls
  - Use the ISN to perform subsequent agent transfer
  - Need to outpulse digits for Transfer Connect
- **Comprehensive IVR.** For customers who:
  - Want to prompt/collect using ASR/TTS
  - Use the ISN to control queued calls
  - Use the ISN to perform subsequent agent transfer
  - Need to outpulse digits for Transfer Connect

Table 1-1 provides a summary of the capabilities of each of these ISN types.

Table 1-1 ISN IVR Functionality

ISN IVR Model	ASR/TTS Support?	Queue Point Control?	Network Transfer Support?	Outpulse Digits?
Advanced Speech IVR	Yes	No	No	No
Queue and Transfer IVR	No	Yes	Yes	Yes
Comprehensive IVR	Yes	Yes	Yes	Yes

The sections that follow provide examples of call flows for each of these models.

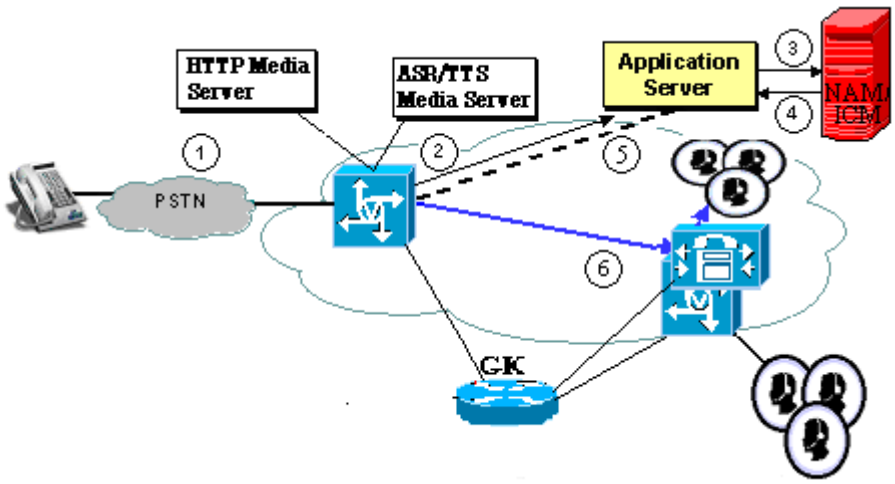
Note For detailed information about each ISN IVR functional model—including configuration instructions—see Appendix C, "ISN Deployment," in the *Cisco ISN Configuration and Administration Guide*.

Advanced Speech IVR ISN

The Advanced Speech IVR ISN functional model is for customers who desire ASR/TTS, but do not need to control queued calls or to outpulse digits for Transfer Connect. In this configuration, the ISN Voice Browser is not required, using the VXML client on the application gateway instead, and the ISN consists solely of the Application Server component.

Figure 1-2 shows the general architecture of the Advanced Speech IVR ISN.

Figure 1-2 The Advanced Speech IVR ISN Solution



The call flow in Figure 1-2 is as follows:

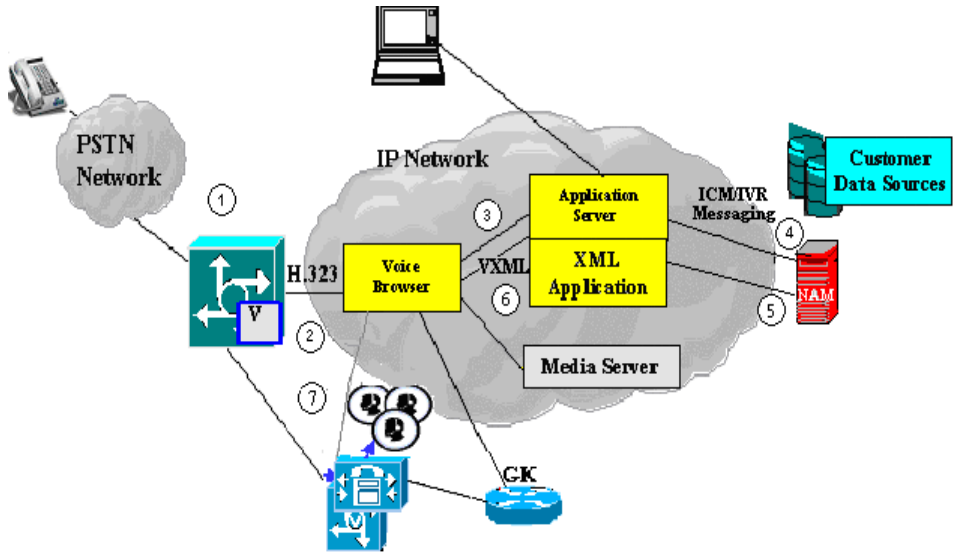
1. The call arrives from the PSTN network to the Gateway.
2. The Gateway treats the call using VXML processing and informs the Application Server that a call has arrived.
3. The ISN Application Server requests instructions of the NAM/ICM.
4. The NAM/ICM consults the customer database/application as needed and determines which scripts to run and what information to communicate. The NAM/ICM passes this information to the Application Server.
5. The ISN uses the Gateway's prompt/collect capabilities, possibly with ASR/TTS.
6. If the NAM/ICM instructed that the call should be transferred, the ISN requests the Gateway to transfer the call to the endpoint (either a traditional ACD or IPCC).

Queue and Transfer IVR ISN

The Queue and Transfer IVR functional model is for customers who have no need of ASR/TTS, but want the ISN Version 1.0 functionality plus the non-ASR/TTS Version 2.0 features — enhancements to grammar, currency, IP phone origination, 3640/3660/5350/5400 support) — who need to use the ISN to control queued calls or to perform subsequent agent transfer, or who need to outpulse digits for Transfer Connect.

Figure 1-3 shows the general architecture of the Queue and Transfer IVR ISN.

Figure 1-3 The Queue and Transfer ISN Solution



The call flow in Figure 1-3 is as follows:

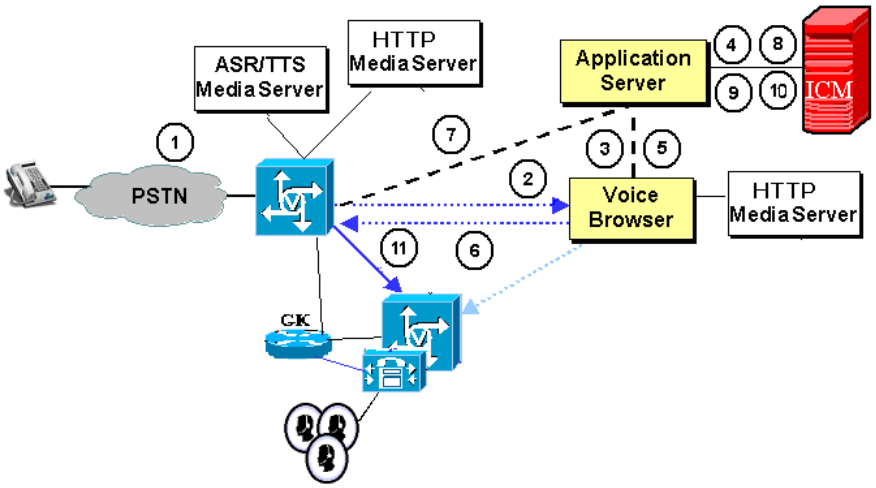
1. The call comes into the PSTN network to the a Gateway. (The call may have been pre-routed by NAM/ICM to the Gateway.)
2. The Gateway notifies the ISN Voice Browser of the call.
3. The ISN Voice Browser informs the ISN Application Server that a call has arrived.
4. The Application Server requests instructions of the NAM/ICM.
5. The NAM/ICM consults the customer database/application as needed and determines which scripts to run and what information to communicate. The NAM/ICM passes this information to the Application Server.
6. The Application Server creates a VXML page, which tells the Voice Browser what to do. The Voice Browser retrieves any media files or announcements from the Media Server.
7. The Voice Browser collects DTMF digits and plays prompts or announcements over the packetized voice stream back through the originating Gateway to the caller.
8. If the NAM/ICM instructed that the call should be transferred, the ISN requests the Gateway to transfer the call to the endpoint (either a traditional ACD or IPCC).

Comprehensive IVR ISN

The Comprehensive IVR functional model is for customers who desire ASR/TTS and who need to use the ISN to control queued calls or to perform subsequent agent transfer, and who need to outpulse digits for Transfer Connect.

Figure 1-4 shows the general architecture of the Comprehensive IVR ISN.

Figure 1-4 Comprehensive IVR ISN Solution



The call flow in Figure 1-4 is as follows:

1. A call arrives from PSTN network to the Gateway.
2. The Gateway notifies the ISN Voice Browser of the call.
3. The ISN Voice Browser informs the ISN Application Server that a call has arrived.
4. The Application Server requests instructions of the NAM/ICM.
5. As a result of the ICM Network VRU configuration for IVR treatment the Application Server creates a VXML page, which tells the Voice Browser to transfer the call to an IP port on the Gateway.

   Note Figure 1-4 shows the same Gateway but a separate Gateway could be used.

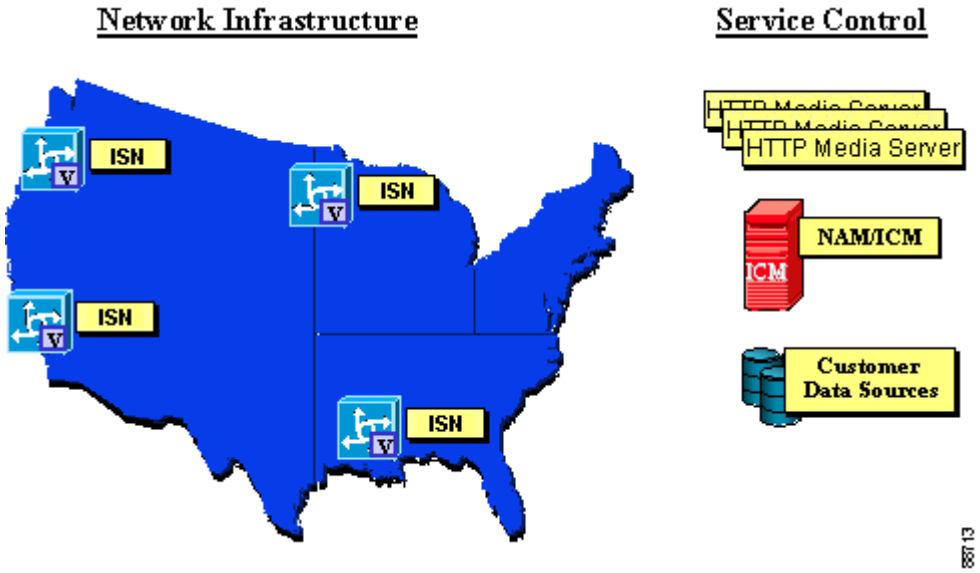
6. The Voice Browser transfers the call and retains call control for future transfers.
7. The Gateway issues a VXML request to the ISN Application Server.
8. The ISN Application Server requests instructions of the NAM/ICM.
9. The NAM/ICM consults the customer database/application as needed and determines which scripts to run and what information to communicate. The NAM/ICM passes this information to the Application Server.
10. The ISN uses the Gateway's prompt/collect capabilities, possibly with ASR/TTS.
11. If the NAM/ICM instructed that the call should be transferred, the ISN requests the Gateway to transfer the call to the endpoint (either a traditional ACD or IPCC).

ISN Network Deployment Options

The ISN is not just a better way to build an IVR; it fundamentally changes the IVR business, the ACD business, and the dynamics of network control. The best way to understand this is to consider the ways the ISN technology can be deployed. There are essentially two distinct deployment scenarios: *Hosted environment (*NAM and ICM) and *Enterprise environment*.

Once Gateways and Voices Browsers are set up in the network infrastructure, as shown in Figure 1-5, then prompting and queuing functions of an IVR or ACD can be provided in an extremely efficient manner: close to the call origin and under direct control of the service provider.

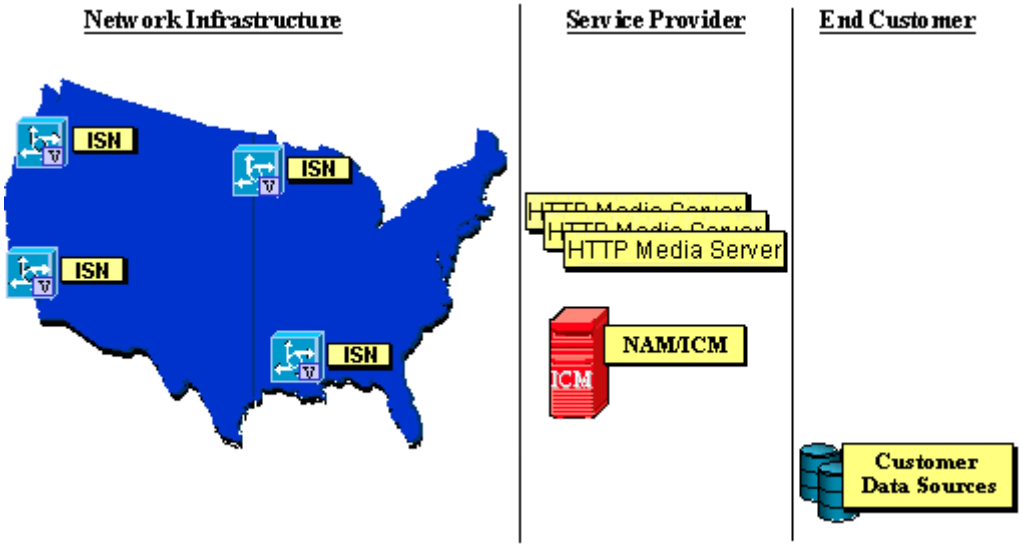
Figure 1-5 ISN Infrastructure



Note ISN Version 2.0 requires that the Voice Browser, Application Server, and ICM software be installed on a secure network.

Figure 1-6 shows a Hosted environment deployment.

Figure 1-6 Hosted Deployment

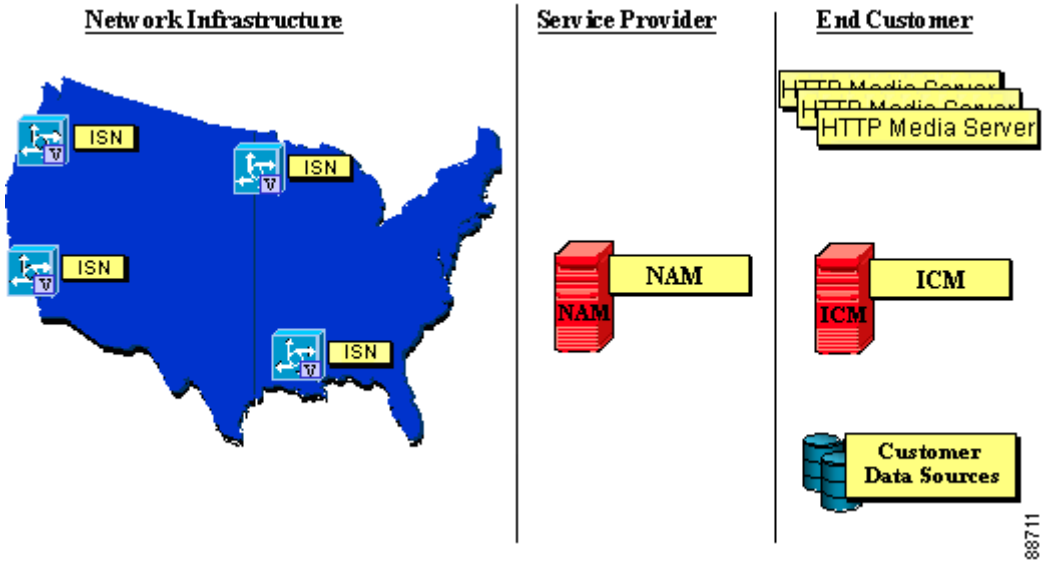


In Figure 1-6, the only thing that is retained on the customer side is the customer's own data. The the Gateways, the ISNs, the ASR/TTS servers, the HTTP media servers, and the NAM/ICM features are all provided on a shared-tenant basis in the network. What is remarkable in this case is the extent to which the fully-hosted service is understood and accepted technology. For both the Application Servers and Media Servers the deployment model is Web hosting, which is known technology in terms of security, reliability, and user control. Similarly, the NAM/ICM technology has been developed and deployed to support the same user control, reliability, and manageability in both premise-based and network-based applications.

The bottom line: There is no barrier to scalability, security, or reliability for this technology to provide the fully-hosted service outlined in Figure 1-6.

Figure 1-7 shows a Enterprise environment deployment.

Figure 1-7 Enterprise Deployment



In Figure 1-7, the customer retains the ICM software and HTTP Media Servers, while the Gateways, ISNs, ASR/TTS servers, and NAM software are in the network. In this method, the end customer controls and manages all the business logic, while the Gateways, ISNs, and ASR/TTS servers provide the infrastructure.

Note HTTP Media Servers can be physically co-located with the Voice Browsers to reduce network bandwidth demands.

ISN Scalability and Fault-Tolerance

ISN's Web-based architecture allows the use of Web methods to handle issues like fault-tolerance, scalability, etc. With the ISN:

- Scaling, fault-tolerance, and file distribution are standard Web issues, with standard solutions.
- By making Gateways, Voice Browsers, Application Servers, and Media Servers available in the IP network, the network itself enables IVR services and switching for carrier or customer Web applications.
- The ability to place Gateways, Voice Browsers, and Media Servers at the edges of the IP network reduces the bandwidth demands on the central part of the network itself.

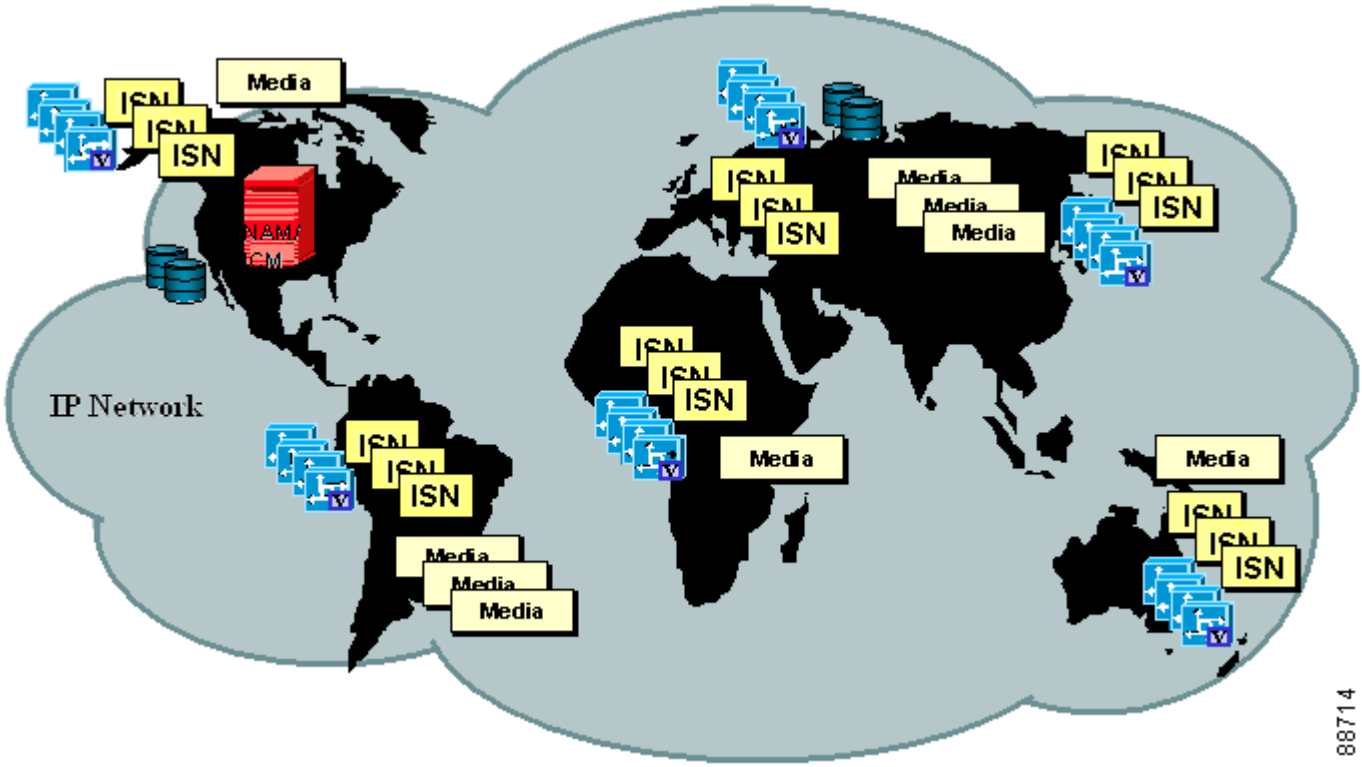
The ISN can accommodate internal fail-over in case a particular component is having difficulties or needs to be upgraded. For example, if an ISN Voice Browser or Gateway Voice Browser is looking for an Application Server and cannot connect with its normal Application Server, it can fail over to a different Application Server.

When using the Gateway for IVR treatment, a content switch may be used to load balance and provide failover capabilities between the Gateway and Application server and between the Gateway and the media server (ASR/TTS/HTTP).

Alternate routing methods are also available. Cisco Gateways can be configured to present calls to a primary Voice Browser, but if the primary Voice Browser is not available the VoIP network can route new calls to an alternate Voice Browser.

Figure 1-8 illustrates ISN's scalability and fault tolerance, where farms of Gateways, Voice Browsers, Application Servers, and Media Servers are distributed throughout the network.

Figure 1-8 ISN Scalability



Putting It All Together: Deployment Decision-Making

There are several different architectures available for ISN-based Network VRU solutions. This section describes questions you should ask when planning the ISN deployment model that would best suit your needs.

Before You Begin: A Note About IVR Types

Essentially, the NAM/ICM categorizes IVRs into one of two types:

- **Intelligent Peripheral IVRs**, where—under NAM/ICM control—the carrier network routes calls to the IVR and then removes calls from the IVR for delivery to the NIC. With Intelligent Peripheral IVRs, once the IVR's prompting or queuing treatment has been completed, the IVR typically has no further role to play for that call.
- **Service Node IVR's**, where—following prompting/queuing treatment—the Service Node IVR initiates call delivery to agents, who are under NAM/ICM control. When functioning as a Service Node IVR, the ISN can stay involved with a call even after it has been transferred to another VoIP endpoint.

The ISN can act as either IVR type. However, to be able to access all the benefits of the ISN functionality, deploy the ISN as a Service Node IVR.

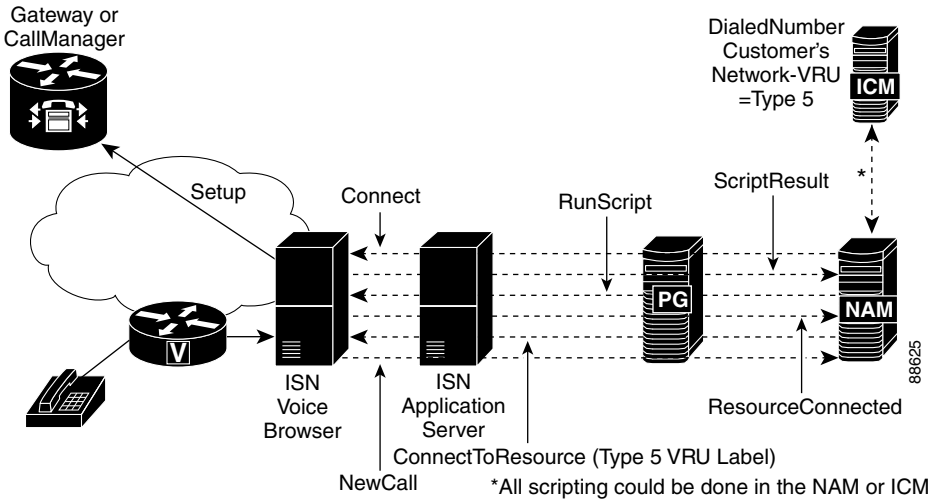
Initial Planning

First, ask yourself these questions:

- **Is the ISN acting as the routing client as well, or is there a separate routing client?**

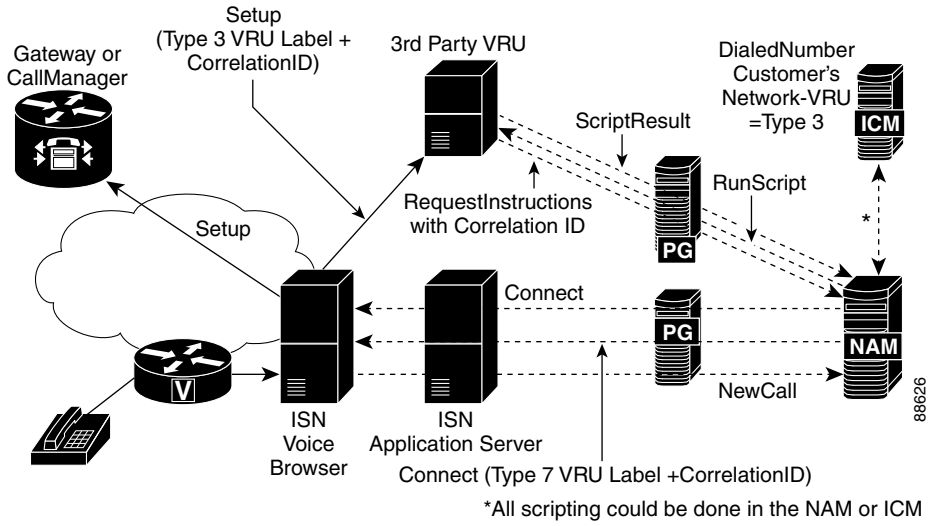
  The scenario where the ISN is acting as the routing client for the call, as well as the voice response function itself, is called a Service Node implementation. Figure 1-9 gives the basic architecture. The ISN is used for both prompting/queuing the call as well as for connecting the call to the call center agent.

Figure 1-9 Service Node Implementation (ISN Queuing and Transfer)



An alternative scenario is where the ISN acts as a routing client that, first, switches the call to a 3rd-party VRU and, then, switches the call to an agent. Figure 1-10 shows this scenario.

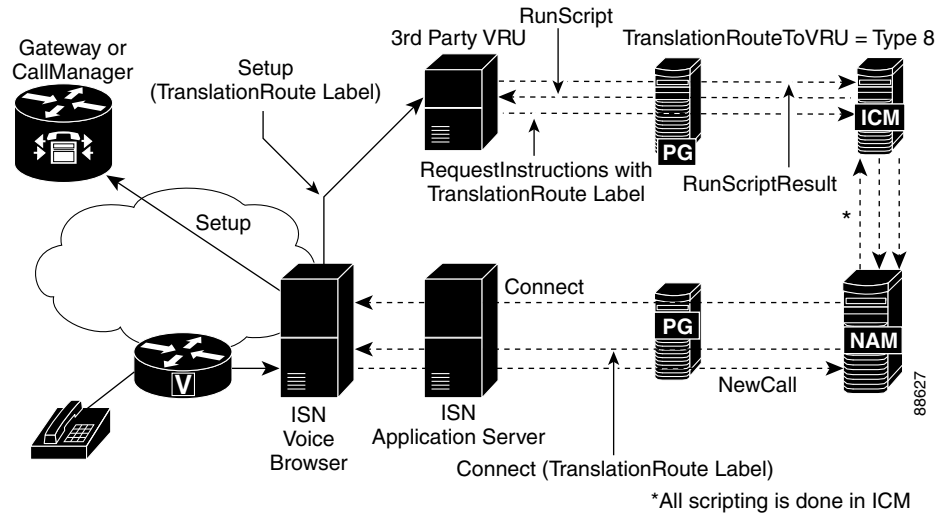
Figure 1-10 ISN as Routing Client with 3rd Party VRU (ISN Queuing and Transfer)



- **If there is a separate routing client, is the ISN connected to the NAM?**

  One of the most significant differences between a network-hosted VRU (connected to the NAM) and a customer premise-hosted VRU (connected to the CICM) is the correlation mechanism used. The correlation mechanism shown in Figure 1-11 takes care of uniquely identifying the same call across the two dialogs that the NAM maintains for each call, one with the routing client and the other with the VRU Peripheral Gateway. Network-hosted VRUs can generally use a simple correlation ID that can be passed along with the call, whereas premise hosted VRUs are typically connected through the PSTN network that cannot transport a correlation ID directly. In that case a translation route mechanism is used to correlate the calls.

Figure 1-11 Network VRU at Customer Premises, Connected to ICM Instead of the ISN



- **What capabilities does the routing client have to divert calls to a VRU and take them back later in order to connect the call to an agent?**

  The answer to this question does not influence the architecture so much as it impacts the call flow. There many variations in routing client capabilities.

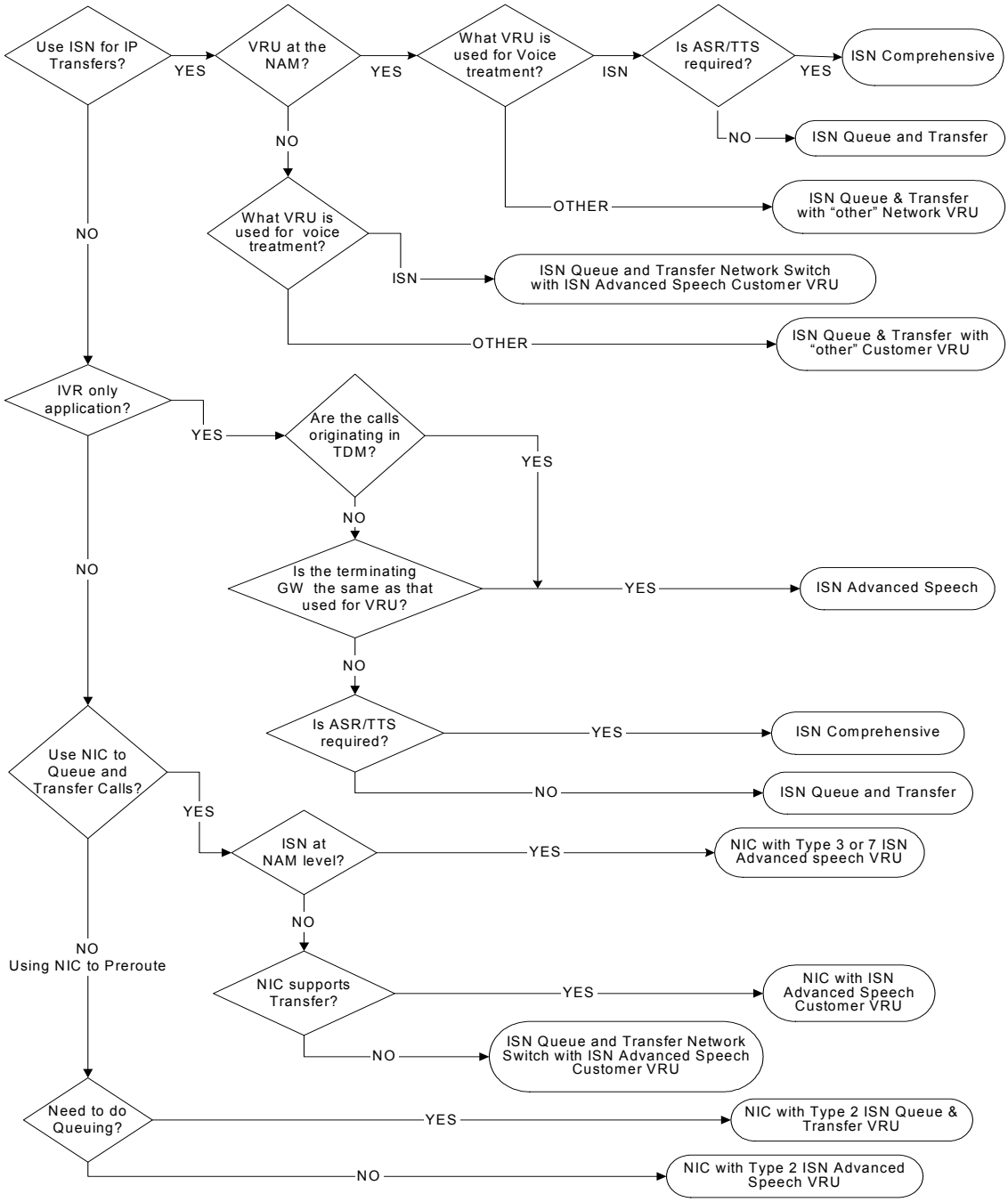
Once you have answers to these questions, you can use the decision trees presented in the next two sections to determine what ISN deployment model you should use.

Note The resulting end points of the trees identify the ISN deployment model(s) needed as well as the VRU type information needed for the NAM/ICM configuration.

Decision Tree for NAM Deployments

Figure 1-12 shows the decision path you might follow in planning an ISN NAM deployment.

Figure 1-12 Decision Tree - NAM Deployments

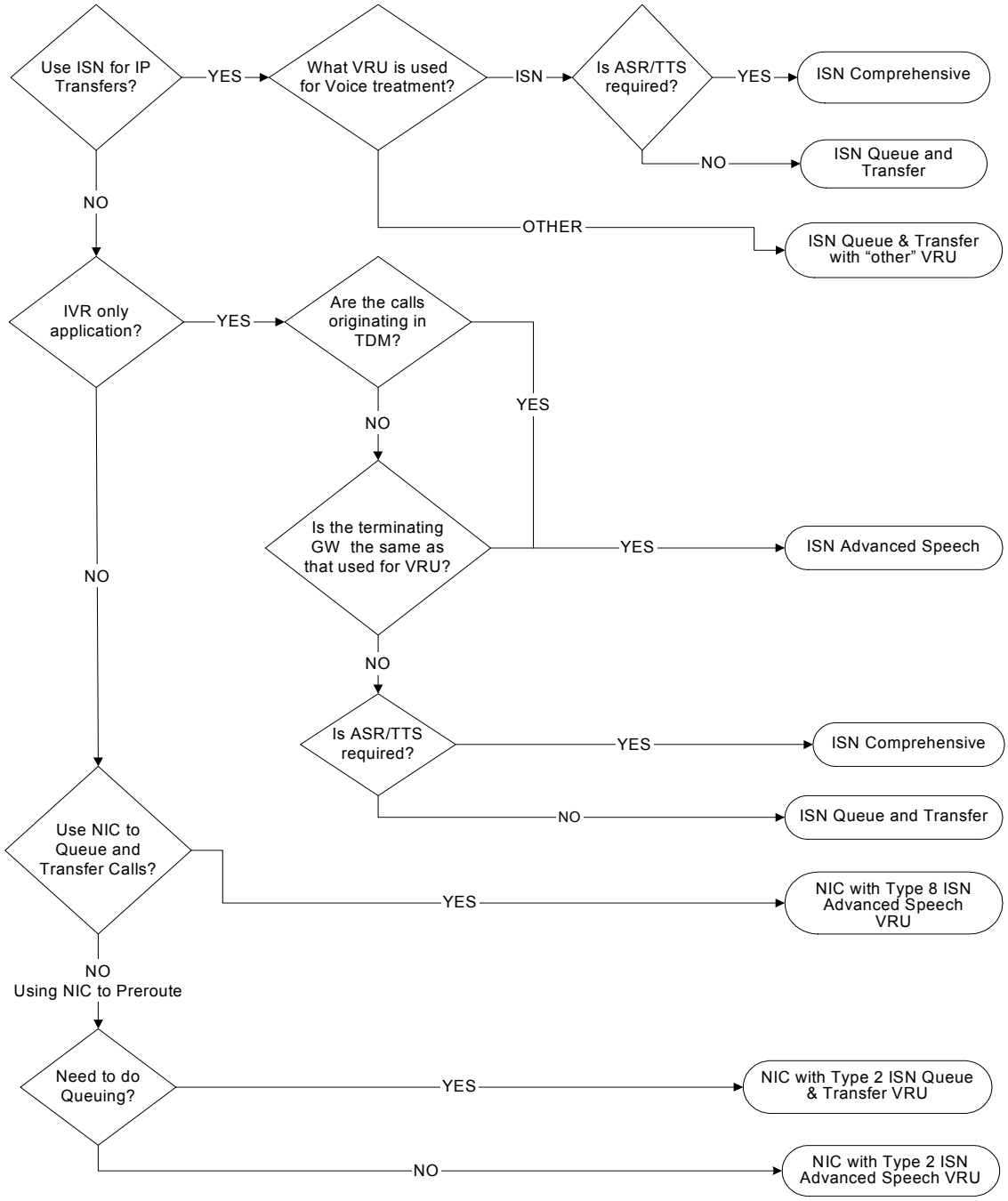


Note For more detailed information about each of these deployment options, including checklists for configuration tasks, see Appendix C of the *Cisco Internet Service Node (ISN) Configuration and Administration Guide*.

Decision Tree for ICM Implementations

Figure 1-13 shows the decision path you might follow in planning an ICM deployment.

Figure 1-13 Decision Tree - ICM Deployments



Note For more detailed information about each of these deployment options, including checklists for configuration tasks, see Appendix C of the *Cisco Internet Service Node (ISN) Configuration and Administration Guide*.

Other ISN Features

This section discusses the following additional ISN features.

- NAM/ICM Scripting
- Transferring Calls with ISN
- ASR/TTS

NAM/ICM Scripting

The ICM Script Editor is the scripting engine behind the ISN. It provides the user-programmable scripting environment for ISN call handling.

ISN Version 2.0 comes with a number of pre-built building block applications, called *micro-applications*. Micro-applications reside on the ISN's Application Server and contain instructions that direct the ISN's software and hardware interaction, enabling communication with the caller.

The interface between the Application Server and the NAM/ICM is a Cisco ICM/IVR Service Control Interface. The Application Server takes information in the messages sent by the NAM/ICM, interprets it using the micro-applications, and generates VXML code that it sends to the Voice Browser for processing.

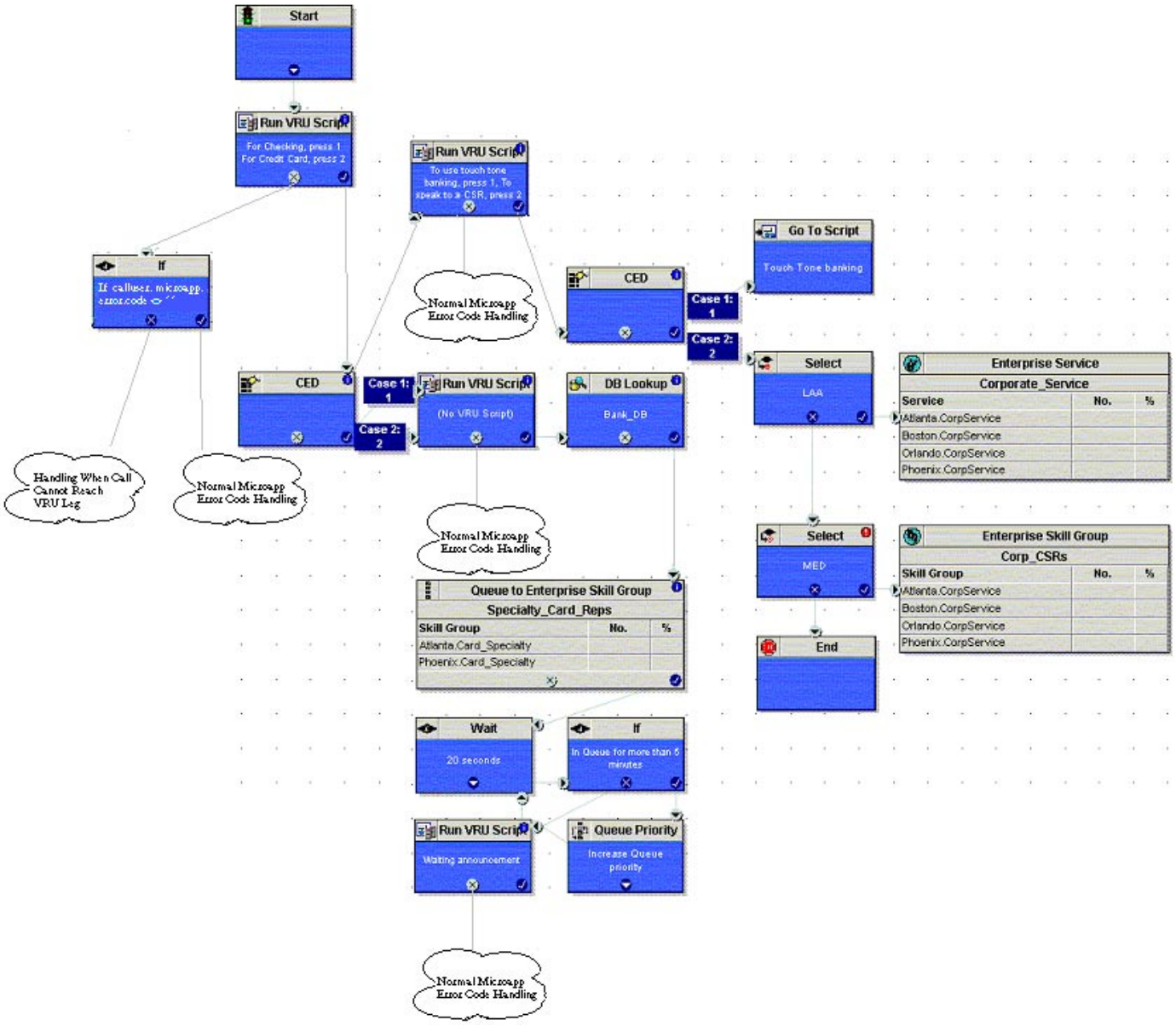
There are five ISN micro-applications:

- **Play Media**. Plays a message to the caller.
- **Play Data**. Plays data such as dates or numbers to the caller in a specific format, called a *data play back type*.
- **Get Digits**. Plays a message to the caller and collects DTMF digits.
- **Menu**. Plays a message (menu) to the caller and collects a single DTMF.
- **Get Speec**h. Collects ASR input (voice or DTMF digits) after prompting a caller.

Note For more information on micro-applications, see the *Internet Service Node (ISN) Configuration and Administration Guide*.

Using the NAM/ICM Script Editor, these building blocks can be combined in any order to build a complete IVR script. Figure 1-14 shows an example of an ISN script.

Figure 1-14 Sample Script for ISN



Automatic Speech Recognition (ASR)

When a caller performs voice input, the speech recognition engine tries to match the caller input to a set of acceptable responses, an *ASR grammar*.

An ASR grammar is a list of choices. ISN 2.0 supports two types of grammars:

- **Inline grammars**. A set of acceptable customer responses defined through the setting in the **user.microapp.grammar_choices** ECC variable.

- **External grammars**. A file containing a set of acceptable customer responses. This file is located on a media server and retrieved from the device performing ASR.The Application Server adds this pointer to the VXML that it sends to the Gateway. The Gateway then loads the grammar and uses it to check ASR input from the caller.

Note For a complete explanation of VXML file grammar format, see the *Internet Service Node (ISN) Configuration and Administration Guide*. Also, consult the user documentation for your ASR Server for a list of supported grammar elements.

ASR Engine Support

ISN Version 2.0's support for ASR is defined by the functionality supported by the ASR engines that are used in the solution. ISN Version 2.0 supports the Nuance 8.0 ASR Server and Speechworks.

See the *Internet Service Node (ISN) Release Notes for Release 2.0* for a list of differences between the Nuance ASR/TTS Engine and the Speechworks ASR Engine.

Transferring Calls with ISN

There are four different ways that the ISN system can transfer a call using the PSTN or IP. In each case, the NAM/ICM initiates the transfer.

A transfer can be triggered by a number of means, such as:

- Call context (that is, DNIS, ANI, Time of Day).
- A caller choosing a menu option from a VRU application.
- An agent behind an ACD or IPCC signalling a transfer to a different agent.
- An agent becomes available.

Table 1-2 describes the transfer types available to the ISN.

Table 1-2 Transfer Types

Type of Transfer	Description	Notes
TDM Network Transfer (traditional take back and transfer)	Executes a PSTN transfer. The NAM/ICM sends a "transfer" command through the network NIC instead of issuing a label to the ISN. This method does not directly involve the ISN since the transfer messages are sent through the NIC to the PSTN.)	Valid for ISN deployed as an Intelligent Peripheral IVR. The call must have been pre-routed by the NAM/ICM, so it can store the network call ID and use it to send the transfer command to the NIC.
IP Transfer (call delivery within the VoIP network)	Executes a transfer within the VoIP network, with the option of first providing IVR treatment to the caller. The ISN uses VoIP to switch the incoming call to an IP-based destination, where the destination may be the actual agent (on an IP Phone) or a Gateway that passes the call to the agent on a traditional telephone (usually behind an ACD/PBX). A Gatekeeper is required for this type of transfer to resolve the NAM/ICM routing label into an IP address for the ISN to communicate with to route the call.	Valid for ISN deployed as a Service Node IVR. The call must be translation routed to a peripheral target (agent on TDM ACD) or be sent to a device target (IPCC agent) in order for the agent to request a subsequent transfer.
Outpulse Transfer	Executes a PSTN transfer from within the VoIP network. The ISN sends DTMF signals to a carrier network through the ingress Gateway, then the carrier network disconnects the call from the Gateway—and the ISN—and delivers it to the agent.	Valid for ISN deployed as a Service Node IVR.
IPCC Local Transfer	Executes a transfer within the VoIP network using the Cisco Call Manager.	Valid for ISN deployed as a Service Node IVR. The CCM is responsible for performing the transfer.

Sample ISN Call Flows

ISN call flow scenarios can differ between deployment models. The sections that follow provide details regarding these differences.

ISN Queue and Transfer

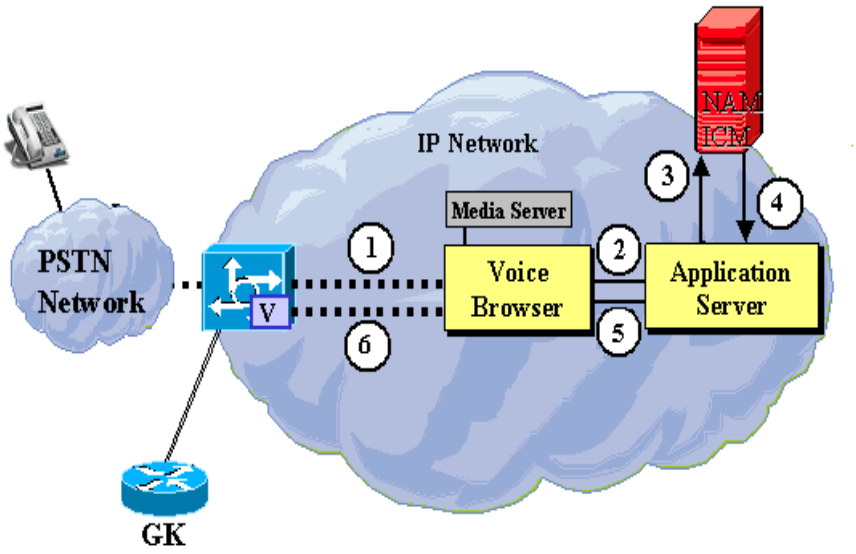
This section outlines the following ISN call flow scenarios for the ISN Queue and Transfer deployment model.

- Call Arrival, prompt and collect
- IP Transfer
- Call Queuing
- IP Takeback and Transfer
- Local Transfer (to IPCC)
- Outpulse Transfer

ISN Call Arrival, Prompt and Collect

Figure 1-15 shows an ISN call arrival scenario.

Figure 1-15 ISN Call Arrival



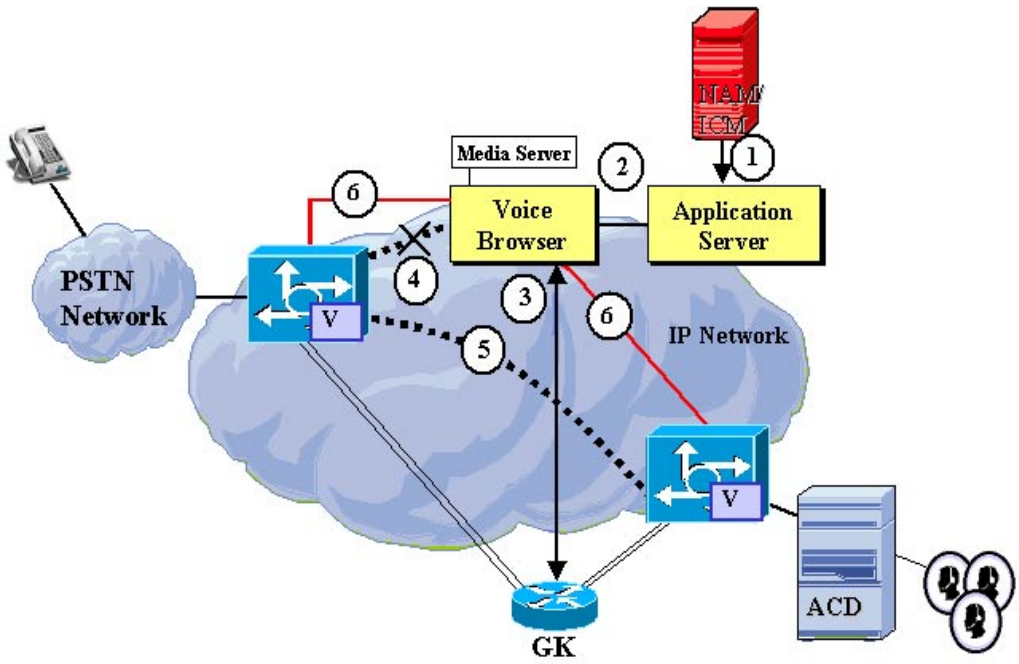
The call arrival flow in Figure 1-15 is as follows:

1. The call comes into the PSTN network and is routed to the Voice Browser through a Gateway. (The call may have been pre-routed by NAM/ICM to the Gateway.)
2. The Voice Browser informs the Application Server that a call has arrived.
3. The Application Server requests instructions of the NAM/ICM.
4. The NAM/ICM consults the customer database/application as needed, then determines which scripts to run and what information to communicate. The NAM/ICM passes this information to the Application Server.
5. The Application Server creates a VXML page, which tells the Voice Browser to do. The Voice Browser retrieves any media files or announcements from the Media Server.
6. The Voice Browser plays prompts or announcements over the packetized voice stream back through the originating Gateway to the caller and collects DTMF input as required.

ISN IP Transfer

Figure 1-16 shows an ISN IP transfer scenario.

Figure 1-16 ISN IP Transfer



The call routing flow in Figure 1-16 is as follows:

1. The NAM/ICM makes a routing decision based on call context or by executing scripts. Once the NAM knows the terminating destination for the call, it sends call routing instructions to the Application Server.
2. The Application Server generates a VXML page with instructions and sends it to the Voice Browser.
3. The Voice Browser conducts a lookup in its Gatekeeper to determine the IP address of where to send the call.
4. Voice Browser tells the originating Gateway to break down the existing packetized voice stream.
5. Voice Browser instructs the Ingress Gateway to set up a new packetized voice stream to the Egress Gateway or Call Manager.
6. Meanwhile, the Voice Browser retains signaling control over the Ingress Gateway and new Egress Gateway, using the H245 signaling channel.

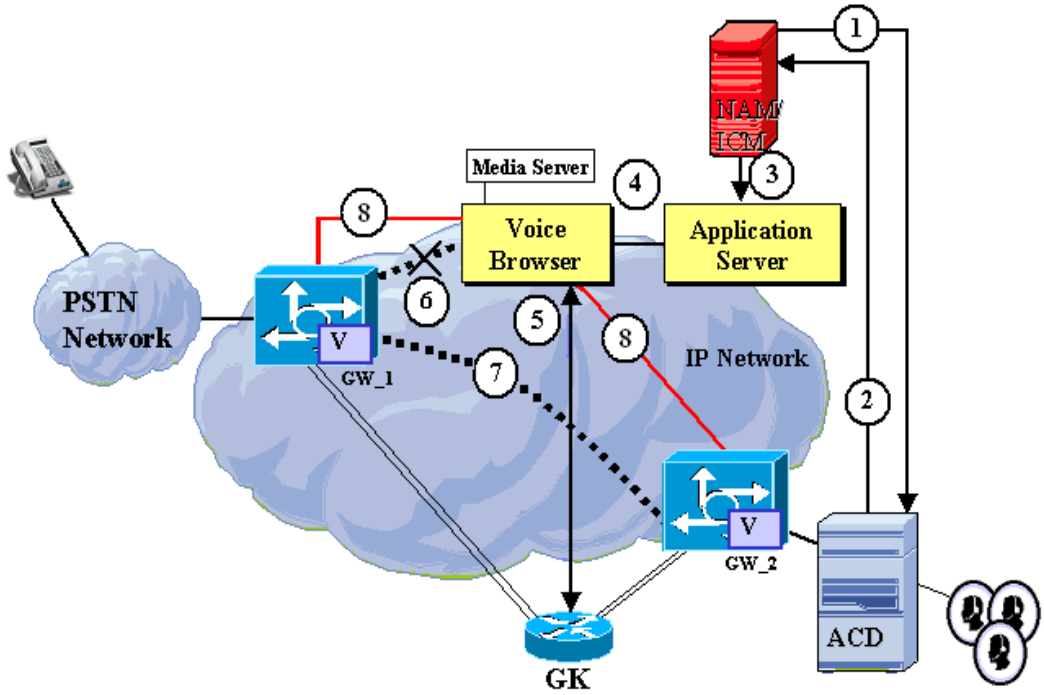
Note The processes described in Steps 4-6 use the *H245 Empty Capability Set* feature. This is a mechanism the Voice Browser uses to tear down a RTP stream and cause it to be redirected somewhere else.

ISN Call Queuing

Figure 1-17 depicts an ISN call queuing scenario.

Note The call flow in Figure 1-17 presumes the call is already on ISN and receiving IVR treatment.

Figure 1-17 ISN Call Queuing



The call queuing flow in Figure 1-17 is as follows:

1. The ICM determines the requested agent is not available; the ISN continues IVR treatment.
2. An agent becomes available.
3. The NAM/ICM instructs the Application Server that an agent is available and to transfer the call.
4. The Application Server generates a VXML page with instructions and sends it to the Voice Browser.
5. The Voice Browser interrupts IVR treatment and conducts a lookup in its Gatekeeper to determine the IP address of where to send the call.
6. The Voice Browser tells the originating Gateway (GW_1) on the left to tear down the existing RTP stream.
7. The Voice Browser commands the originating Gateway (GW_1) to redirect the RTP stream to a new destination, the second Gateway (GW_2).

Note The new destination could also be another IP termination point or a third Gateway that would ultimately route the call back to the TDM.

8. Meanwhile, the Voice Browser retains signaling control over call control over both Gateways, using the H245 signaling channel.

Note The processes described in Steps 6-8 use the *H245 Empty Capability Set* feature. This is a mechanism the Voice Browser uses to tear down a RTP stream and cause it to be redirected somewhere else.

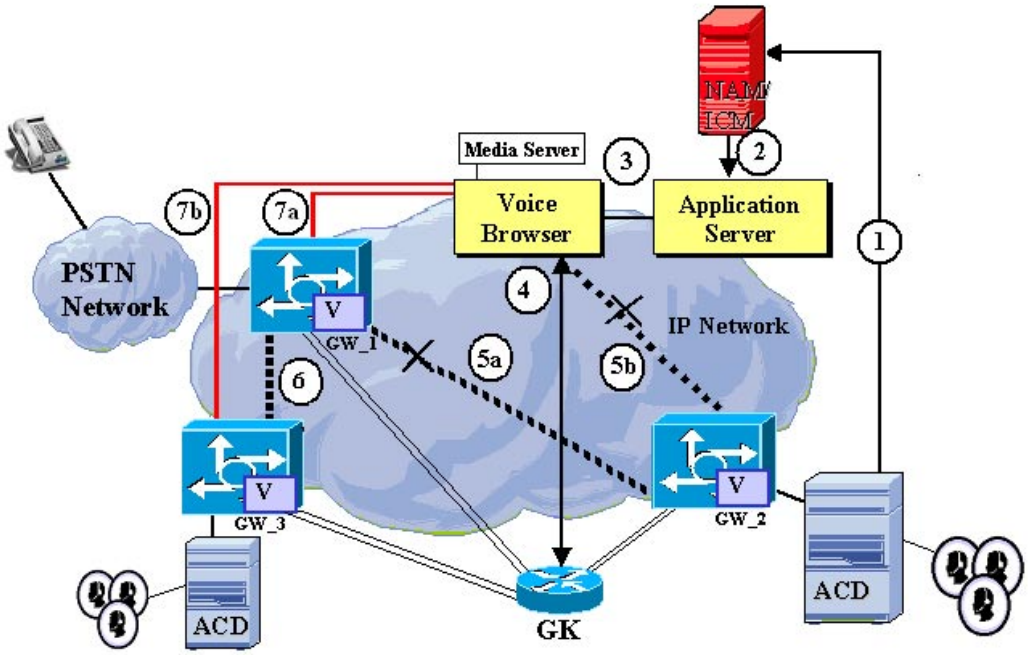
ISN IP Takeback and Transfer

A powerful feature of the ISN is its ability to re-route a call through the IP network by doing a takeback of the outbound call and transferring the call to a new destination.

Figure 1-18 shows an example of an ISN IP takeback and transfer.

Note The call flow in Figure 1-18 presumes the call was previously routed by the ISN to GW_2, using IP Transfer.

Figure 1-18 ISN IP Takeback and Transfer



The takeback and transfer flow in Figure 1-18 is as follows:

1. An agent initiates call transfer.
2. The NAM/ICM sends route information and instructions informing the Application Server to transfer the call.
3. The Application Server generates a VXML page with instructions and sends it to the Voice Browser.
4. The Voice Browser conducts a lookup at its Gatekeeper to determine the IP address where the call should be transferred.

5. The Voice Browser (**a**) tells the originating Gateway (GW_1) to tear down the existing RTP stream to the agent and (**b**) terminates call control with the Gateway on the right (GW_2).
6. The Voice Browser instructs the originating Gateway (GW_1) to redirect the RTP stream to the new Gateway (GW_3).
7. Meanwhile, the Voice Browser keeps H.245 control over both (**a**) the originating Gateway (GW_1) and (**b**) the new Gateway (GW_3).

Since the Voice Browser retains signaling control over the endpoint, the call can be transferred again – multiple transfers – where the call stays under the control of the Voice Browser and just the voice path itself is moved around.

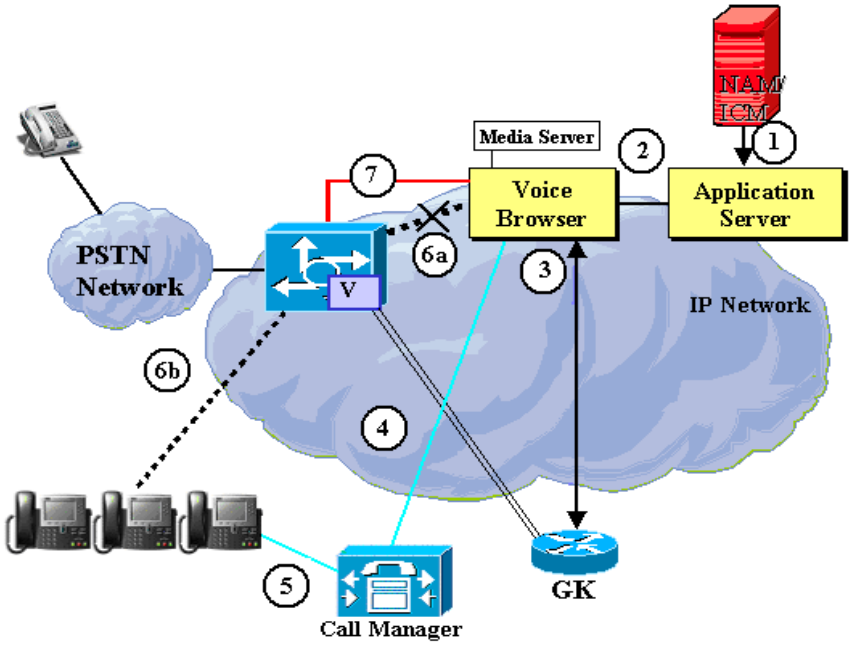
ISN Local Transfer To IPCC

A *local transfer* is one that is routed to IPCC. This means that Cisco Call Manager is responsible for performing the transfer.

Figure 1-19 depicts a local transfer scenario.

Note The call flow in Figure 1-19 presumes the call is already on ISN and receiving IVR treatment.

Figure 1-19 ISN Local Transfer to IPCC



1. The NAM/ICM sends route information and instructions informing the Application Server to transfer the call.
2. The Application Server generates a VXML page with instructions and sends it to the Voice Browser.
3. The Voice Browser conducts a lookup at its Gatekeeper, which returns the IP address of Call Manager.

4. The Voice Browser communicates with the Call Manager, which returns the IP address of the IP phone.

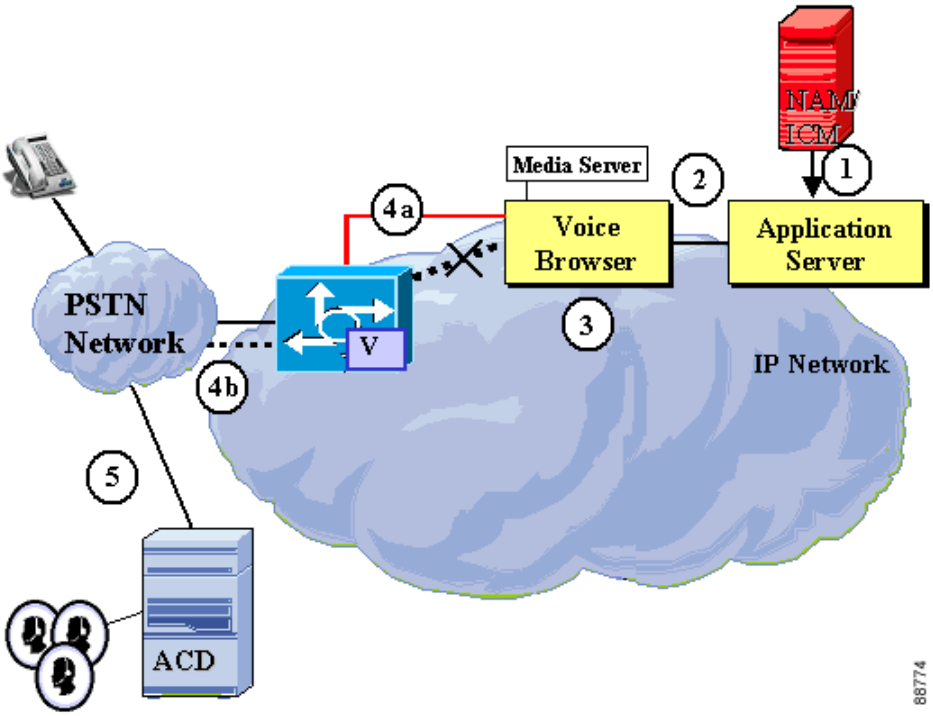
Note The transfer is performed using H.323 protocol, as the ISN appears to the CCM as an H.323 device.

5. The Call Manager reserves an agent for the call.
6. The Voice Browser (**a**) tells the ingress Gateway to tear down the existing RTP stream and (**b**) re-route it to the designated agent's IP phone.
7. Meanwhile, the Voice Browser keeps H.245 control over the originating Gateway.

ISN Outpulse Transfer

Figure 1-20 shows an ISN outpulse transfer scenario.

Figure 1-20 ISN Outpulse Transfer



1. The NAM/ICM sends route information and instructions informing the Application Server to transfer the call.
2. The label begins with **DTMF** to indicate that the label should be used to outpulse the DTMF characters. The Application Server removes the DTMF and generates a VXML page that tells the Voice Browser to transfer the call in this way.

Note In outpulse transfer mode, the ISN will send whatever digits are in the label to the Gateway for outpulsing. It is the customer's responsibility to confirm interoperability with the target switch.

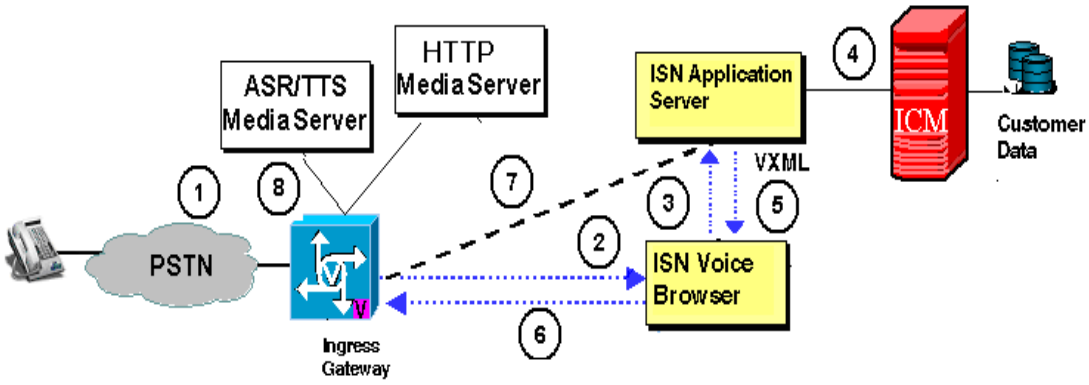
3. The Voice Browser *does not* perform a lookup in the Gatekeeper, because the Voice Browser already knows it will communicate with the ingress Gateway in order to perform the transfer.
4. Voice Browser (a) provides the transfer information to the Ingress Gateway and (b) the Gateway outpulses the transfer information to the network.
5. The external telephony network transfers the call to its final destination.

ISN Comprehensive

ISN Comprehensive calls flows are the same as those diagrammed for the ISN Queue and Transfer models with the exception that the ISN sends the call to a **Gateway** for IVR treatment, rather than the ISN performing the IVR function itself.

Figure 1-21—and the text that follows it—describes the call flow in the ISN Comprehensive Model for a new call performing prompt and collect with ASR/TTS.

Figure 1-21 ISN Comprehensive Model, Call Arrival with ASR/TTS Prompt and Collect



The call flow in Figure 1-21 is as follows:

1. A call arrives from the PSTN network to the IP network via the Ingress Gateway. (The call may have been prerouted by the ICM.)
2. The Gateway connects the call to the ISN Voice Browser.
3. The ISN Voice Browser informs the ISN Application Server that a call has arrived.
4. The ISN Application Server requests instructions of the ICM and passes call data such as CLI and DNIS. The ICM consults its customer data and returns instructions to the ISN Application Server.
5. The ISN Application Server issues a VXML request telling the ISN Voice Browser to transfer the call (via IP switching) to an IP port on an IVR Gateway (either the Ingress Gateway or another Gateway not shown),
6. The ISN Voice Browser transfers the call and retains control of the call for future transfers.
7. The IOS Gateway uses VXML processing to tell an ISN Application Server (either the ISN Application Server shown or a different ISN Application Server) that the call has arrived.
8. Prompt/collect at the IVR Gateway (with ASR/TTS support) proceeds per the Advanced Speech Model. Calls can be queued at the IVR Gateway because the ISN Voice Browser still has control of the call. When prompt/collect is finished at the IVR Gateway, the ISN Voice Browser can command the Ingress Gateway to route the call by using one of the following Call Transfer types:

  - IP switching with subsequent agent initiated transfers under ICM control
  - Outpulse Transfer to PSTN
  - IN Transfer

ISN Advanced Speech

The following ISN Advanced Speech call flow scenarios are the same as those diagrammed for the ISN Queue and Transfer deployment model except there is no ISN Voice Browser; the **Gateway** performs the IVR treatment and transfers:

- Call Arrival/Prompt and Collect
- IP Transfer
- Local Transfer

Note The Outpulse Transfer, IP Takeback and Transfer, and Queuing scenarios are not available for this deployment model.

ISN Solution Components

This chapter presents additional information about the ISN solution runtime components first introduced in Chapter 1, "Introduction":

- Non-ISN Cisco products (NAM/ICM, Media Server, Gateway, Gatekeeper, IPCC, Content Switch, Remote Monitoring Tools).
- ISN product components (Application Server, Voice Browser, SDDSN).

The chapter focusses on describing ISN solution:

- System administration.
- Internal interfaces.
- Software component co-residence.
- Security.

Non-ISN Cisco Products

The ISN solution includes other Cisco products:

- NAM/ICM
- Media Server
- Gateway and Gatekeeper
- IPCC (for IP-based call centers)
- Content Switch
- Remote Monitoring Suite (optional)

NAM/ICM

The **NAM/ICM** is the engine for making call treatment and routing decisions for calls as they progress through the network. To the NAM/ICM, the ISN is simply a VRU peripheral; this is true whether the network is classic PSTN, VoIP, or a combination of both.

In addition, the NAM/ICM provides the means to access specific call detail records, as well as customer databases and applications.

Note The ISN does not access customer databases directly.

Media Server

The Media Server is an off-the-shelf Web Server—or set of Web Servers or Cisco Content or Cache Engines—which provides the media files that contain messages and prompts that callers will hear. The Voice Browser retrieves media files from the Media Server using standard Web access methods.

You do have the option of installing local media files on the Voice Browser instead of using a separate Media Server. However, to maximize Voice Browser performance, the Media Server should not be installed on the same machine as the Voice Browser.

The Web-based Media Servers are deployed in a replicated high availability environment. It is assumed that standard Web tools, such as Directors—which direct the client to the appropriate server based on availability, load balancing, and/or proximity—might be used for some large-scale deployments. **However, Web Directors were not tested as part of the ISN 2.0 release, so they are not supported.**

Gateway and Gatekeeper

In an ISN solution, a **Gateway** is required to support TDM clients. On the TDM side, the Gateway accepts ISDN PRI signaling interfaces. It also supports direct digital connections to ACDs and VRUs without going through an intervening switch. (For these digital connections to ACDs and VRUs, the Gateway must function as the "network side.")

Note For more information on Gateways and Gatekeepers, see Chapter 4, "VoIP Routing."

A Gateway:

- Converts PSTN calls to H.323 protocol and routes them to a VoIP endpoint, the Voice Browser.
- Passes call information—such as the called number— to the ISN's Voice Browser so the call can be segmented and an application chosen.
- Is responsible for performing call redirection in the IP transfer mode of operation, using either the G.711 codec or the compressed G.729 codec. (G.729 allows for bandwidth savings during the portion of the call when a call is transferred to the agent.) This call redirection feature enables the Voice Browser to retain call control, separately controlling each leg of the transfer, including subsequent transfers.

Note At the time of software release, ISN Version 2.0 had been tested with and is supported on Cisco AS5300, AS5350, and AS5400 Gateways running IOS Version 12.2. (13) T3. Additional Gateways are being certified; for the most current information, see the *Cisco Internet Service Node (ISN) Data Sheet* on Cisco Connection Online (CCO) at http://www.cisco.com.

A **Gatekeeper** is required for IP Transfers. The Gatekeeper is H.323 compliant and is responsible for call control services for the H.323 endpoints, that is, the Gateways and the Voice Browsers in the ISN system.

A Gatekeeper:

- Provides the called point's network address resolution for the calling point through ARQ/ACF messages upon the calling endpoint's request, if both called and calling points are registered to the same Gatekeeper.
- Provides the called point's network address resolution for the calling point through LRQ/LCF messages upon the calling endpoint's request, if the called point is registered in another Gatekeeper.
- Supports BRQ/BRJ/BCF messages for bandwidth control. (This might be based on bandwidth management or be a null function which accepts all requests for bandwidth changes).

Note At the time of software release, ISN Version 2.0 had been tested with and is supported on Cisco 36XX Gatekeepers running IOS Version 12.2 (11) T. For the most current information, see the *Cisco Internet Service Node (ISN) Data Sheet* on Cisco Connection Online (CCO) at http://www.cisco.com.

IPCC

The Cisco IPCC delivers an integrated suite of proven products that combine Cisco IP telephony and contact center solutions.

ISN Version 2.0s design and features enable it to function as a network or premise based IVR and/or queue point for IPCC.

Automated Speech Recognition (ASR) and Text-to-speech (TTS)

Automatic Speech Recognition is the ability to provide speaker independent voice recognition to gather information from a caller. Text-to-speech signifies the ability to convert a text string to speech to play for a caller.

When an ICM script uses ASR and/or TTS, it sends pre-recorded voice prompts to the caller, or generates them with TTS through a voice synthesizing process. In response, the caller either uses a typed or voice response. If the caller chooses a voice response, the speech recognition engine attempts to match the caller's voice to a set of stored options and responses. Speech recognition can be a set of words or type of response.

An additional ISN feature for ASR/TTS is referencing an external VXML document from the Application Server VXML. This enables the reuse of previously defined VXML documents, which can contain lenghty TTS text or multiple prompt and collect steps.

Caution The Application Server does not validate the contents of imported any VXML documents. External VXML documents need to follow a very specific format in order to function correctly with ISN. Additionally, external VXML documents cannot return results/values to the ICM script.

Content Switch

The gateway requests VXML documents, media and ASR/TTS treatment from back-end servers. A pair of content switches provides high availability and load-balancing to these back-end servers.

ISN Product Components

ISN Version 2.0 consists of the following components:

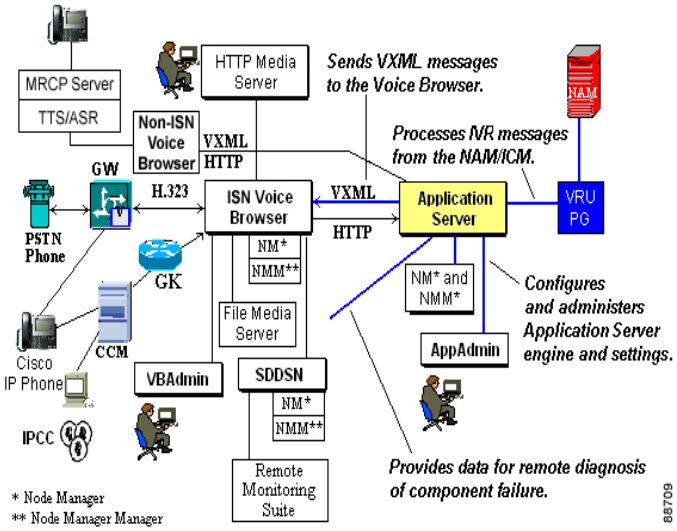
- Application Server
- Voice Browser
- SDDSN

In addition to the call processing roles discussed in Chapter 1, "Introduction," the Application Server and Voice Browser perform configuration and administrative functions. They also supply data to the SDDSN that enables remote diagnosis of ISN solution problems.

Roles of the Application Server

Figure 2-1 illustrates the roles of the Application Server.

Figure 2-1 Roles of the Application Server



In addition to its call processing roles—sending VMXL messages to the Voice Browser and processing IVR messages from the NAM/ICM—the Application Server provides:

- An administration tool, the *Application Administrator*.
- Information to the SDDSN process for remote diagnosis of component failure. (This process is described in the "SDDSN" section on page 2-8.)

Application Administrator

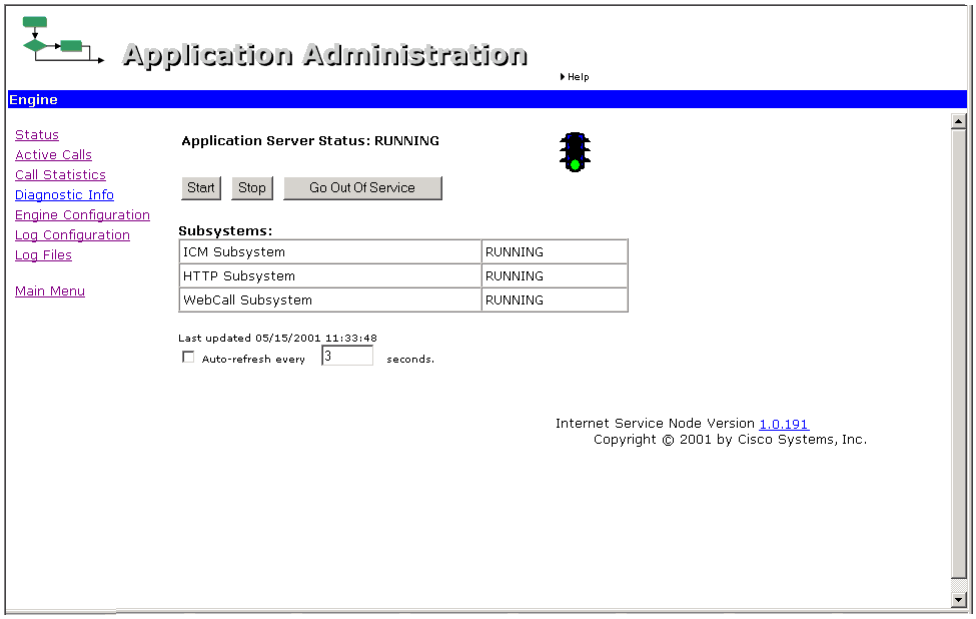
The Application Server's **Application Administrator** tool is a Web browser interface that can be used to perform tasks such as:

- Take the Application Server engine in and out of service.
- Monitor call status.
- Configure timeout settings.

- Perform remote configuration.

Figure 2-2 shows a sample Application Administrator Web page.

Figure 2-2 Engine Status Page

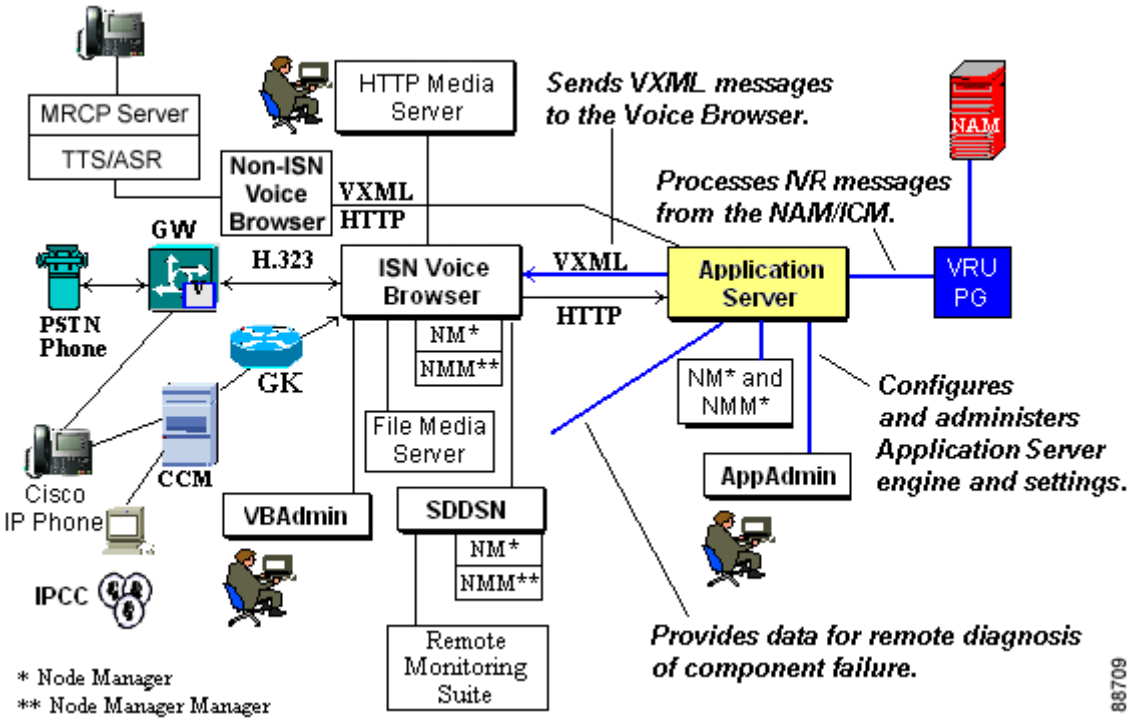


Note For instructions on how to use the Application Administrator tool, see the *Cisco Internet Service Node (ISN) Configuration and Administration Guide*.

Voice Browser

Figure 2-3 illustrates the roles of the Voice Browser.

Figure 2-3 Roles of the Voice Browser



In addition to its call processing roles—accepting H.323 VoIP calls, sending URL requests to the Application Server, and retrieving system prompts from the Media Server—the Voice Browser provides:

- A configuration and administration tool, *VB Admin*.
- Information to the SDDSN process for remote diagnosis of component failure. (This process is described in the "SDDSN" section on page 2-8.)

VB Admin

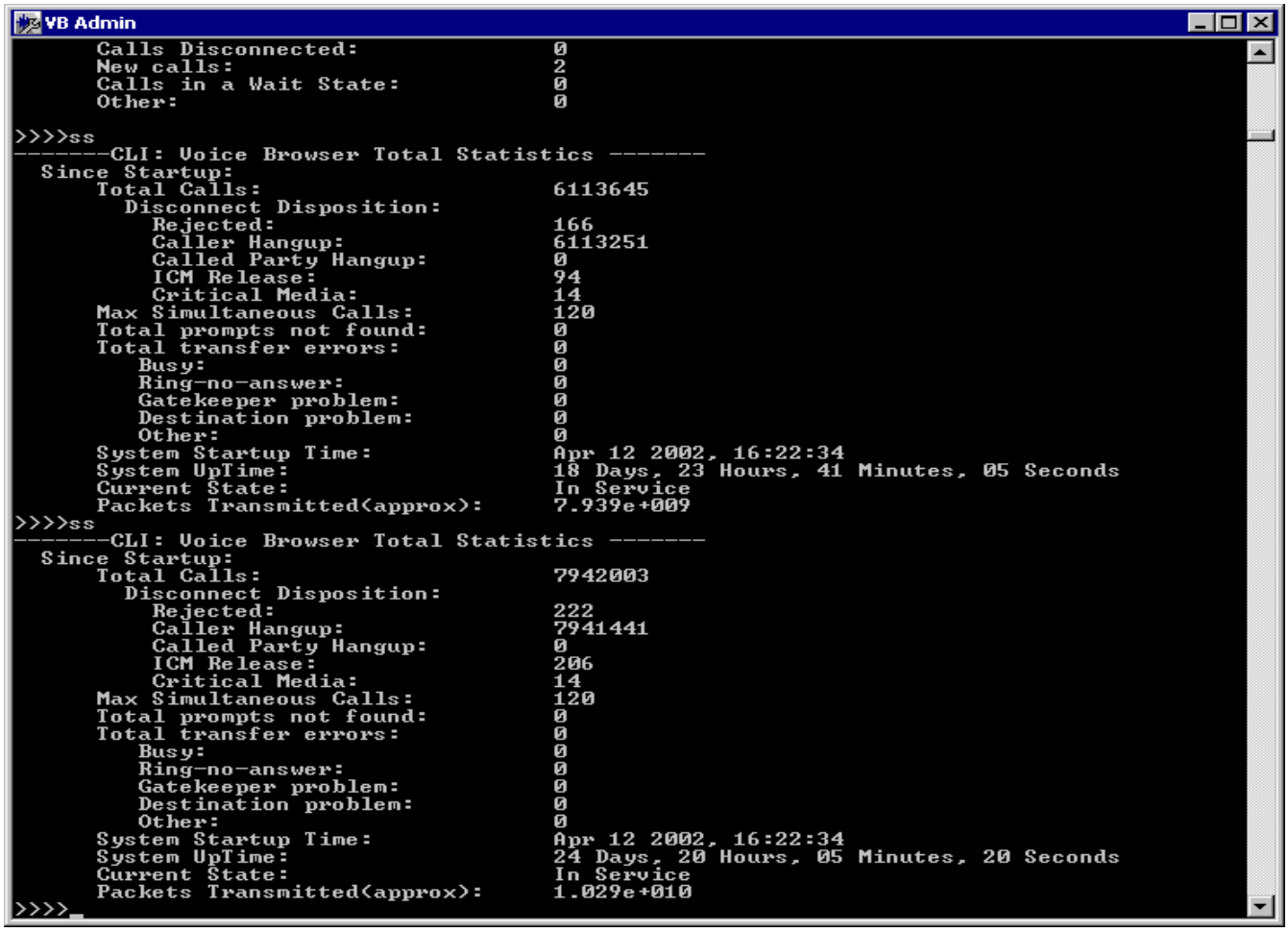
Voice Browser configuration and administration tool— **VB Admin**— helps you keep track of the Voice Browser's interactions with various ISN solution components. This tool provides a command line interface (CLI) you can use to:

- Gather statistics.
- Modify configuration settings.
- View system metrics and status.
- Control the Voice Browser.

Since there are often many Voice Browsers in network installations, VB Admin can be run locally or remotely. Also, since VB Admin is a command line tool, it can easily be scripted to manage multiple remote Voice Browsers.

Figure 2-4 shows an example of a VB Admin Console window.

Figure 2-4 VB Admin Console Window



Note For more information on the VB Admin tool, see the *Cisco Internet Service Node (ISN) Configuration and Administration Guide*.

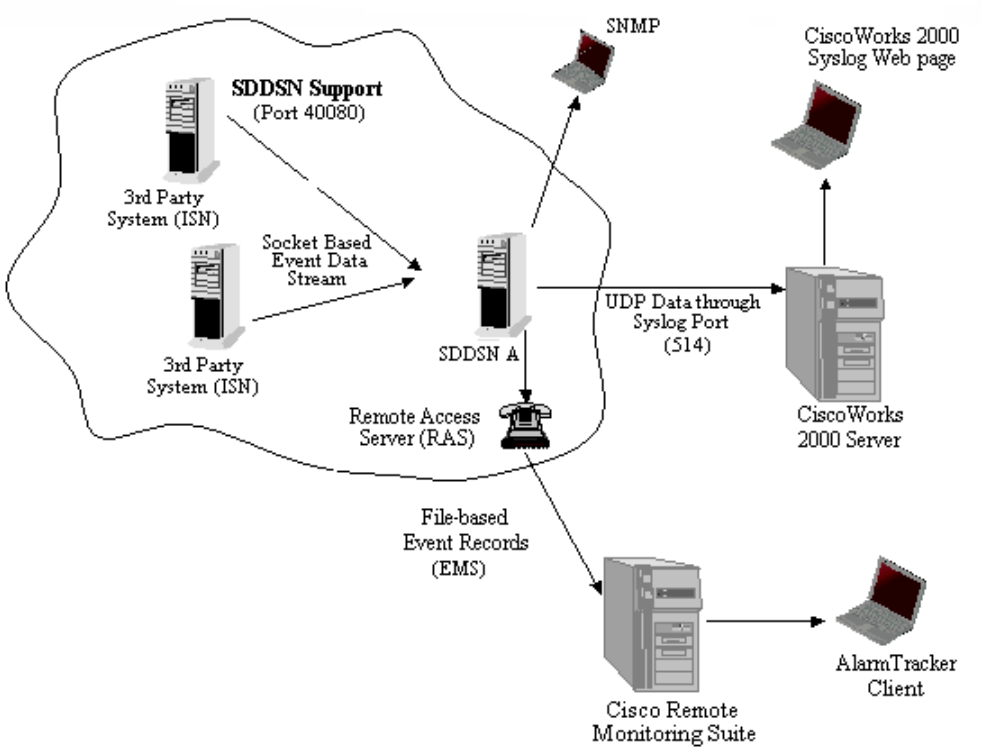
SDDSN

The Standalone Distributed Diagnostics and Services Network (SDDSN) is a component that provides alarm reporting for ISN through a variety of mechanisms:

- SNMP traps.
- CiscoWorks 2000 Syslog, which receives log messages and permits queries on the logs.
- Windows Remote Access Server (RAS) and NAM/ICM Event Management System (Cisco Remote Monitoring Suite).

Figure 2-5 shows a diagram of SDDSN support mechanisms.

Figure 2-5 SDDSN Support



Note For complete details on each of these methods and the tools available to use them, see the *Cisco Internet Service Node (ISN) Configuration and Administration Guide*.

ISN Internal Interfaces

Table 2-1 summarizes the interfaces between the ISN components and other Cisco products.

Table 2-1 Major Internal Interfaces

Interface		Interface characteristics	
Between This Component...	***...and This Component***	***InterfaceType***	***Selection Determined by***
Gateway	Voice Browser	H.323	Gatekeeper or Gateway dial-peers, based on Voice Browser availability and proximity
CCM/IP Telephone			
Gateway	Gatekeeper	H.323	Gateway configuration
Voice Browser	Application Server	HTTP (URL with VXML response). Voice Browser client, Application Server server.	Voice Browser configuration
	Media Server	HTTP	URL is given in VXML generated by the Application Server from information specified in the ICM. Normal web access (DNIS, distributors, etc.), is used to resolve it.
Application Server	NAM/ICM	ICM/IVR Messaging	ISN configuration
	SDDSN	Proprietary	ISN configuration
NAM	ICM	Proprietary	Customer identified by calling information; NAM configuration determines ICM
ICM	Customer Database	SQLGateway	ICM configuration
		Application Gateway	ICM configuration

Software Component Co-residence

This configuration is provided for functional testing purposes. To achieve the quoted performance, it is assumed that the ISN components do not reside with any other components, and the other components are deployed as recommended for their product. Measuring and monitoring performance for any other combinations are the responsibility of the customer.

- ISN Voice Browser 2.0
- ISN Application Server 2.0
- ISN VBAdmin 2.0
- ICM 4.6.2 (installed on its own machine)
- SDDSN (cannot be co-resident with any ISN, ICM, or Remote Monitoring Suite product)
- Remote Monitoring Suite 2.0
  - Listener
  - LGMapper
  - LGArchiver
  - AlarmTracker

Security

Since the ISN is a Web-based solution and does not use secure connections such as SSL, security issues should be approached as you would any other non-secure Web application on your system. Some issues to take under consideration are how to:

- Set up user access for maintenance.
- Protect communication between system components.
- Ensure customer isolation and privileges in multi-tenant environments, specifically:
  - Browser access to both Application Service Provider (ASP)- and Customer-hosted Media Servers.
  - Customer access to ASP-hosted Media Servers.
  - Customer access to Application Administration (start, stop, scheduling).
- Maintain NAM/ICM data security.

ISN System Administration

This section describes ISN:

- System Management
- Reporting
- Error handling

System Management

The ISN system is managed using several tools:

- **Application Administrator**. Web-based tool for Application Server configuration and administration. (See page 4 for more information on this tool.)
- **VB Admin**. Command line interface (CLI) for Voice Browser configuration and administration.(See page 6 for more information on this tool.)
- **ICM Service Control**. Tool for managing the Application Server and Voice Browser service nodes.
- **Dumplog.exe utility**. Tool for displaying per-process log files.

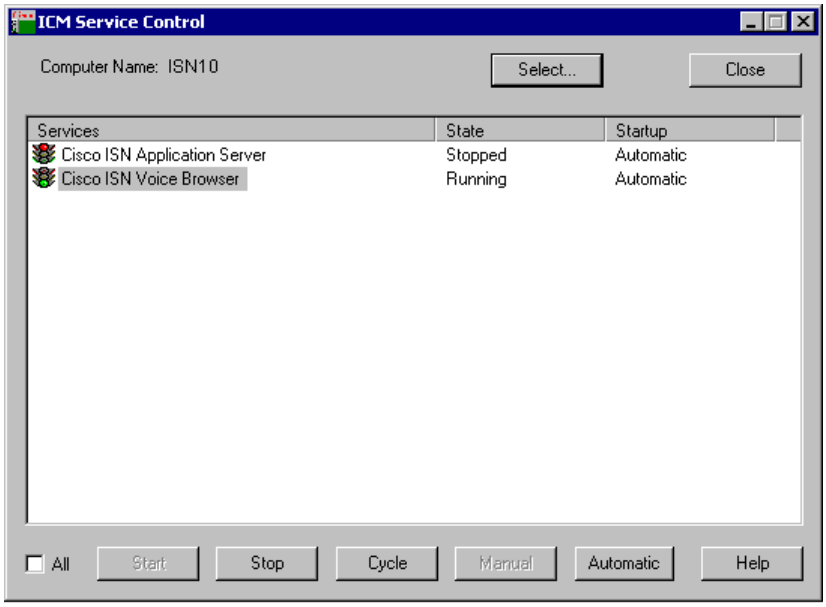
Note For information on using ICM Service Control and the **dumplog.exe** utility, see the *Cisco Internet Service Node (ISN) Configuration and Administration Guide*.

ICM Service Control

The ISN is a node-managed process that runs under ICM Service Control. ICM Service Control allows you to view, start, and stop all Windows services related to the ICM software. ICM Service Control also provides control over all other Windows services—such as the Application Server and Voice Browser—on machines selected through the All checkbox.

Figure 2-6 shows an example of an ICM Service Control window.

Figure 2-6 ICM Service Control Window



ISN Reporting

ISN reporting is provided by the NAM/ICM's capabilities, specifically, termination call detail (TCD) records).

The NAM/ICM creates one TCD record per ISN call, independent of the number of times a call maybe transferred to a new termination endpoint (that is, using the VRU Network Transfer feature). The NAM/ICA also creates a TCD for each *leg* of the transferred call, providing the destination endpoint is managed though another ICM connection (IPCC or ACD-PG).

For example, if a new call arrives at the ISN and receives IVR treatment there, the following call sequence might take place:

1. The ISN connects the call to an IPCC agent.
2. An IPCC agent consults with a second IPCC agent.
3. The IPCC agent transfers the call to the second agent, using the VRU Network Transfer feature such that the ISN performs the takeback and transfer.

The NAM/ICM would create four TCDs as a result of this call sequence:

- The first record representing the entire ISN call.
- The second record for the leg where the ISN connects the caller to Agent 1.
- The third record for the leg where Agent 1 consults with Agent 2.
- The fourth record for the leg where Agent 1 transfers the caller to Agent 2.

These records are correlated through the RouterCallDay and RouterCallKey fields, which will contain the same values for all the TCD associated with this call.

Note If the ISN is connected to the NAM, and agent connection (IPCC or ACD-PG) is at the ICM, the first record representing the entire ISN call will be generated at the NAM and the other TCD records will be generated in the ICM database. In that case, the RouterCallKey field in the NAM is different from the RouterCallKey field in the ICM records. If a link between the NAM and ICM records is required, the NAM can force the NAM RouterCallKey value into the ICM records by using the script to put it in one of the call variables that get passed along to the ICM.

Table 2-2 shows TCD fields of particular interest to ISN users:

Table 2-2 Termination_Call_Detail Record Fields

Field Name	Description
Duration	Total time calling party is connected.
DelayTime	Amount of time before the calling party is connected to the first called party, including connection and ring time to the first called party. **Note** If this call never connects to another party, this value is the same as Duration.
TimetoAband	(Time to Abandon) For calls which are abandoned without ever connecting to a called party (that is, an agent), this value is the same as Duration. For all other calls, TimetoAbandon is 0 (zero).
TalkTime	Amount of time from the connection to the first called party to the end of the call, including (optional) subsequent VRU network transfers.

In addition, the following standard TCD record fields are also populated when used with the ISN.

- Peripheral ID
- Day
- RouterCallKey
- DateTime
- PeripheralCallKey
- CallDisposition
- DNIS
- ANI
- CallerEnteredDigits (for ISN, this field contains the digit(s) for the last digit collection node executed in the ICM router script)

Also of possible interest are ECC variables associated with the ISN call record. In particular, user.media.id can be used to correlate the data to Gatekeeper and Gateway data, and to the log messages in the Voice Browser and Application Server logs.

The TCD records are linked to the RouteCallDetail records which contain more information about the call such as DialedNumber, Label (destination number of connected agent), and CallType.

Note Please refer to Cisco ICM Software documentation for more information regarding these fields.

Service Control Database Reporting

The Service Control Interface reports termination call detail records, service, trunk group, and peripheral real-time records. The VRU PG derives the real-time statistics from the Service Control Messages exchanged with ISN.

ISN Error Handling

ISN error handling and reporting generate information the system can use to:

- Diagnose a system remotely.
- Automatically report service-affecting events.

Some logging is controlled by the user; some logging–such as entries related to error conditions–is always reported.

There are a variety of methods the ISN uses to calculate metrics and handle and report errors:

- Standalone Distributed Diagnostics and Services Network (SDDSN) provides a mechanism for remote diagnosis of component failures.
- Voice Browser and Application Server log files—accessible through the remote connections—enable local diagnosis.

Trace Message Levels

Trace levels are defined during ISN installation and configuration. Some trace messages—such as catastrophic and service-effecting events—will always be logged, regardless of the current trace level settings.

Note It is the customer's responsibility to purchase and configure a server of sufficient capacity for their logging volumes.

Trace messages can be grouped into two categories:

- Those intended to help diagnose problems caused by configuration or network errors, for example, informational, error, and basic call detail messages.
- Those intended solely for use by your support organization or Cisco software developers to diagnose problems which may be software bugs, for example, component-level call detail and debug.

Log files

Log files provide trace messages for information, error logging, and—optionally—for component metrics. Both the Voice Browser and Application Server generate log files. The Application Server files are plain text, accessible through standard means or through the Application Administration Web pages.

The Voice Browser logs can be viewed using the **dumplog.exe** utility.

Example 2-1 shows a sample log file.

Example 2-1 Sample Application Server Log File

```
1579: Jun 22 01:08:53.187 EDT %ISN-SS_HTTP-6-INFORMATIONAL:
% Jun 22 01:08:53 EDT %ISN metrics -----------------------------------
% Jun 22 01:08:53 EDT %HTTP counts:
% Jun 22 01:08:53 EDT %  Total requests:0
% Jun 22 01:08:53 EDT %  Requests in progress:0
% Jun 22 01:08:53 EDT %  Maximum requests:0
% Jun 22 01:08:53 EDT %Call counts:
% Jun 22 01:08:53 EDT %  New calls:0
% Jun 22 01:08:53 EDT %  Calls ended:0
% Jun 22 01:08:53 EDT %  Calls in progress:0
% Jun 22 01:08:53 EDT %  Maximum calls in progress:0
% Jun 22 01:08:53 EDT %Latencies in milliseconds:
% Jun 22 01:08:53 EDT %  New call average (ms):0
% Jun 22 01:08:53 EDT %  New call maximum (ms):0
% Jun 22 01:08:53 EDT %  Call event average (ms):0
% Jun 22 01:08:53 EDT %  Call event maximum (ms):0
% Jun 22 01:08:53 EDT %  Node manager ping average:0
% Jun 22 01:08:53 EDT %  Node manager ping maximum:0
% Jun 22 01:08:53 EDT %
% Jun 22 01:08:53 EDT %Interval 751 result at Fri Jun 22 01:08:53 EDT 2001
% Jun 22 01:08:53 EDT %Object memory in use, bytes:11926064
% Jun 22 01:08:53 EDT %Object memory free, bytes: 436272
% Jun 22 01:08:53 EDT %System up 62:40:00
% Jun 22 01:08:53 EDT %-----------------------------------------------

1580: Jun 22 01:11:04.859 EDT %ISN-LIB_ICM-6-INFORMATIONAL:ICM Metrics:
---
% Jun 22 01:11:04 EDT %  ICM Messages in interval:    10
% Jun 22 01:11:04 EDT %  Interval size, seconds:      305.0
% Jun 22 01:11:04 EDT %  ICM messages since startup:  73
```

Note For more information on generating log files and using the **dumplog.exe** utility, see the *Cisco Internet Service Node (ISN) Configuration and Administration Guide*.

CHAPTER 3

Prompt Recording and Distribution

This chapter provides:

- An overview of ISN media file handling.
- Information about ISN system prompts.

Note For information on using media files and system prompts with ISN micro-applications, see the *Cisco Internet Service Node (ISN) Configuration and Administration Guide.*

Media File Overview

This section presents a brief overview of how ISN performs media file handling. It includes information about:

- What the Media Server is.
- Media file names and types ISN supports
- File address for the media files

Media Server

In ISN, the Media Server is a computer or set of computers, which "serve" the media files that contain messages and prompts that callers will hear. There are two types of Media Servers defined in ISN according to the mechanism where the media file is accessed:

1. File Media Server: Media Files are located on the same machine as the ISN Voice Browser and accessed by the ISN Voice Browser using File protocol.
2. HTTP Media Server: Media Files are located on a remote Web server and accessed by both ISN and the Non-ISN Voice Browser using HTTP protocol. This type of Media Server uses standard Web access methods.

There is no artificial limit on the number of prompts; these pages will be limited only by file system capacity.

Note To maximize ISN performance, do not install the HTTP Media Server on the same machine as the ISN Voice Browser and Application Server.

When the Application Server receives an IVR message from the NAM/ICM software, the VXML page the Application Server generates includes an URL or file location address to the Media Server. The Voice Browser, upon receiving this VXML page, submits an HTTP or FILE request to the Media Server to retrieve the media file.

The Voice Browser maintains several voice buffers so that it can play out to the caller from one buffer while retrieving and filling the others. By not waiting for the entire media file to be read in, the Voice Browser minimizes latency to the caller while also minimizing the amount of memory consumed by the Voice Browser.

The ISN system supports *system prompts* and *application prompts*. System prompts have predefined, well-known names and are used for Play Data functions and for standard error handling.

The system supports libraries of system prompts and libraries of application prompts. Any prompt library may be used in more than one call session; a call session may use multiple libraries.

Tools for prompt creation are off-the-shelf, such as Cool Edit Pro by Syntrillium Software Corporation (http://www.syntrillium.com), and Vox Studio (http://www.xentec.be).

Note It is the customer's responsibility to select the tool, select a voice talent, record the system and application media files for the supported applications and languages in the supported format and encoding, and deploy the media files on the Media Server(s) in the appropriate directory.

It is also the customer's responsibility to select and deploy Media Servers with adequate capacity and throughput.

Media File Names and Types

A *media file name* is specified in the ICM VRU Script Configuration and used in the Run VRU Script request for the Play Media, Get Digits, Menu, and Get Speech (in non-TTS applications) micro-applications. The media file naming convention allows alpha-numeric characters with the underbar character as a separator. (Spaces or hyphens are not allowed.) This naming convention provides a mechanism for an "understandable" naming convention as opposed to numeric media file names typically used by stand-alone VRUs.

Caution The ISN includes a library of media files/prompts for individual digits, months (referenced internally by ISN software for a Play Data script type request), and default error messages, etc. **Creation of a *full set of media/prompts for each locale* referenced by the ISN customer is the responsibility of the customer's Media Administrator.**

The *media file types* ISN supports are Mu-Law 8-bit .wav files and A-law 8-bit .wav files. Media files specified with an extension will be used "as is," for example, **hello.xxx**. (The default file extension is .wav.)

Caution Any unexpected (and unsupported) type of media file encountered will generate the logging of an error and a result code of False will be returned to the ICM along with the ECC **user.microapp.error_code** set appropriately. From the caller's perspective, nothing was played, however it is the Script Editor developer's responsibility to write the script to handle this error condition.

Media File Address

The address for media files that reside on the Media Server(s) is generated by the ISN. The ICM provides information about the file location or base URL address in the ICM/IVR messages it passes when the Run VRU Script node is executed. The ICM/IVR messages include ECC variables for: locale, media server set address, as well as optional system and application library name overrides.

Note For more information, see the *Cisco Internet Service Node (ISN) Configuration and Administration Guide*.

CHAPTER 4

VoIP Routing

This chapter contains information about:

- Using ISN and IP Phones with Cisco CallManager.
- Inbound routing.
- Outbound routing.

It also describes some limitations that exist in the ISN Version 2.0 Voice Browser concerning interaction with VoIP endpoints.

Note This chapter presents an overview of how the ISN uses Voice over IP Routing. For detailed information about the Voice over IP routing *configuration* process, see the *Cisco Internet Service Node (ISN) Configuration and Administration Guide*.

ISN, IP Phones, and Cisco CallManager

The ISN can route calls to Cisco IP Phones, using the signaling services of the Cisco CallManager (CCM), which acts as an H.323 Gateway for the IP Phones.

Note ISN Version 2.0 can also accept incoming calls from an IP Phone. In this case the CallManager connects directly to the ISN Voice Browser in ISN Comprehensive and ISN Queue and Transfer modes, and directly to the gateway in ISN Advanced Speech mode.

While the CCM is similar in some respects to Cisco Voice Gateways, there are also significant differences. For ISN purposes, the most noteworthy difference is that the CCM does *not* support DNS lookups. Thus, when no Gatekeeper is present, all call routing configuration is performed on the CCM.

For ISN to access IP Phones through CCM, certain configuration rules must be followed. Specifically, the ISN Voice Browsers must be defined as *Gateways* on CCM, which enables CCM to receive *multiple* calls from the Voice Browsers.

Note For instructions on how to define a Voice Browser as a Gateway, see the *Cisco Internet Service Node (ISN) Configuration and Administration Guide*.

Inbound Routing

This section describes ISN inbound call routing and the different ways in which inbound calls can be routed to the ISN using H.323 protocol.

At the highest level, ISN Inbound call routing on an H.323 IP network is determined by the presence or absence of an H.323 Gatekeeper.

The choice of whether to use a Gatekeeper is typically determined by the network's size and/or complexity. In general:

- Smaller/simpler networks consisting of 100 or less H.323 endpoints can function without using a Gatekeeper.
- Larger, more complex networks often require a Gatekeeper to consolidate routing information.

Note Throughout the "Inbound Routing" section, an *ISN node* is assumed to consist of one or more physical Voice Browser machines, which are controlled by a logical Application Server through VXML, and the Voice Browsers function as H.323 Gateways.

Gateways and Gatekeepers

A *Gateway* (GW) is an H.323 or SIP device that allows a standard PSTN-based phone, using TDM technology, to access an IP-based network.

There are a variety of ways to tell the Gateway where to route to find the Voice Browser. For instance:

- The NAM/ICM can be configured to tell the PSTN network to route the call to a VoIP Gateway.
- The Gateway can be configured to directly route a call to the Voice Browser based on information provided from the public network or NAM/ICM.
- The Gateway can query a Gatekeeper, which can provide centralized control for a number of Gateways.

A *Gatekeeper* (GK) is an H.323 device that controls route requests originating from H.323 endpoints.

Gatekeepers can provide additional services such as bandwidth control, and permit access to advanced routing servers such as Cisco's NAM/ICM.

The Gatekeeper also has an interface to the NAM/ICM which is called Gatekeeper TMP, which allows the Gatekeeper to query a NAM/ICM system for specific customized routing instructions.

Inbound Call Routing with No Gatekeeper Present

When no Gatekeeper is present, inbound call routing to the ISN is controlled by dial plan information configured at each H.323 originating endpoint, a Cisco Voice Gateway.

Cisco Gateways provide several capabilities:

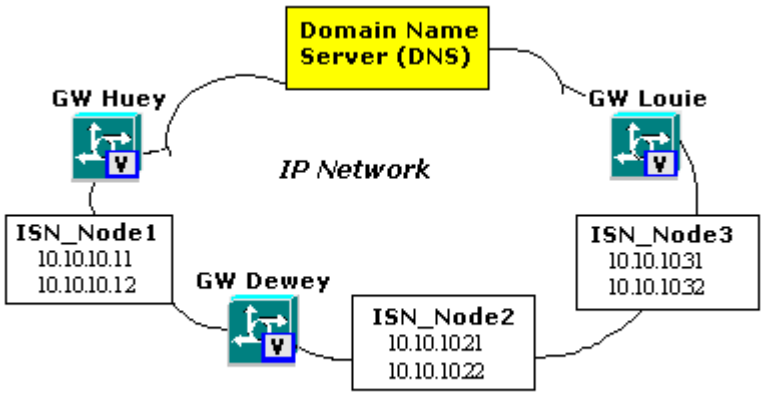
- **Dial-Peers**. A Gateway dial-peer associates a dialed number (or range of numbers, defined by wild cards) with a Session Target. The Session Target can be either an *IP address* (such as **10.10.10.1**) or a *Domain Name* (such as **ISN_1@cisco.com**). If the Session Target is a Domain Name, the Gateway resolves it through the Domain Name Server (DNS).
- **Domain Name Server**. A Domain Name Server (DNS), such as Cisco Network Registrar, can map a Domain Name to one or more IP addresses. If a Gateway DNS query on a dialed number returns multiple IP addresses, the Gateway routes the call to each successive IP address until it obtains a successful connection.
- **Multiple Dial-Peers**. Multiple dial-peers can be specified for the same dialed number, or range of numbers. In this case, each dial-peer associates the dialed number with a different IP address or Domain Name. The Gateway resolves multiple dial-peers according to well-defined rules, including the number of digits matched, target preference, and round robin.
- **Default Route**. Gateways can be configured with a default target that will be used to route any Inbound call not defined in dial-peers.
- **Nearest Voice Browser Option**. If multiple ISN nodes exist in a solution, it might be desirable to have Gateways route inbound calls requiring ISN treatment to Voice Browsers at the nearest ISN node. This is done by configuring each of the Gateways with dial-peers that point to the preferred Voice Browsers.
- **Codecs**. ISN currently supports only two voice codecs for inbound calls: g711 u-law or g711 a-law. (G.729 is supported during IP transfers, only.) ISN codec selection is specified through VB Admin (the Voice Browser command line interface). However, Gateway dial-peers must also be configured to indicate which of the codecs need to be supported. (Dial-peers can be set up to process one or both of the codecs for ISN communications.)

Note For detailed instructions on how to configure Gateways for use with the ISN, see the *Cisco Internet Service Node (ISN) Configuration and Administration Guide*.

Gateway Example

Figure 4-1 shows an H.323 network with three Gateways (Huey, Dewey, and Louie), three ISN nodes, and a Domain Name Server (DNS). Each ISN node contains ***two*** Voice Browsers with the IP addresses noted.

Figure 4-1 Inbound Call Routing, No Gatekeeper



Suppose this network processes calls made to several toll free numbers (800-555-0020 through 0029) and that each call requires ISN treatment before it can be routed to its final destination. In addition, to enhance performance, Gateways should first route ISN calls to Voice Browsers in the *nearest* ISN node (For failover purposes, if the nearest ISN node is unavailable, the Gateways should route ISN calls to Voice Browsers in an alternate ISN node.)

Two ways to accomplish this would be to configure dial-peer Session Targets:

- As *IP Addresses* (for example, **10.10.10.11)**
- As *Domain Names* (for example, **isn_Node2@cisco.com**)

Note By default, all dialed numbers *not* defined as dial-peers are routed to the PSTN.

Session Target Preference

Preferences can be assigned to Session Targets—whether specified as IP Address or Domain Names—so you can indicate a hierarchy of which Voice Browser should be routed to first, which should be second, etc.

Table 4-1 illustrates a possible preference configuration for Gateway Huey:

Table 4-1 Preference Configuration

Node	Session Target ID (Voice Browser)	Preference
ISN_Node1	10.10.10.11	0
	10.10.10.12	0
ISN_Node2	10.10.10.21	1
ISN_Node3	10.10.10.31	2

Note For complete details about the command syntax for setting preferences, see the Cisco IOS documentation.

In this configuration, Huey will attempt to route the call as follows:

- First, Huey will try connecting to one of the two Voice Browsers in ISN_Node1, since they have the lowest preference value (0).
- Next, if the Voice Browsers in ISN_Node1 do not respond properly, Huey will then attempt to route the call to the next lowest preference value (1), which is Voice Browser 10.10.10.21 in ISN_Node2.
- Finally, Huey will attempt to route the call to Voice Browser 10.10.10.31 in ISN_Node3.

Inbound Call Routing With a Gatekeeper Present

When a Gatekeeper is present, Inbound call routing to the ISN is controlled by information kept at one or more H.323 Gatekeepers.

Cisco Gatekeepers provide several capabilities:

- **Zones**. H.323 enforces the concept of *zones*, where a single *logical* Gatekeeper (which might consist of one or more actual Gatekeepers) is responsible for routing control within its zone. The Gatekeeper can be configured to associate each dialed number (or range of numbers) with a prioritized list of target endpoints, in the case of the ISN, a list of Voice Browsers.

  When an originating endpoint queries the Gatekeeper for routing information, the Gatekeeper tries to find the *longest* match with its list of dialed numbers. If a match is found, the Gatekeeper selects the associated target with the highest priority, and returns its IP address (along with any alternate endpoint IP addresses) to the originating endpoint. If all the associated targets for the matched number have equal priority (and have available resources), then the Gatekeeper selects one of those targets *at random*, and returns its IP address (along with any alternate endpoint IP addresses) to the originating endpoint.
- **Alternate Endpoints**. A Gatekeeper can be configured with a list of alternate endpoint IP Addresses for each target endpoint. When an originating endpoint (that is, a Gateway) queries the Gatekeeper for routing information, the Gatekeeper returns the IP Address of the target endpoint, plus the IP Addresses of any alternate endpoints for the primary target. First, the Gateway attempts to route the call to the primary target. If the primary target does not respond properly, the Gateway tries the other destinations, in the order defined in the alternate endpoint list.
- **Out of Service Condition**. If the Gatekeeper finds that a target—that is, a Voice Browser—is out of service (either the Voice Browser has not re-registered during the keep-alive period or has sent a explicit message to “unregister”), the Gatekeeper *will not*:
  - **Choose that Voice Browser as a target**. For example, if VB#1 is registered at the Gatekeeper with VB#2 as its alternate endpoint, and VB#1 goes out of service, then the Gatekeeper will only return the IP Address for VB#2 (along with IP Addresses for *its* alternates).
  - **Update its alternate endpoint lists**. For example, if VB #1 is registered at the Gatekeeper with VB #2 and VB #3 as its alternate endpoints, and VB#2 goes out of service, the Gatekeeper will still return the IP Address for VB#2 on any lookups where VB#1 is the target endpoint.
- **Resource Availability/Unavailability**. A Voice Browser can also indicate Resource Unavailability/Availability to the Gatekeeper:

  - If a Voice Browser indicates Resource Unavailability, the GK will move that Voice Browser to the *bottom* of its routing priority lists. (This means the GK can still route calls there, if higher priority targets go out of service).
  - If the Voice Browser later indicates Resource Availability, the GK will place it back at the priority listed in the zone prefix command.

- **Re-Queries**. Gateways can be configured to re-query the Gatekeeper if the target Voice Browser (plus any alternates) does not properly respond to call setup. If the target Voice Browser goes out of service during the time period between the original GK query and the re-query (because either the Voice Browser has failed to re-register during the keep-alive period or the Voice Browser has unregistered with a URQ message), then the re-query can return a *different* target Voice Browser.

  Note The time period between the original query and the re-query is short, so there may be limited benefit to re-queries

- **Technology Prefix**. A Gatekeeper requires all Gateways (including the ISN Voice Browsers) to register with a Tech Prefix, where the Tech prefix precedes the dialed number and is simply a number followed by the # sign. (By default, the ISN Voice Browsers all register with the Tech Prefix 2#.)

  All Gateways in an H.323 zone of a given type (for example, all Voice Browsers) register with the Gatekeeper with the same Tech Prefix; the Gateways prepend it to the dialed number that they pass to the Gatekeeper. The Gatekeeper is configured to recognize the Tech Prefix and associate it with a list of Gateways. Once the tech prefix association is made, the Gatekeeper uses its zone prefix configuration to determine which associated Voice Browser to route the call to. After the Gatekeeper indicates the target Voice Browser to the querying Gateway, the Gateway prepends the same tech prefix to the dialed number it passes to the target Voice Browser during H.323 call setup. The Voice Browser strips off the tech prefix before passing the dialed number to the ISN Application Server for further processing.

  There is a situation where an ISN Voice Browser would register with the 1# tech-prefix. That situation is as follows: If the ISN Voice Browser is a Type 2 VRU (target of an ICM translation route) and the switch that is directing the call to it is itself an ISN Voice Browser, then the Type 2 Voice Browser must be tech-prefix 1#. By default, ISN Voice Browsers register as 2# for inbound call routing. This value would need to be adjusted via the Voice Browser CLI after installation. The reason is that unlike a gateway, the Voice Browser routing the call cannot prepend a tech-prefix to the called-number. Therefore the gatekeeper must choose from endpoints that are registered in its default technology prefix (1#).

- **GKTMP Option**. A Gatekeeper can query another server for routing information using the Gatekeeper Transaction Message Protocol (GKTMP). The GKTMP is a RAS-like protocol that gives an external application like the NAM/ICM the ability to override Gatekeeper behavior. GKTMP can be used to perform *conditional* routing to the ISN Voice Browsers. For example:
  - If an agent is available, do not route the call to the ISN; route it directly to the agent.
  - If today is Monday, do not route calls to the ISN.
  - Route the Inbound call to an ISN Voice Browser *nearest* to the originating Gateway.

Note The current version of the Gatekeeper only allows the GKTMP interface to be "on" or "off." That is, the Gatekeeper will either query a GKTMP server like the NAM for *all* calls, or none of the calls. This means that if GKTMP is desired for conditional routing into the ISN (recommended), it must also be used on all ISN lookups to the Gatekeeper for call transfers. However, this latter lookup is superfluous if the NAM/ICM is the GKTMP server, as the NAM has already made the routing decision by the time the ISN does a Gatekeeper lookup. In this case, the NAM would need to be configured to perform the equivalent of a "null" lookup for the ISN's GKTMP queries.

Gateway Configuration

If a Gatekeeper is present in an inbound routing configuration, you can minimize Gateway configuration. It is recommended that the Gateways be configured to always query the Gatekeeper for routing information. This may be done by specifying a *wildcard dial-peer.*

Note For detailed instructions on how to configure wildcard dial-peers on Gateways, see the *Cisco Internet Service Node (ISN) Configuration and Administration Guide*.

Gateways not in the ISN zone must be configured to query their own zone Gatekeeper for routing information. The originating Gatekeeper will discover the ISN Zone Gatekeeper through an H.323 Location Request (LRQ) message. The ISN Zone Gatekeeper will determine proper routing, which will be returned to the originating Gateway (by way of the originating Gatekeeper).

Nearest ISN Node Option

For performance reasons, it may be desirable to route inbound calls to the ISN node *nearest* to the originating Gateway. Aside from using the GKTMP interface, this can be accomplished by setting up separate H.323 Zones for the different ISN nodes.

Note While H.323 requires each zone to be controlled by a single (logical) Gatekeeper, there is nothing to prevent multiple zones from being controlled by the *same* Gatekeeper. However, ISN Version2.0 **does not** support *multiple* logical Gatekeepers on the same physical Gatekeeper machine. For ISN 2.0, multiple Gatekeepers must be implemented on separate Gatekeeper machines.

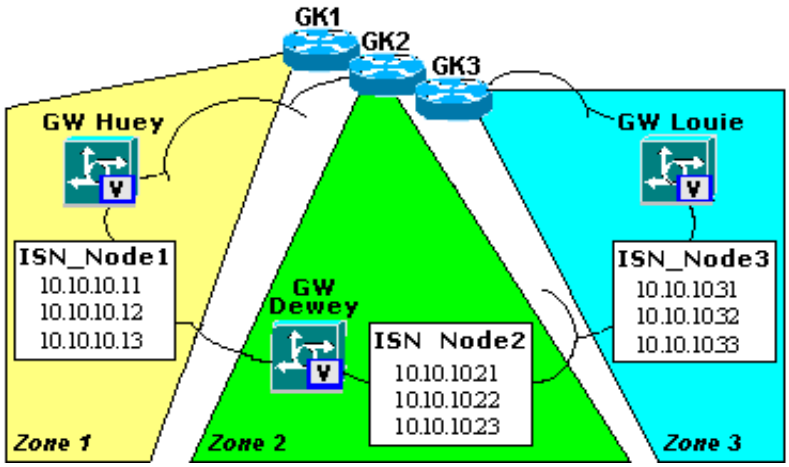
Gatekeeper Example

Figure 4-2 shows ISN nodes and Gateways placed in three different H.323 zones:

- ISN_Node1 and Gateway Huey are assigned to Zone 1, which is controlled by GK1.
- ISN_Node2 and Gateway Dewey are assigned to Zone 2, which is controlled by GK2.
- ISN_Node3 and Gateway Louie are assigned to Zone 3, which is controlled by GK3.

Each ISN node contains *three* Voice Browsers, with the IP addresses shown, each of the Voice Browsers is registered with its Gatekeeper, and the Gateways are configured to perform RAS lookups in their Gatekeeper for incoming calls.

Figure 4-2 Inbound Call Routing, With Gatekeepers



The Gatekeeper is divided into three logical Gatekeepers (GK1, GK2, and GK3); the ISN Nodes register with their appropriate Gatekeeper. Gateways would, in turn, be assigned to a zone, based upon the nearest ISN node. Each logical Gatekeeper is configured with the same list of supported numbers, but *associated* with Voice Browsers in *their own zone's* ISN node. (For example, GK1 would point 800-555-0010 toward Voice Browsers at ISN_Node1, while GK2 would point 800-555-0010 toward Voice Browsers at ISN_Node2.)

Calls which enter the IP network thorough a Gateway in Zone 1 (GW Huey) would query GK1 for routing information, which would return the IP Address for a Voice Browser at ISN_Node1.

Note More than one ISN node may be placed in each zone, in which case prioritized routing and/or alternate endpoints capabilities may also be used. However, alternate endpoints cannot be used to reroute calls to a different zone if all targets in the first zone are unreachable.

Another method of implementing nearest node routing is to use multiple *tech-prefixes*, where "neighboring" Gateways and Voice Browsers can be configured to support the same tech-prefix. Referring to Figure 4-2 again:

- The Voice Browsers at ISN_Node1 would register at a Gatekeeper with the tech-prefix **2#**.
- The Voice Browsers at ISN_Node2 would register at the same Gatekeeper with the tech-prefix **3#**.
- Gateway Huey's dial-peers would be configured to pre-pend **2#** to all RAS queries to the Gatekeeper.
- Gateway Dewey's dial-peers would be configured to pre-pend **3#** to all RAS queries to the Gatekeeper.

With this configuration in place, when Huey performs a RAS lookup at the Gatekeeper, the Gatekeeper will only return IP addresses for the Voice Browser's at ISN_Node1.

Note For detailed instructions on how to configure Gatekeepers for inbound routing, see the *Cisco Internet Service Node (ISN) Configuration and Administration Guide*.

Call Transfers and Outbound Routing

This section examines *initial* call transfer from the ISN, specifically, how the NAM/ICM, ISN, Gatekeeper, and Voice Gateways work together to perform H.323-based call transfer.

Note Subsequent call transfers (such as agent initiated transfers), being similar to the examples described below, are not discussed separately. One important difference, however, is that the **Call.NetworkTransferEnabled** variable must be set to 1 in each script that contains network transfer instructions.

Outpulse Transfer Mode

When the ISN receives the ICM/IVR message from the NAM/ICM, the ISN examines the initial two characters in the Label field to determine the transfer mode. If the initial four characters are **DTMF**, then the ISN will use *outpulse transfer* mode to transfer the call. Outpulse transfer mode instructs the ISN to send the transfer information to the originating Voice Gateway, which will then outpulse the information to the ingress leg of the call. This initiates the call transfer in an external telephony network.

Note When the *outpulse* mode is used, the first two characters of the *transfer information* may be an *attention sequence* for the telephony network, such as ***8**.

The ISN initiates the outpulse transfer by stripping off the **DTMF** characters from the Label field, and sending the remaining transfer information to the originating Voice Gateway, using the call's existing H.245 control session. (The transfer information is passed in an H.245 userInputIndication message.)

Gatekeeper Configuration and Behavior, Outpulse Transfer

With outpulse transfer mode, the ISN communicates with the incoming Gateway, which already has an H.245 control session for that particular call. Therefore, the ISN does not need to perform a lookup in its assigned H.323 Gatekeeper, and can proceed directly with the transfer.

Gateway Configuration and Behavior, Outpulse Transfer Mode

A Voice Gateway can provide access to a Time-Division Multiplexing (TDM) switching network; or it can be connected to an ACD, PBX, or to one or more phones.

In outpulse transfer mode, the originating Gateway receives transfer information from the ISN for a particular call through H.245 messaging. The Gateway converts the transfer information to DTMF signals and outpulses them to the call's ingress TDM leg. From that point, the call transfer becomes the responsibility of equipment on the TDM network.

Two things must happen for the Gateway to support relay of the H.245 information:

- First, the Gateway must have been configured to support H.245 relay for that particular call. This is done by adding an **H245 relay** command to the dial-peers that route inbound calls to the ISN. The **H245 relay** command provides the option of choosing either the **signal** or **alphanumeric** methods of relay. The **signal** option is recommended for use with the ISN.
- Second, the ISN must indicate support for a compatible method of H245 relay during the H.245 capabilities exchange with the Gateway.

The ISN must then use that method when it sends the H.245 userInputIndication message to initiate the call transfer. If the ISN does not indicate a compatible method of H.245 relay during the capabilities exchange with the Gateway, the Gateway reverts to its default mode of **no** H.245 relay.

IP Transfer Mode

When the ACD is connected to the VoIP network, the ISN can be treated as a network control point—a place for the ACD to access advanced network features. The ISN is an excellent vehicle for implementing those features because of its voice processing ability and position in the network. Invoking such a feature requires that the ISN stay involved with a call even after it has been transferred to another VoIP endpoint. Staying involved with the ACD endpoint means using H.323 to redirect the audio stream to a new endpoint, previously the Voice Browser and now the ACD, while the signaling control path is unchanged. The control path still terminates at the ISN, but ISN switches the audio path. This is called the *IP transfer mode* of operation because the ISN is creating an outgoing call leg.

In IP transfer mode, the NAM/ICM:

- Determines the type of transfer and the destination for the initial call transfer to be performed by the ISN.
- Passes this information to the ISN through the ICM/IVR message.
- Specifies transfer information in the **Label** field of the CONNECT message.

The ISN will perform a lookup in its assigned Gatekeeper to determine the IP Address of a destination endpoint to which it should transfer the call. These steps are discussed in greater detail in the following sections.

ISN Behavior, IP Transfer Mode

In IP transfer mode, the ISN must obtain the IP Address of the VoIP destination endpoint to which it will transfer the call. This requires the ISN to perform an H.323 RAS lookup to its assigned Gatekeeper. Specifically, the ISN Voice Browser sends the Gatekeeper an ARQ (Admission Request) message, passing the contents of the CONNECT Label. After the Gatekeeper returns an ACF (Admission Confirmation) message, the ISN Voice Browser attempts to transfer the call to the destination endpoint. As part of the call setup, the ISN passes the *transfer information* to the destination endpoint.

If the destination endpoint does not respond correctly to the call setup, the ISN shall successively try to transfer the call to the alternate endpoints.

The ISN shall *not* perform additional lookups in the Gatekeeper if it cannot successfully transfer the call to the destination endpoint or one of its alternates (as the Gatekeeper cannot provide any additional routing information). Instead, the ISN can provide treatment under NAM/ICM script control (such as play a message and hang up).

Gatekeeper Configuration and Behavior, IP Transfer Mode

The Gatekeeper's primary responsibility in outbound routing is to determine the IP Address of the VoIP destination endpoint, based on the transfer information the ISN sends it in the ARQ (Admission Request) message.

Unlike inbound calls to the ISN, the Gatekeeper is *not* expected to use the GKTMP interface to query a separate server (such as the NAM) for call routing information on transfers from the ISN. (The reason for this is that the NAM has already determined the transfer destination by this point in time, so another lookup from the Gatekeeper is unnecessary.)

The ISN's assigned Gatekeeper must know whether it "owns" the destination endpoint, or whether it belongs to another Gatekeeper. If the endpoint is:

- In the ISN Gatekeeper's zone, then the ISN Gatekeeper can determine it directly.
- In a different zone, the ISN Gatekeeper must determine which Gatekeeper does own it.

An efficient way to do this is by using Gatekeeper **zone** commands. For example, suppose that the ISN Gatekeeper (GK-A) controls Zone A, which supports numbers in the 408 area code; while GK-B controls Zone B, which supports the 617 area code. Instead of having GK-A send out queries to determine which Gatekeeper owns 617 numbers, GK-A can be configured using a **zone prefix** command so that it "knows" that GK-B owns them. This means that, whenever the ISN requests destination information for a 617 number, the GK-A can immediately communicate with GK-B to determine the correct endpoint.

Note For more information on Gatekeeper IOS commands, see the Cisco IOS documentation. For detailed examples of how to configure Gatekeepers for use with the ISN, see the *Cisco Internet Service Node (ISN) Configuration and Administration Guide*.

Gateway Configuration and Behavior, IP Transfer Mode

A Voice Gateway can provide access to a Time-Division Multiplexing (TDM) switching network; or it can be connected to an ACD, PBX, or to one or more phones.

In *IP transfer* mode, once the Gatekeeper has determined the destination endpoint name during ARQ processing, the Gatekeeper must then find the endpoint's IP Address. The Gateways provide this information when they register with their Gatekeeper.

As discussed in the "Gatekeeper Configuration and Behavior, IP Transfer Mode" section on page 4-10, one way to manage the mapping of the transfer information to destination endpoints is by having the Gateways pass a list of their supported E164 numbers when they register with their Gatekeeper. This is done using the **register e164** command for each dial-peer destination pattern that the Gateway should register with the Gatekeeper. Only fully-qualified destination patterns (that is, completely defined numbers with no wild cards) may be registered in this manner, and different Gateways may not register with the same numbers.

Gateways should be configured to notify their Gatekeeper (through H.323 RAI message) if they are unable to accept additional calls. This will prevent the Gatekeeper from selecting those Gateways as destination endpoints for ISN IP mode call transfers.

It is expected that Gateways will provide access to call center ACDs in many ISN implementations. Care must therefore be taken to configure the Gateway dial-peers to conform with ACD dial-plan requirements. A discussion of how this may be accomplished is given in the Examples section.

Codecs

When the call is being transferred, the ISN Voice Browser negotiates the codec between the ingress Gateway and egress Gateway (or CallManager) for the rtp packetized voice connection. Note that the Voice Browser merely proxies the codec capability set between the ingress and egress gateways. If the desired transfer codec is G.729, for example, then the terminating Gateway must be configured with G.729 as its default (highest preference) codec.

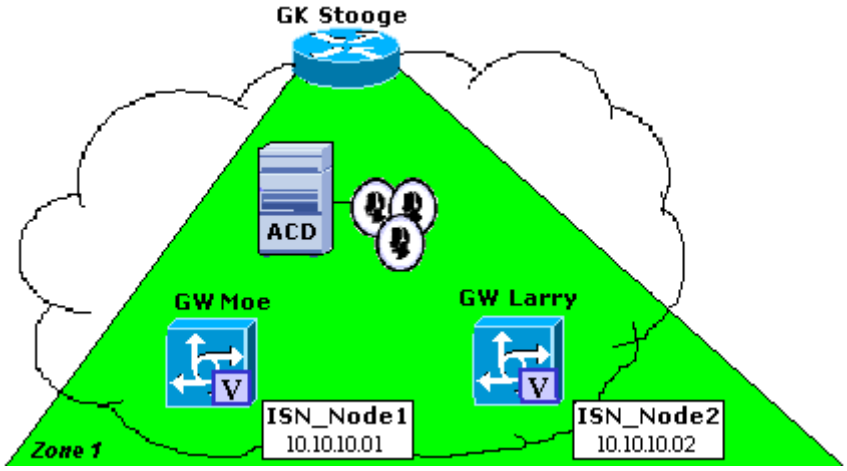
In the Comprehensive mode of ISN there is also a switched transfer that occurs when there is a need to perform ASR/TTS IVR treatment. In this case, the transfer is always to a Cisco VXML-enabled voice gateway. Only voip dial-peers are involved in that transfer (no pots dial-peer). The target voip dial-peer **must** be configured for G711Ulaw since that is the only codec that is supported as of this writing by the known ASR/TTS vendors.

Note For more information on Prompt Codec and IPCC Transfer Codec commands, see the *Cisco Internet Service Node (ISN) Configuration and Administration Guide*.

IP Transfer Example (ACD Routing)

The ISN uses a Gatekeeper to determine the correct VoIP endpoint to transfer calls to when it uses the IP mode. In Figure 4-3, our endpoints are two Voice Gateways, *Moe* and *Larry*, which provide redundant access to a call center ACD. Moe has the IP address 10.10.10.1, while Larry has the IP address 10.10.10.2. For simplicity's sake, we assume the Gateways and the ISN are in the same H.323 zone, controlled by Gatekeeper *Stooge*.

Figure 4-3 IP Transfer Example



In this example, the ACD uses a numbering plan in the format **xxxxyyzzzz**, where:

- **xxxx** is a location code.
- **yy** is the destination trunk group on the ACD.
- **zzzz** is the DNIS (Dialed Number Identification Service), identifying an ACD agent skill group, service, extension, etc.

The ISN initiates the transfer using all these digits:

- The Gatekeeper uses the **xxxx** digits to determine a destination Gateway (8888 for the ACD in our example).
- The Gateway uses the **yy** digits to determine the correct ACD trunk group.
- The Gateway outpulses the **zzzz** digits to the proper ACD trunk group, which uses them to connect the call to an agent.

Since the ACD numbering plan is simple and well-known, we specify the routing information—including Alternate Endpoint instructions—directly on the Gatekeeper, instead of having the Gateways pass the information during Gatekeeper registration. (In fact, since Moe and Larry support the *same* set of numbers, the Gatekeeper would not even allow them to jointly register with those same numbers).

Note For detailed instructions on how you might configure Gatekeeper Stooge and Gateways Moe and Larry for this routing scenario, see the *Cisco Internet Service Node (ISN) Configuration and Administration Guide*.

A

ACD Automatic Call Distributor

AIN Advanced Intelligent Network, a broad term encompassing a carrier's interface to adjunct computing devices like the NAM.

ANI Automatic Number Identification (calling party number).

Application A specific set of customer call-processing business rules as captured in the customer's custom NAM/ICM scripts, the customer's custom prompts, and any database lookups/API interactions defined to the NAM/ICM. Generally these rules will apply to a specific customer function.

App Admin Application Administrator, an ISN configuration and administration tool with a Web browser interface, which you use to perform tasks such as taking the Application Server engine in- and out-of-service, and monitoring system and call status.

Application Developer The person who designs and writes the NAM/ICM scripts which comprise the logic of the application.

Automated Speech Recognition (ASR) The ability to provide speaker independent voice recognition for gathering information form the calling party.

ASP Application Service Provider.

AS or App Server Application Server, one component of the ISN. The VXML application responding the voice browser.

AVVID AVVID (**A**rchitecture for **V**oice, **V**ideo and **I**ntegrated **D**ata) is the foundation of tomorrow's converged enterprise communication networks. This architecture encompasses converged client devices, infrastructure hardware/software, directory services, call processing, telephony/data applications, network and policy management, and service and support.

Application Prompts The customer's custom prompts for use with their NAM/ICM scripts.

Asynchronous Communications See "Out-of-band Communications."

B

Bearer Path Term referring to the actual voice path (RTP stream in VOIP), as opposed to a data or signaling path for call control.

Blind Transfer Generally, a transfer is the handing-off of a call from one agent/number to another agent/skill group/number. In a blind (or single step) transfer, the transfer is made without the initial "agent" determining whether the second "agent" is willing/able to take the call—and is thereby distinguished from a consultative transfer. Blind transfer can be provided by a premise switch, an Intelligent Network, or through a VRU (when supported). The ISN supports blind transfer, referred to as VRU Blind Transfer.

C

Call Context The collection of per-call information pertaining to a given call, used in conveying call (and caller) information between call routing service points. Call context typically refers to the set of peripheral (call) variables and/or ECC data gathered for the call (that is, caller account number, PIN, etc.); this data is moved to the CTI desktop via translation routing and is also used in ICM reporting (Termination Call Detail and Call Route Detail).

Caller The person who originates the session by picking up the phone and dialing the number which terminates on an ISN port.

Call segment Each time the call adds, drops or changes a participant, a segment ends and a new one starts. The first segment occurs between the caller and the ISN, the second between the caller and an agent (or other called party), the third may be either.

Called party The party who answers the second leg of a transferred call. They become part of the call when the ISN initiates an outbound call. Their only actions (as recognized by the ISN) are to either (a) answer the call or to (b) hang up.

Central Controller The computer or computers running the ICM router and ICM database manager (Logger). In addition to routing calls, the Central Controller maintains a database of data collected by the Peripheral Gateways.

CICM Customer ICM. In the optional two-tier service bureau (carrier) configuration, the CICM is the tier providing the carrier customer-specific routing function. CICM's receive customer-specific call route requests from the NAM; they typically perform more elaborate scripted call routing using customer-specific advanced services or agent and skill context. See NAM below.

Consultative Transfer Generally, a transfer is the handing-off of a call from one agent/number to another agent/skill group/number. In a consultative transfer, the transfer is made only after the initial "agent" determines whether the second "agent" is willing/able to take the call—and is thereby distinguished from a blind transfer. When ISN is deployed premise based, it can be used as a switch, and queuing point, for consultative transfer. (Note that ICM does not support consultative transfer with Network based switches or VRUs.)

D

DDSN Distributed Diagnostics and Service Network

DLL Dynamic Link Library

DNIS Dialed Number Information Service (called party number)

DTD Document-Type-Definition. Syntax rules for an XML document.

dumplog A command line utility (dumplog.exe) you used to view the Voice Browser log files. The command reads the file, formats the event data, and writes the formatted data to the workstation screen.

E

ECC **E**xpanded **C**all **C**ontext variables used n the Script Editor, but also passed to VRU or ISN through ICM/VRU messaging. All ECC variables have fixed names.

Empty Capability Set Specification within H.225 which specifies the mechanism for transferring calls while maintaining call control.

EMS Event Management System. As used by ICM, EMS is a library of API calls that provide a framework for storing system events to a local log file and for formatting the alarm traffic sent to SDDSN. Some ISN processes (nmm, nodeman, voicebrowser, af) use the API for local process logging. All ISN components use the API for generating the alarm events that are sent to the SDDSN.

Endpoint (EP) A device that can accept/originate VoIP calls.

Enterprise A singular company or agency, possibly spanning multiple call centers. The Enterprise ICM configuration consists of single-tiered ICM topology, where the PSTN interface receives and responds to call routing requests wholly targeted at the enterprise itself. (This is in contrast with the two-tiered NAM model deployed for service providers.)

G

Gatekeeper, GK An H.323 device that controls route requests originating from H.323 endpoints.

Gateway, GW An H.323 or SIP device that allows standard PSTN-based phone, using TDM technology, to utilize an IP-based network.

Get Digits, GD Micro-application that plays a media file and retrieves digits.

Get Speech, GS Micro-application that collects ASR input after prompting a caller.

GKTMP Gatekeeper Transaction Message Protocol

H

HTML Hypertext Markup Language

I

ICM Intelligent Contact Management.

ICM/IVR Service Control Interface Formerly called *GED-125 VRU Service Control Interface*.

In-band Signaling Using the audio path of a telephone call to signal the network; this usually implies DTMF.

Initial Routing Client The first ICM Routing Client that uses a New Call message to announce the call to the ICM Router. This Routing Client will also be the only Routing Client eligible to receive a Network Transfer Connect.

Internationalization The process of (re-) engineering an information product so that it can be easily adapted for native use in any locale around the world.

IPC Inter Process Communication. Used to pass data between separate local or remote processes.

IP-IVR IP based IVR product produced by Cisco.

ISN Internet Service Node

ITSP Internet Telephony Service Provider

IVR Interactive Voice Response. See *VRU*. (Cisco makes no distinction between these terms.)

IXC Inter-exchange Carrier. A long-distance telephone company owning or controlling the voice and control network infrastructure. AT&T, MCI and Sprint are examples of IXCs in the domestic North American market.

L

Label A text string issued by the NAM to its routing client in response to a route request. Labels are predefined using the ICM Configuration tool. A label is a symbolic representation of the exact target location. Labels are free-form and the format is generally dictated by the specific peripheral (ACD, VRU, ISN, PSTN, etc.)

Locale An identifier for a particular combination of language, region and optional variant. In the context of the ISN, this defines:

- Part of the directory structure for accessing media files.
- The grammar to be used when playing numbers and dates.

Localization The process of adapting an internationalized information product for use in a specific locale.

M

M, Menu — Micro-application that plays a menu media file and retrieves the digit entered as the menu choice.

Micro-App or Micro-Applications — General term for a specific, predefined function in the ISN that can be invoked from the ICM. Micro-applications for ISN consist of: Play Media, Play Data, Get Digits, Get Speech, and Menu.

MDS — Message Delivery System. The mechanism used to provide IPC messages in the ICM system.

Media Resource Control Protocol (MRCP) — Protocol defined by Cisco, Nuance and Speechworks for providing ASR and TTS capabilities.

MIB — Management Information Base. The MIB defines all the information about a managed system that a manager can view or modify. The **isnlarms.mib** file is a text file in a standard MIB format, provided for third party software interpretation of the SNMP traps. The **isnlarms.mib** file is installed on the Voice Browser and Application Server target machine in the directory **<***destination location***>\bin**.

N

NAM — Network Applications Manager. In an two-tier service bureau (carrier) configuration, the NAM is the tier providing direct communication with the carrier PSTN. Route requests arrive at the NAM from the IXC carrier network and are forwarded, based on specific call properties, to the appropriate Customer ICM (CICM). A NAM usually contains only a small configuration that allows it to directly route a subset of calls and dispatch other calls to the appropriate CICM. The NAM receives route responses from all CICMs and forwards them to the carrier network.

NIC — Network Interface Controller. The ICM process that enables communication to the Inter-Exchange Carrier's (IXC) signaling network. NICs typically communicate with the PSTN SSP via the ICM SS7 gateway or directly to customer service control points (SCP) using UDP/IP or X.25. The NIC receives call routing requests from the IXC network, formats and transfers them to the ICM router, and subsequently obtains routing labels in response and returns them to the IXC signaling network.

NMM — Node Manager Manager (manages the NM process(es)). One nmm can manage multiple nm processes even for different components.

Nodeman — Node Manager, self-healing feature of Cisco ISN, NAM, and ICM software.

Node Managed Process — A fundamental concept within the ISN NAM's platform. Node managed processes are started, stopped, and monitored by the platform.

O

Out-of-band Communications — A connection to the Voice Browser initiated by the Application Server for processing information asynchronous to the normal call steps, for example, for transferring a queued call.

Out-of-band Signaling Using a shadow data path to signal the network; ISDN is an example of out of band signaling.

Outpulse Transfer The ability to perform a transfer by sending DTMF tones to a carrier network indicating a transfer should occur, and the destination PSTN address. An example is ATT's transfer connect.

P

PG Peripheral Gateway, a basic component of the ICM distributed system. The PG consists of a dedicated set of ICM processes and typically resides on a dedicated machine; it communicates directly with the peripheral (ACD, PBX, VRU) at the Call Center. The PG reads status information from the peripheral and forwards it to the ICM Central Controller. The PG may itself be a *routing client*, generating route requests to the Central Controller and receiving route responses in return. A PG hosts one or more *PIMs*.

Phone Home Refers to a capability of the Cisco Remote Monitoring Suite to report alarms back to a customer support center. This can be used, together with SDDSN, to provide alarm reporting for ISN.

Play Data, PD Micro-application that retrieves data from a storage area and plays it to the caller in a specific format, called a *data play back type*.

Play Media, PM Micro-application that plays a message to the caller.

Post-route The ICM concept that enables the ICM to execute secondary routing decisions after a call has been initially terminated at the ICM-determined destination (for example, a Call Center agent). Post-routing allows the ICM to process calls when an ACD, VRU, or PBX receiving the initially routed call in turn generates a route request. Like pre-route requests, an ICM router call type and script is used to determine the resolved destination label for the request.

Pre-route The ICM concept that enables the ICM to execute routing decisions before a call terminates at the ICM-provided destination (for example, a Call Center). With pre-routing, the routing client receives the route request from the IXC and presents the request to the Central Controller. Based on a call type and associated ICM routing script, the ICM router (typically using real-time PG data) generates a routing label back to the routing client, which in turn presents it to the IXC.

Procmon Process Monitor. A console process tool used to troubleshoot information on the ISN through ICM processes. Procmon can be run locally from Windows 2000 command prompt or remotely from a Telnet session.

prompt A media file played to the caller.

PSTN Public Switched Telephone Network. The public telephone number, providing the capability of interconnecting any home or office with any other. The term is typically used to pertain to any given country telephone domain, e.g. domestic US and European carrier networks (and local PTT) alike.

R

RAI Resource Availability Indication. A message sent from an H.323 endpoint (like the Voice Browser) to a gatekeeper informing it that resources are low and that it should stop allowing calls to that endpoint. When the resources are again available, another message is sent to reverse the effect.

Requesting Routing Client In Network Transfer, the Requesting Routing Client is the ICM Routing Client that initiated the Post-Route Request that started the ICM routing script that is performing the Network Transfer.

Routing Client An entity or abstraction capable of generating control path call route requests to the ICM system. Each ICM logical interface controller (that is, the NIC) is mapped to one or more routing clients. A routing client typically corresponds to a subsystem within an IXC or to a peripheral performing ICM *post-routing*.

S

SCP Service Control Point. A node in the IXC signaling network responsible for database routing functions and billing. The ICM can both communicate with the SCP or appear as the SCP, depending upon signaling network topology and deployment capabilities.

SDDSN Standalone Distributed Diagnostics and Service Network. Also known as the "Mini-logger," this system allows non-ICM products to use the logging system in a standalone fashion.

Service Node A network-addressable resource providing specialized call services beyond those found in a VRU. In Intelligent Network (IN) terms, a Service Node and VRU (or Intelligent Peripheral, IP) can both provide VRU and queuing functions. A Service Node, however, also has the additional ability to perform call switching and call control – whereas the VRU alone does not. For example, since the Cisco ISN product can initiate call transfers, it's a Service Node. (In IN, the IP prompt / collect / queuing services belong to the Service Control Function.)

Service Provider The term pertaining to IXC carriers; those companies owning or controlling some aspect of the PSTN. Service Providers typically deploy the ICM in a two-tiered NAM configuration (NAM and CICM) to offer enhanced call routing services to their own customers. (Contrast with Enterprise.)

SIP Session Initiation Protocol

SNMP Simple Network Management Protocol

Socket An IPC mechanism that is supported on a variety of platforms. Allows for data to be passed between processes on both local and remote systems.

Source Routing Client The Routing Client through which a call is transferred to the VRU. (In most cases this will be the *Initial Routing Client.*)

Stable Call A call with an established audio path and no background switching activity taking place.

Switched Mode Referring to the ISN, the switched mode is when the ISN moves a call within the IP network and continues to receive signaling events.

Syslog UNIX based logging mechanism similar to the Windows NT Event Viewer.

System Prompt A set of prompts that are predefined by the ISN platform.

System Standard Prompts A set of pre-defined prompts used by the system for the playback of dates, times, currency, errors, etc.

T

Text to Speech Synthesis (TTS) Ability to convert text string to speech for playing to calling party.

TDM Time Division Multiplexing. Used to process calls in a circuit switched network.

TNT Take Back And Transfer, a feature whereby a call is redirected from one target location to another. TNT helps to eliminate tandem connections between call centers by rearranging the network's switched connection.

Traditional Translation Route A target at a peripheral that does not map to a specific service, skill group, or agent. When a call arrives with the trunk group and DNIS corresponding to a translation route, the PG determines the ultimate target. When the ICM routes a call to a translation route, it sends a preliminary message to the PG. For example, the PG might be instructed to coordinate with a host computer so the caller's account number is displayed on the CTI desktop application of the agent receiving the actual call. *See also: Translation Route to VRU*.

Translation Route to VRU A target at a Peripheral Gateway that does not map to a specific service, skill group, or agent. When a call arrives at a translation route, the Peripheral Gateway (PG) is responsible for determining the ultimate target. When ICM software routes a call to a translation route, it sends a message to the PG. This message contains the ultimate target and further instructions for the PG. For example, the PG might be instructed to coordinate with a host computer so that the caller's account number is displayed on the teleset of the agent who picks up the call.

U

Unstable Call A call whose state is transitioning. For instance, during a transfer operation a call is termed unstable.

Unswitched Mode Referring to the ISN, the unswitched mode of operation is when the PSTN transfers a call. No switching function takes place within the ISN.

URI Uniform Resource Indicator

URL Uniform Resource Locator

V

VB Admin Voice Browser Administration, an ISN configuration and administration tool with a command line interface (CLI) you use to perform tasks such as controlling the Voice Browser, gathering statistics, and viewing system metrics and status.

Voice Browser (VB) The ISN Voice Browser is one component of ISN. It is the VXML client that queries the Application Server.

Voice Gateway Gateways that convert PSTN calls to VoIP.

VRU Voice Response Unit. An automated voice system designed for call center applications.

VRU Blind Transfer The ability for a VRU to support blind transfer (see Blind Transfer definition) using the VRU interface.

VRU Type A classification system for different types of call flows within the ICM system, used for determining how to manage calls at VRUs or to be transferred to VRUs.

VXML or VoiceXML **V**oice e**X**tensible **M**arkup **L**anguage. A DTD specifying a language for defining forms and menus which are used to conduct interactive dialogues with a user. The dialogue may involve the playing of recorded audio prompts or TTS audio generated from the text in the document. Input from the user is collected through ASR or DTMF. A VXML script may result in the playing of information retrieved from a web application, posting of collected inputs to a web application, or transfer of the call to a third party. VoiceXML is specified by the VoiceXML Forum (http://www.voicexml.org).

VoIP Voice over IP, the concepts of transmitting voice through a data network.

A

C

D

E

G

H

I

L

M

N

O

P

Q

R

S

T

V

Z