

# VOCAL

Vovida Open Communication Application Library

Technology Overview

Software Version 1.4.0

---

**Copyright** Copyright © 2002, Cisco Systems, Inc.

---

**Guide Versions** The following table matches the software versions with the guide versions:

<b>Software Version</b>	<b>Guide Version</b>	<b>Date</b>	<b>Comments</b>
1.0.0			Internal Trials Only
1.1.0			Internal Trials Only
1.2.0	1.2	March 26, 2001	Open Release to Public
1.2.0	1.2 A	April 11, 2001	Copy edit errors corrected.
1.3.0	1.3	December 21, 2001	Support new open release to public
1.4.0	1.4	June 23, 2002	Update for release of version 1.4.0.

---

**Version** This manual is written to support VOCAL Version 1.4.0.

---

**Support** The primary location for support, information and assistance for the VOCAL system is <http://www.vovida.org/>. This site contains other documentation, training materials, development tools, development resources and informational mailing lists.

---

# Preface

---

**Introduction** This chapter is a general introduction to the System Technology Overview manual, and provides information about the intentions and organization of the manual. It also provides information about additional resources available from <http://www.vovida.org>.

---

**Objectives of this manual** This manual provides information about the technical architecture of VOCAL. Information about installing the software and provisioning servers is provided in the [VOCAL Installation Guide](#). Information about adding users and assigning features is provided in the [System Administration Guide](#).

---

**Intended audience** This manual is intended for technicians who will be installing and provisioning the VOCAL system. These technicians should be familiar with either the Linux operating system or with the operating system on which VOCAL is being installed; and should also be familiar with Session Initiation Protocol (SIP) and the general concepts and principles of Voice over IP (VoIP) telephony networks.


---

**Organization** This guide is organized as follows:

<i>Chapter</i>	<i>Title</i>	<i>Description</i>
<b>Chapter 1</b>	System Overview	A high level overview of the system architecture.

---

**Documentation Conventions** The following is a list of conventions used in this guide:

<b>Convention</b>	<b>Description</b>
<b>bold text</b>	Names of elements found on the GUI screen, including buttons, and selectable entities such as, servers and server groups.
< >	Text that appears between angle brackets describes variables such as, <group name>.
<code>courier font</code>	System responses and prompts either from the CLI or GUI.
<b>bold courier font</b>	Indicates information that you must enter.
■ <b>Note</b>	Highlights points of additional interest for the user.
 <b>Caution</b>	Be careful, this symbol highlights a potential for equipment damage or loss of data.

## Additional resources

### Publications

A [VOCAL Installation Guide](#), which covers the material found in this manual plus instructions about installing the software and provisioning servers.

A [System Administration Guide](#), which covers adding users, SNMP message flows, call flows and working with features is also available from Vovida.org (<http://www.vovida.org>)

### On-Line Resources

Vovida.org is a community web site dedicated to providing a forum for open source software used in datacom and telecom environment. This site was created to provide an environment where open source communications information and software can be easily located, accessed, retrieved and shared.

# Table of Contents

---

## Preface

### Chapter 1.

#### VOCAL System Overview

Overview . . . . .	1-3
SIP Overview . . . . .	1-8
Vocal System Functionality . . . . .	1-14

## Table of Contents *(continued)*

---

# VOCAL System Overview

## Chapter Contents

This chapter describes the Vovida Open Communication Application Library (VOCAL) system from a high-level point of view, highlighting the Session Initiation Protocol (SIP) and the functionality of the VOCAL system.

Topic	See Page
<b>Overview</b> .....	<b>1-3</b>
Servers .....	1-6
<b>SIP Overview</b> .....	<b>1-8</b>
Compatible Protocols .....	1-9
SIP User Agents and Servers .....	1-10
Basic SIP Call Flow .....	1-11
SIP Messages .....	1-12
<b>Vocal System Functionality</b> .....	<b>1-14</b>
SIP-Based Call Control .....	1-16
Signaling .....	1-16
Call Control .....	1-16
Calling to Parties on the Public Switched Telephone Network ..	1-20
Call Routing Through a Feature Server .....	1-22
Quality of Service .....	1-25
Quality of Service Enabled .....	1-26
Open Settlement Protocol .....	1-28
Operation System Support .....	1-33
Provisioning .....	1-33

<b>Topic</b> <i>(continued)</i>	<b>See Page</b>
Authentication .....	1-33
Access List .....	1-33
Digest .....	1-35
Call Detail Records and Billing .....	1-36
Call Detail Records .....	1-36
Billing .....	1-40
Network Management .....	1-41
Features .....	1-42
SIP Messages and Feature Servers .....	1-42
Core Features .....	1-46
Set Features .....	1-48
Scriptable Feature Development .....	1-48

---



# Overview

## Introduction

This section describes the VOCAL system from a high-level point-of-view.

## What is VOCAL?

The VOCAL system is a distributed network of servers that provides Voice Over Internet Protocol (VoIP) telephony services. VOCAL supports devices that communicate Session Initiation Protocol (SIP, RFC 2543), Media Gateway Control Protocol (MGCP) or H.323 messages. VOCAL also supports analog telephones via residential gateways.

VOCAL supports on-network and off-network calling. Off-network calling enables subscribers to connect to parties through either the Internet or the Public Switched Telephone Network (PSTN).

## High-Level System View

Figure 1-1 shows a high-level, simplified view of the system.

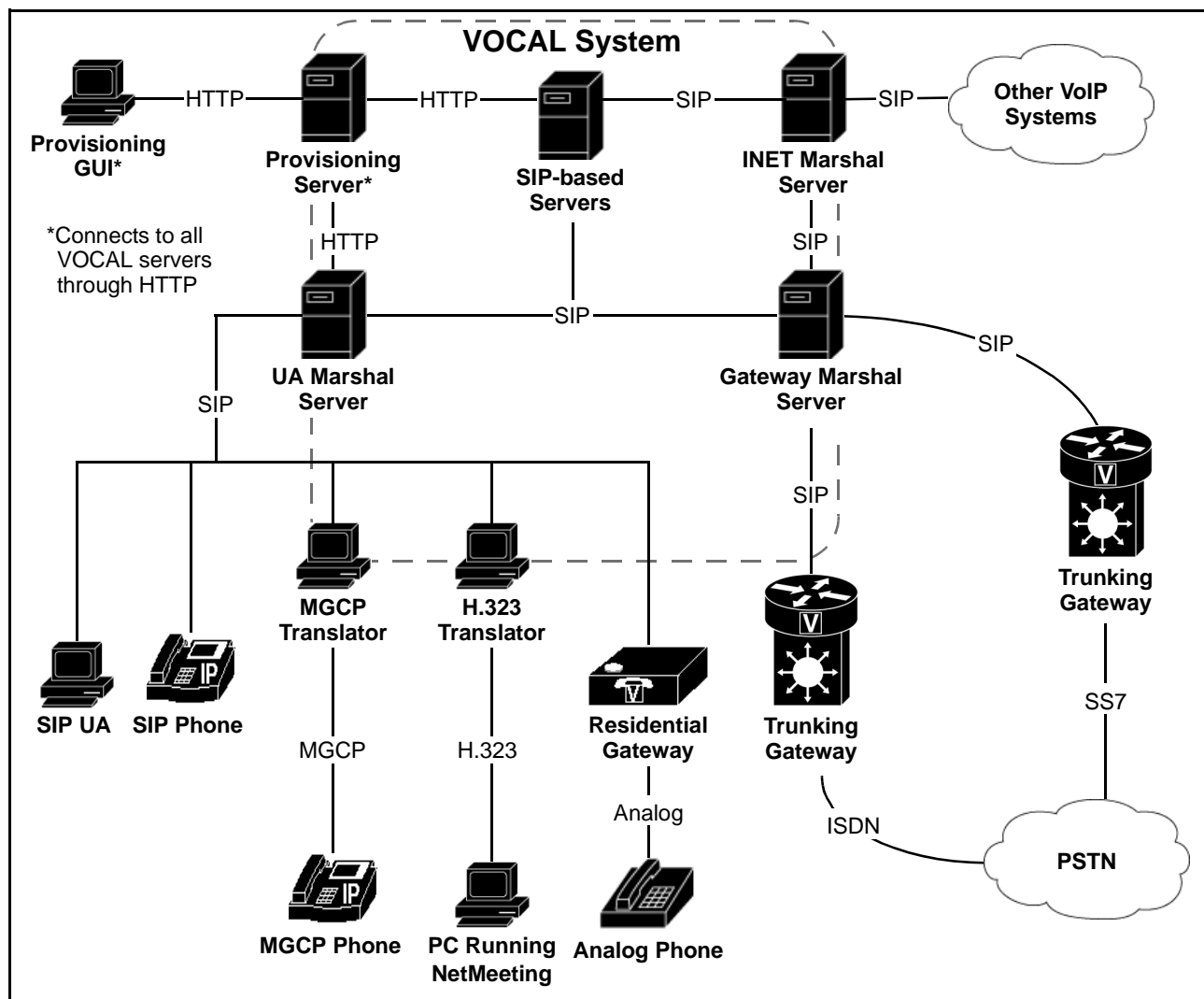


Figure 1-1. Simplified View of the VOCAL System

**System  
Components**

From a high-level point-of-view, the VOCAL system appears as an assembly of basic components. These components are described below in Table 1-1.

**Table 1-1. VOCAL System Components**

<b>Component</b>	<b>Description</b>
VOCAL System	<p>This is the telephony application. <a href="#">Figure 1-1</a> shows an abstract representation of the VOCAL system server modules. A description of each server appears in the next section, see <a href="#">“Servers” on page 1-6</a>.</p> <p><b>Protocols</b></p> <p>The VOCAL system uses several protocols to communicate between its components. The call signaling processes use SIP messaging to communicate internally within the VOCAL system and externally with gateways and IP phones. For more information about SIP, see <a href="#">“SIP Overview” on page 1-8</a>. For more information about the other protocols used in the system, see <a href="#">“Compatible Protocols” on page 1-9</a>.</p>
GUI	<p>The graphical user interface (GUI) enables technicians to provision the system, and administrators to set up users and monitor the system’s performance. The GUI is web-enabled and requires a Java plug-in to run in a web browser. For more information, see <a href="#">“Accessing the Java Provisioning” on page 2-26</a>. In Version 1.4.0, you can bypass the requirement for the Java plug-in by using a simplified HTTP-based provisioning GUI.</p>
IP Phone	<p>VOCAL supports a variety of phone appliances including SIP phones and SIP User Agent (UA) software applications. SIP phones may be connected to the VOCAL system over any IP network.</p>
Translators	<p>MGCP- and H.323-based appliances require translators to convert their messages into SIP before they can communicate with the VOCAL system. The translators are included in VOCAL.</p>

**Table 1-1. VOCAL System Components (Continued)**

<b>Component</b>	<b>Description</b>
Gateways	<p>Gateways not only provide entry points between networks, they also provide translation between SIP-based networks and other network types. The VOCAL system works with two types of gateways, the Residential Gateway and the Trunking Gateway.</p> <p><b>Residential Gateway</b></p> <p>Residential gateways translate analog signals into IP packets, to permit subscribers with analog phone sets/devices to make and receive SIP-based calls.</p> <p><b>Trunking Gateway</b></p> <p>Trunking gateways permit SIP-based networks to exchange calls with end-points on the PSTN, by providing translation between SIP messages and one of these signal types:</p> <ul style="list-style-type: none"><li>• Analog</li><li>• Channel Associated Signaling (CAS)</li><li>• Primary Rate Interface (PRI)</li></ul>

---

## Servers

**Description** Table 1-2 describes the server modules included in the VOCAL system.

**Table 1-2. VOCAL Server Modules**

<b>Server Modules</b>	<b>Description</b>
Marshal Server	The Marshal Server (MS) is an implementation of the SIP proxy server and acts as the initial point of contact for all SIP signals that enter the VOCAL system. The MS provides authentication, forwarding and billing functions. For more information about SIP proxy servers, see <a href="#">"SIP User Agents and Servers" on page 1-10</a> . For more information about authentication, see <a href="#">"Authentication" on page 1-33</a> . For more information about forwarding, see <a href="#">"Call Control" on page 1-16</a> . For more information about billing, see <a href="#">"Call Detail Records and Billing" on page 1-36</a> .
Redirect Server	The Redirect Server (RS) is a combined implementation of the SIP redirect, registration and location servers. The RS stores contact and feature data for all registered subscribers and a dialing plan to enable routing for off-network calls. For more information about SIP servers, see <a href="#">"SIP User Agents and Servers" on page 1-10</a> . For more information about registration, see <a href="#">"Authentication" on page 1-33</a> .
Call Detail Record Server	The Call Detail Record (CDR) server receives call data from the Marshal Servers and formats it into data that can be transmitted to third party billing systems for invoicing. For more information about billing, see <a href="#">"Call Detail Records and Billing" on page 1-36</a> .
Network Manager	The Network Manager provides the administrator with the ability to monitor the system through Simple Network Management Protocol (SNMP) messages. For more information about the Network Manager, see the <a href="#">System Administration Guide</a> .
Voice Mail Server	The Voice Mail server provides unified messaging whereby voice mail messages can be distributed as .wav files attached to e-mail messages.
Feature Server	The Feature Servers are another implementation of the SIP proxy server. These servers are scripted in Call Processing Language (CPL) and provide basic system features such as Call Forward and Call Blocking. For more information about features, see <a href="#">"Features" on page 1-42</a> .
JTAPI Server	The VOCAL system includes an implementation of the Core JTAPI package that supports basic third-party call control capability, and a basic User Agent application, the VOCALpad, that utilizes the implementation. For more information, see <a href="#">"JTAPI Servers" on page 3-60</a> .
Provisioning Server	The Provisioning Server (PS) stores data records about each system user and server module, and distributes this information throughout the system via a subscribe-notify model. The PS provides a web-enabled graphical user interface (GUI) to permit technicians and system administrators to manage the system. The For more information about provisioning servers, see <a href="#">Chapter 3, Provisioning</a> in this guide. For more information about provisioning users, see the <a href="#">System Administration Guide</a> .

**Table 1-2. VOCAL Server Modules (Continued)**

<b>Server Modules</b>	<b>Description</b>
Policy Server	The Policy Server has been designed to use Common Open Policy Service (COPS, RFC 2748) to provide Quality of Service (QoS) bandwidth reservation for calls or call segments that are transmitted over the Internet. The Policy Server is also capable of using Open Settlement Protocol (OSP, a product of the Telecommunication and Internet Protocol Harmonization over Networks (TIPHON) project at the European Telecommunications Standards Institute (ETSI)) to interact with clearinghouses for authorization, authentication and accounting (AAA). For more information about QoS and OSP, see <a href="#">“Quality of Service” on page 1-25</a> .
Heartbeat Server	The Heartbeat Server monitors the flow of pulsing signals emitted by the other servers, and provides information about to the flow of heartbeats to the Simple Network Management Protocol (SNMP, RFC 1157) GUI. This information helps the System Administrator know if the server modules are up or down. For more information about heartbeats, see <a href="#">“Heartbeat Servers” on page 3-62</a> . For more information about the SNMP GUI, see the System Administration Guide.

---

**Scaling the System** The VOCAL system can be provisioned onto a single hardware unit or onto multiple hosts. While a single hardware unit may be useful for laboratory testing, systems that are intended to support customers are normally scaled up to larger systems that may include any number of hosts. See [Appendix A, Engineering Guidelines](#) for more information about scaling the system.

---

## SIP Overview

### Introduction

This section describes SIP with respect to its features and benefits, compatible protocols, user agents and servers along with basic call flows.

### What is SIP?

The Session Initiation Protocol (SIP: RFC 2543) is an ASCII-based, peer-to-peer protocol designed to provide rendezvous services over the Internet. SIP is an Internet Engineering Task Force (IETF) specification that was derived from Hyper-text Transfer Protocol (HTTP: RFC 2616) and Simple Mail Transfer Protocol (SMTP: RFC 821).

SIP, along with Media Gateway Control Protocol (MGCP: RFC 2705), and H.323 (an International Telecommunications Union (ITU) specification), is one of three commonly used open protocols for VoIP implementations. A slide presentation that compares these three protocols, called VoIP Protocol Overview, is available on <http://www.vovida.org>.

### Features and Benefits

Table 1-3 describes some of the features and benefits of SIP-based systems:

**Table 1-3. SIP Features and Benefits**

<b>Feature</b>	<b>Benefit</b>
Simplicity	The SIP stack is smaller than other VoIP protocols. SIP can be considered as a simple toolkit that enables smart endpoints, gateways, processes and clients to be built and implemented.
Scalability	The peer-to-peer architecture permits inexpensive scaling. When compared to other Voice over IP (VoIP) protocols, the hardware and software requirements for adding new users to SIP-based systems is greatly reduced.
Distributed Functionality	A decentralized intelligence permits more functionality within each component. Changes made to specific components have a minor impact on the rest of the system.  It is possible to connect one SIP phone to another with an ethernet cable and make calls between the sets without the aid of any other server modules. The other system components become useful when the network requires more than two phones.
Internet-enabled	SIP-based systems can take advantage of the growth of the Internet. Translating gateways permit SIP-based systems to contact parties on the Public Switched Telephone Network (PSTN) without being encumbered by its legacy standards.

## Compatible Protocols

**Introduction** This section describes protocols that are compatible with SIP.

**Protocols and Descriptions** SIP can work alone or together with the following protocols:

**Table 1-4. Compatible Protocols**

<b>Protocol Acronym</b>	<b>Protocol Name</b>	<b>Description</b>
COPS	Common Open Policy Service	Used to signal network, routers and switches with requests for Quality of Service. COPS is a companion protocol to RSVP.
DHCP	Dynamic Host Configuration Protocol	Helps systems automatically configure network settings.
DNS	Domain Name System	Resolves host names to IP addresses.
HTTP	Hypertext Transfer Protocol	HTTP is the standard protocol used for serving web pages over the Internet.
MGCP	Media Gateway Control Protocol	MGCP is a master/slave protocol whereby the gateways are under the direct control of the user agents. SIP-based systems can communicate to MGCP endpoints through translators.
OSP	Open Settlement Protocol	OSP is used to exchange authorization, authentication and accounting (AAA) information with clearinghouse servers.
RADIUS	Remote Authentication Dial-In User Service	A freely available distributed security system that can be used to transmit call detail records to a billing system.
RSVP	Resource Reservation Protocol	Enables SIP-based systems to reserve bandwidth for call sessions. RSVP is a companion protocol to COPS.
RTP	Real-time Transport Protocol	Provides voice channels between end points.
SDP	Session Description Protocol	Describes the content of multi-media sessions. SDP messages are attached to SIP messages as Multi-Purpose Internet Mail Extensions (MIME).
TCP	Transmission Control Protocol	Can be used as the underlying transport protocol in SIP-based systems.
UDP	User Datagram Protocol	Provides best effort service to deliver packets with minimal overhead and minimal delay.

## SIP User Agents and Servers

**Introduction** This section describes SIP User Agents and Servers, and how they function within the VOCAL system.

**User Agents** User Agents (UA's) are specified in RFC 2543 as applications such as, SIP phones and software that initiate and receive calls over a SIP network.

**Servers** Servers are specified in RFC 2543 as application programs that accept requests, service requests and send back responses to those requests. Table 1-5 describes the servers included in RFC 2543 and how they function within the VOCAL system.

**Table 1-5. SIP Servers**

<b>Server Type</b>	<b>RFC 2543 Definition</b>	<b>VOCAL Functionality</b>
Location Server	A Location Server can be used by a SIP redirect or proxy server to obtain information about a called party's possible location. The location server can also be an entity outside of the SIP network that uses an alternative protocol, such as Telephony Routing over IP (TRIP, RFC 3219) to communicate with the Redirect Server.	The Location server is a logical function within the VOCAL Redirect server.
Proxy Server	An intermediary program that acts as both a server and a client for the purpose of making requests on behalf of other clients. Unlike User Agents, Proxy Servers do not initiate new SIP requests. A Proxy Server interprets, and, if necessary, rewrites a request message before forwarding it. Requests are serviced internally or by passing them on, possibly after translation, to other servers.	The VOCAL system includes specialized SIP Proxy servers called Marshal and Feature servers.
Redirect Server	A redirect server is a server that accepts a SIP request, maps the address into zero or more new addresses and returns these addresses to the client. Unlike a proxy server, it does generate SIP requests on behalf of UA's and it does not accept calls.	The SIP Redirect server is a logical function within the VOCAL Redirect server.
Registrar Server	A registrar is a server that accepts REGISTER requests. A registrar is typically co-located with a proxy or redirect server and <i>may</i> offer location services.	The SIP Registrar server is a logical function within the VOCAL Redirect server.



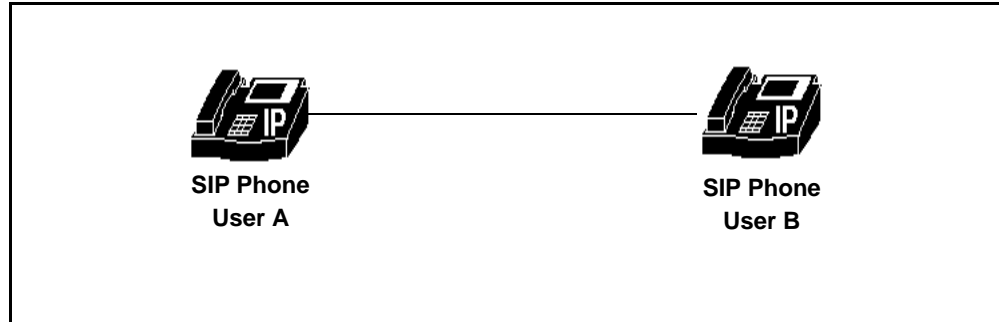
## Basic SIP Call Flow

### Introduction

This section illustrates a simple call flow. More complex examples can be found in the System Administrator's Guide.

### Call Scenario

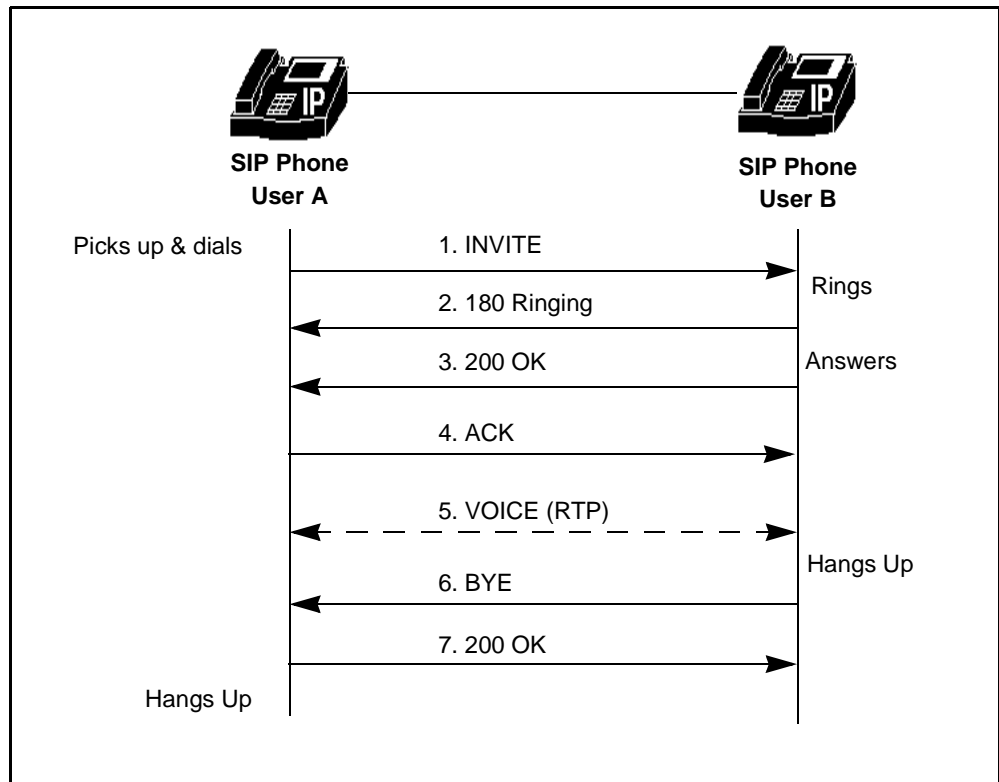
Figure 1-2 shows a simple SIP phone call where user A is calling user B.



**Figure 1-2. Basic Connection Between Two SIP Phones**

### Call Flow

Figure 1-3 and Table 1-6 describe the SIP messages exchanged for call establishment and tear down.



**Figure 1-3. Basic Call Flow Diagram**

### Call Flow Details

The following table explains each of the “hops” shown in [Figure 1-3](#).

**Table 1-6. Call Flow Details**

<b>Step</b>	<b>Description</b>
1	INVITE: User A initiates a call to User B.
2	180 Ringing: User B sends a ringing signal back to User A.
3	200 OK: User B picks up.
4	ACK: User A acknowledges that it received the 200 message.
5	VOICE: A two-way voice channel is established over Real-time Transport Protocol (RTP) and a conversation takes place between User A and B.
6	BYE: User B hangs up.
7	200 OK: The call is torn down and User A hangs up.

## SIP Messages

### Overview

SIP messages can be divided into requests and responses.

### Request messages

Table 1-7 shows a few of the most commonly used SIP request messages.

**Table 1-7. Some SIP Request Messages**

<b>SIP Request Message</b>	<b>Description</b>
INVITE	Indicates that the user or service is being invited to participate in a session.
ACK	Confirms that the client has received a final response to an INVITE request.
BYE	Indicates that the user wishes to terminate the call.
REGISTER	Indicates that a User Agent is attempting to add its address to the Redirect server's user database.
CANCEL	Cancels a pending request but does not affect a completed request.

**Response Messages**


---

The SIP response messages are numbered, and the first digit in each response number indicates the type of response. Table 1-8 explains the different message types.

**Table 1-8. Some SIP Response Messages**

<b><i>SIP Response Message Types</i></b>	<b><i>Description</i></b>
1xx	Information Responses For example: 180 Ringing
2xx	Successful Responses For example: 200 OK
3xx	Redirection Responses For example: 302 Moved Temporarily
4xx	Request Failures Responses For example: 403 Forbidden
5xx	Server Failure Responses For example: 504 Gateway Time-out
6xx	Global Failure Responses For example: 600 Busy Everywhere

Further examples of these messages are shown in the following sections where call flows through distributed networks are discussed.

**For More Information**


---

For more information about SIP messages, see RFC 2543.

---

## Vocal System Functionality

---

### **Introduction**

This section provides a high-level overview of message flows between VOCAL system components for selected functions.

---

### **What is Functionality?**

Functionality refers to how the system components interact with each other to produce desired results. These results include phone calls being established and torn down, new users being added to the system, unauthorized users being kept out, and customers receiving invoices for the service.

In this guide, functionality is organized into discussions about the VOCAL system, the operation support system and the features.

---

### **Illustration**

Figure 1-4 shows a high-level view of some of the VOCAL system elements and how they connect to outside entities such as User Agents, billing servers and others.

The connections between VOCAL and User Agents, gateways, clearing houses, billing servers and other VoIP systems are explained later in this chapter.

The other connections are optional and are to be documented in the user guides.

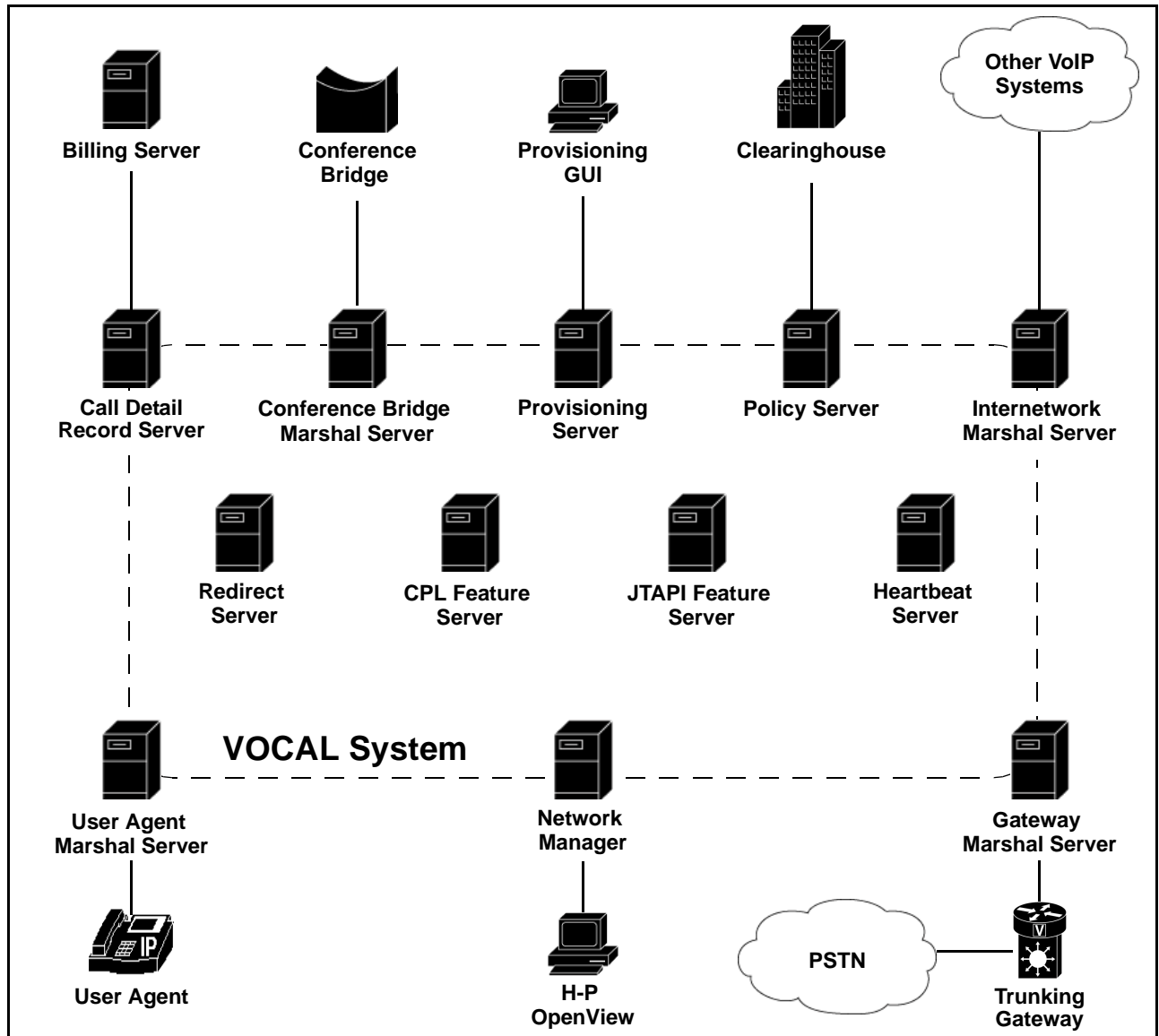


Figure 1-4. High-Level View of the Vocal System

## SIP-Based Call Control

**What is SIP-Based Control?** The SIP-Based Call Control portion of the VOCAL system includes those elements that enable call processing.

### Signaling

**What is Signaling?** The VOCAL system uses SIP messages to signal requests and responses between the core, call processing servers. For examples of SIP messages, see [“SIP Messages” on page 1-12.](#)

### Call Control

**Introduction** This section describes how calls are controlled over the VOCAL system through SIP messages, and how these messages are transmitted when the call is routed to the PSTN or to a feature server.

**What is Call Control?** Call control is the ability to initiate, establish and tear down calls.

**Diagram #1: Call Initiation** Figure 1-5 shows a SIP phone initiating a call by sending an INVITE message through the VOCAL system.

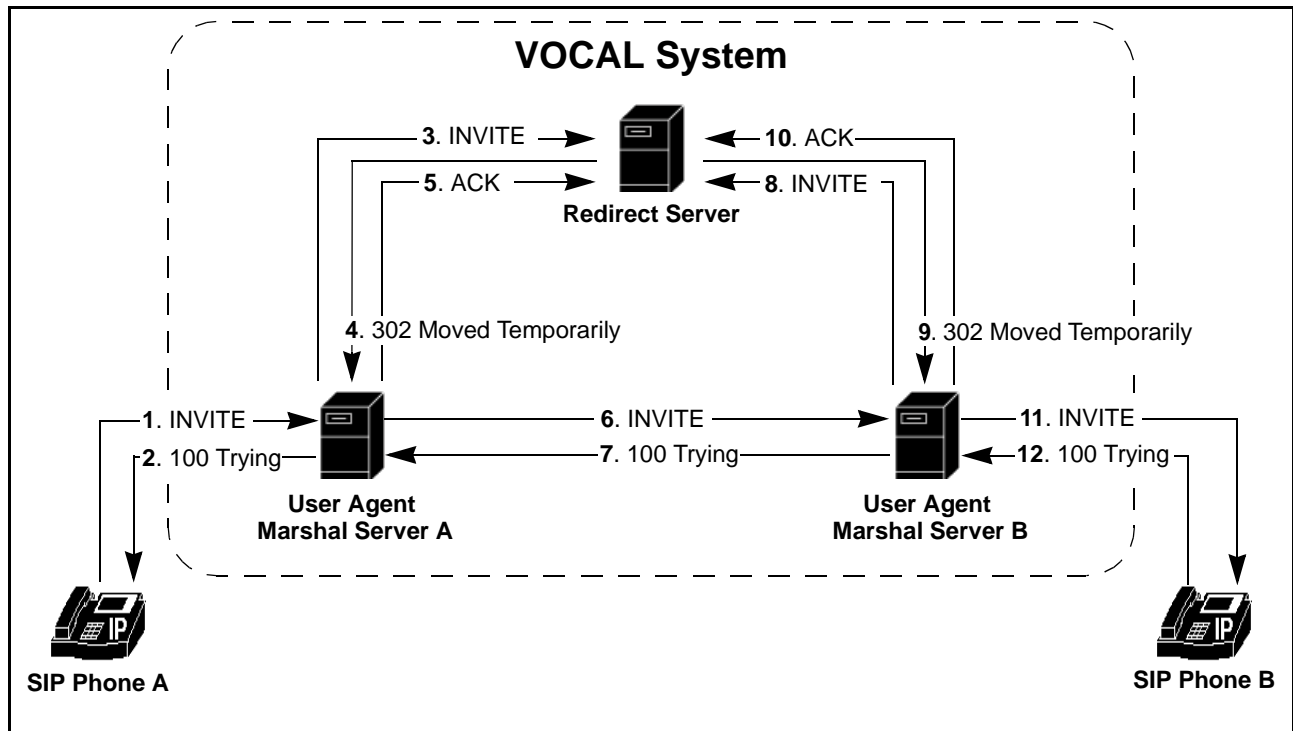


Figure 1-5. Call Initiation

**Messages 1 - 9 Described**

Table 1-9 describes the messages illustrated in Figure 1-5.

**Table 1-9. Interactions Shown in Figure 1-5**

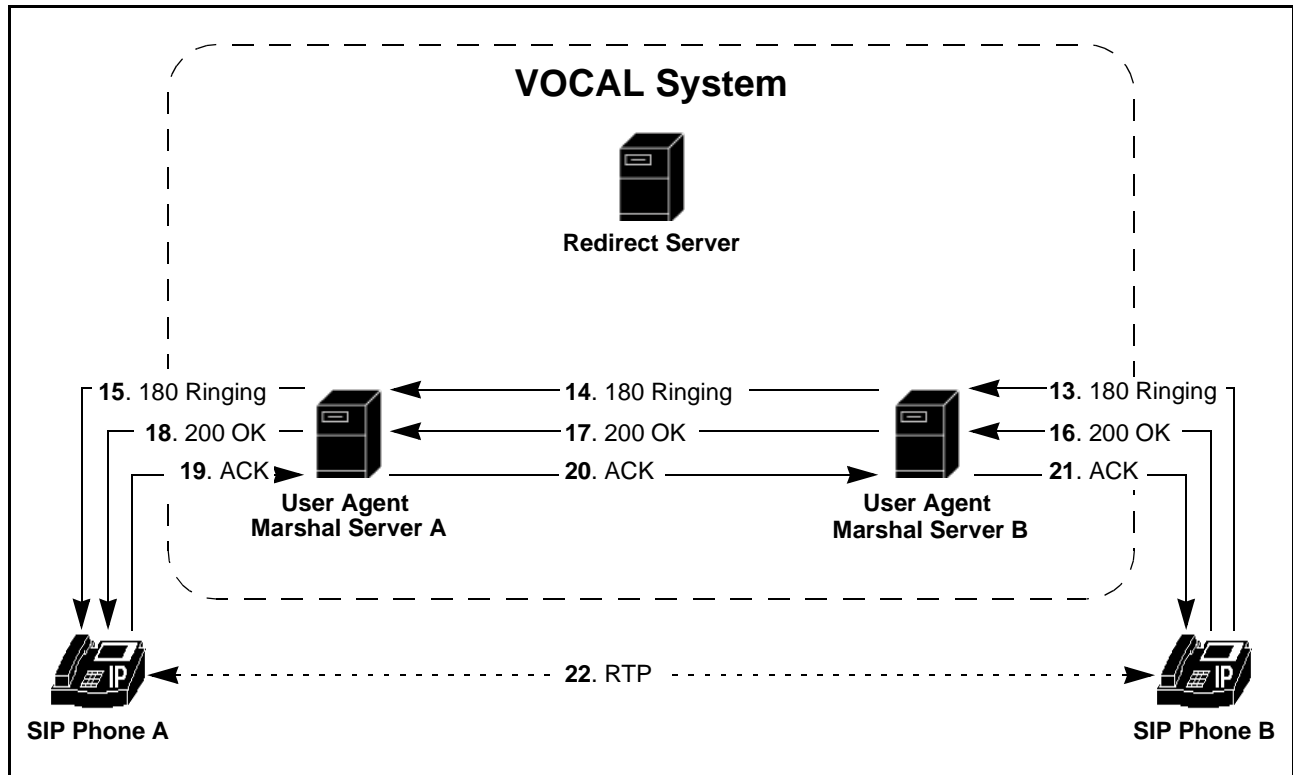
<i>Interaction</i>	<i>Step</i>	<i>Description</i>
SIP Phone A to UAMS A	<b>1-2</b>	SIP Phone A and SIP Phone B are on the local IP network. SIP Phone A sends an INVITE message intended for SIP Phone B. The INVITE is received by User Agent Marshal server (UAMS) A, which responds with a 100 Trying message to stop retransmissions of the INVITE.
UAMS A to the RS	<b>3</b>	UAMS A authenticates the user and forwards the INVITE message to the Redirect server (RS). This is the normal routine: the UAMS forwards all INVITE's from authorized users to the RS.
	<b>4</b>	The RS responds with a 302 Moved Temporarily, message and sends it to UAMS A. The 302 message serves two purposes: <ul style="list-style-type: none"> <li>• It informs the UAMS that the INVITE was not intended for the RS.</li> <li>• It provides routing information that enables the UAMS to forward the INVITE towards its intended destination. This destination could be a Feature or a Marshal server. Feature servers are explained later in this chapter.</li> </ul>
	<b>5</b>	UAMS A sends an ACK message back to the RS acknowledging receipt of the 302 message. This completes the transaction.
Forwarding the INVITE Message to SIP Phone B	<b>6 - 12</b>	UAMS A forwards the INVITE message to UAMS B, the proxy server for the intended destination, which responds with a 100 Trying message. UAMS B forwards the INVITE message to the RS, which responds with a 302 Moved Temporarily message and sends it to UAMS B. UAMS B sends an ACK message back to the RS acknowledging receipt of the 302 message, and forwards the INVITE message to SIP Phone B, which responds with a 100 Trying message. The INVITE, having arrived at its final destination, makes the phone ring. The ringing can be a sound, a visual indicator, a vibration, a combination of these indicators or any indicator that has been implemented in the phone.

**Diagram #2: Call Establishment**

Figure 1-6 shows SIP phone B responding and setting up an RTP path with SIP Phone A.

**Note**

In a distributed network, the RTP path may travel over the VOCAL system's backbone without being processed by any of the servers. The RTP path may also bypass the VOCAL system altogether.



**Figure 1-6. Call Establishment**

**Messages 10 - 19 Described**

Table 1-10 describes the messages illustrated in Figure 1-6.

**Table 1-10. Interactions Shown in Figure 1-6**

<i>Interaction</i>	<i>Step</i>	<i>Description</i>
Ringing	<b>13 - 15</b>	SIP Phone B rings and sends a 180 Ringing response to UAMS B, which is forwarded through the network back to SIP Phone A.  <b>Note</b> The 180 does not pass through the RS because the RS does not request to be included in further messages from this call.



**Table 1-10. (Continued) Interactions Shown in Figure 1-6**

<b>Interaction</b>	<b>Step</b>	<b>Description</b>
Pick-up	<b>16 - 18</b>	SIP Phone B sends a 200 OK response to the UAMS. This means that the phone has been activated and is ready to establish voice channel contact with SIP Phone A.
Pick-up acknowledged	<b>19 - 21</b>	SIP Phone A sends an ACK message confirming that it is ready to connect to a voice channel.
A conversation takes place	<b>22</b>	<p>A voice channel is established using Real-time Transfer Protocol (RTP), and the users can talk to each other.</p> <p><b>■ Note</b>                      It is also likely for the 180 Ringing message to contain session description information that permits a one-way audio path to be established from the called party to the calling party. This is known as early RTP.                      If early RTP is established, the return media path is setup after the called party has sent an ACK in response to the 200.</p>

**How is the Call Torn Down?**

When the conversation is over, both phones hang up. The first phone to hang up sends a BYE message to the other. This BYE message tears down the RTP path for that phone. The other phone responds with 200, OK, and tears down its side of the RTP path.

**Diagram #3: Call Tear Down**

Figure 1-7 shows the call being torn down. In this example, SIP Phone B hangs up first.

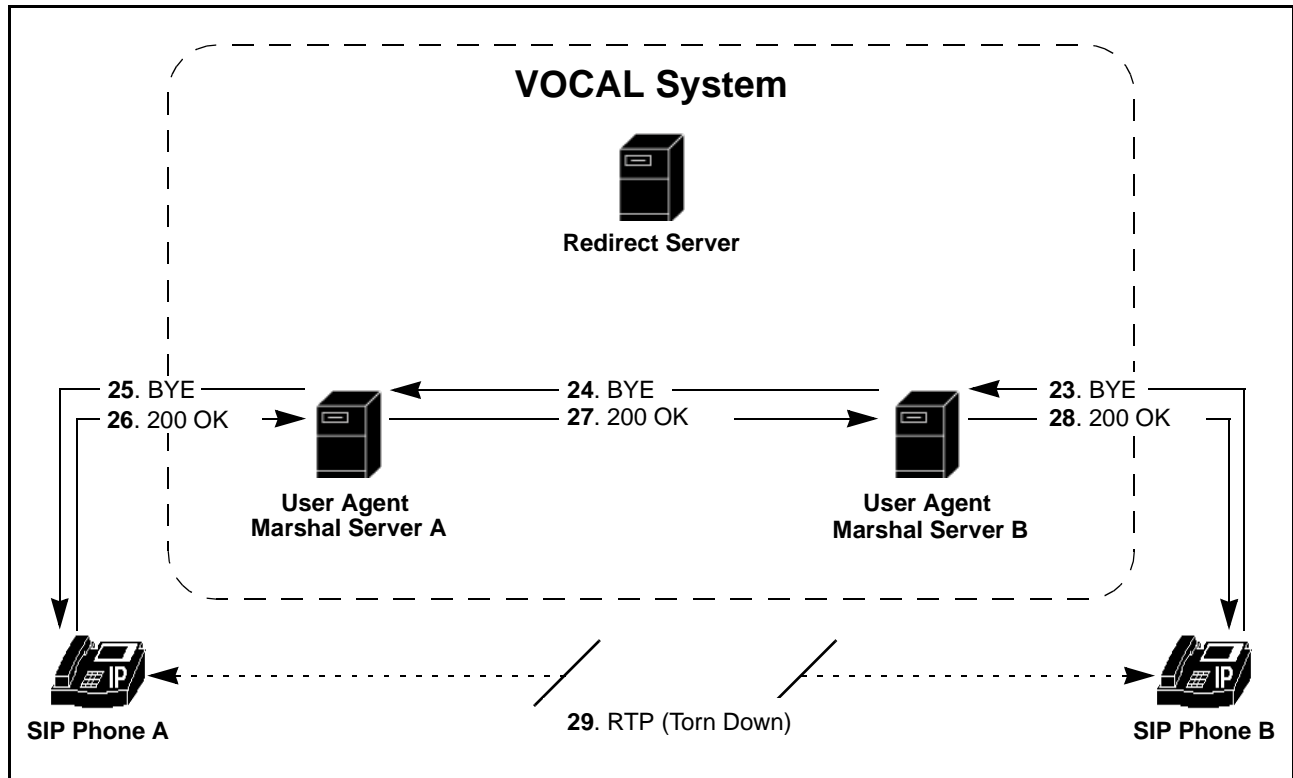


Figure 1-7. Call Tear Down

**Messages 20 - 26 Described**

Table 1-11 describes the messages illustrated in Figure 1-7.

**Table 1-11. Interaction Shown in Figure 1-7**

Interaction	Step	Description
SIP Phone B Hangs Up	23 - 25	SIP Phone B sends a BYE request through the system to SIP Phone A.
	26 - 28	SIP Phone A responds with a 200 OK.
The Voice Channel is torn down	29	The BYE and 200 messages trigger the voice channel to shut down.

**Calling to Parties on the Public Switched Telephone Network**

**Introduction**

This section describes how calls are routed to the public switched telephone network (PSTN).

**Translating SIP into PSTN Signals**

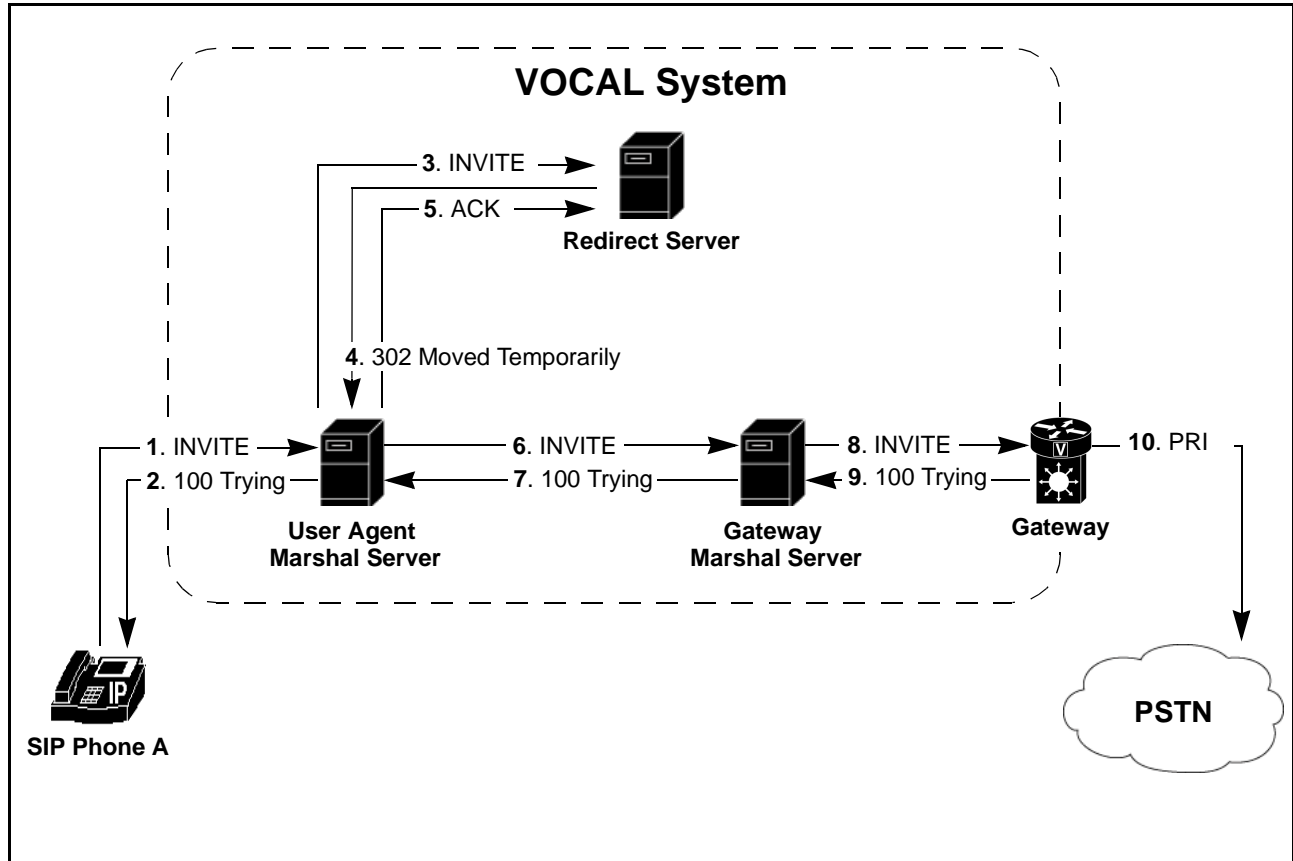
Connections to the PSTN are made through SIP-based PSTN gateways, which are attached to a Gateway Marshal Server, one Marshal server per gateway.

**Diagram #1: SIP Phone to the PSTN**

Figure 1-8 shows a message path from a SIP phone to the VOCAL system.

**Note**

In version 1.4.0 of VOCAL this is the only example where a Marshal server forwards an INVITE directly to another device without going through the Redirect Server for further routing information.



**Figure 1-8. INVITE Message Sent to the VOCAL System**

**Messages 1 - 7 Described**

Table 1-12 describes the messages illustrated in Figure 1-8.

**Table 1-12. Interaction Shown in Figure 1-8**

<i>Interaction</i>	<i>Step</i>	<i>Description</i>
SIP Phone A to the RS via the UAMS	<b>1 - 4</b>	SIP Phone A sends an INVITE message intended for a destination on the PSTN. The User Agent Marshal Server (UAMS) authenticates the message and forwards it to the Redirect Server (RS). The RS returns a 302 Moved Temporarily, message that provides routing information.
UAMS to the GWMS	<b>5 - 7</b>	The UAMS acknowledges receipt of the 302 message and forwards the INVITE to the Gateway Marshal Server (GWMS).

**Table 1-12. Interaction Shown in Figure 1-8**

<b>Interaction</b>	<b>Step</b>	<b>Description</b>
GWMS to the gateway and the PSTN	<b>8 - 10</b>	The GWMS forwards the INVITE to the SIP-based PSTN gateway, where it is translated into a format that is understood on the PSTN.

## Call Routing Through a Feature Server

### Introduction

This section describes how calls are routed through feature servers.

### Features

The VOCAL system supports a variety of system and set features. For more information, see [“Features” on page 1-42](#).

### Call Routing to Feature Servers

As it has been shown above, the marshal servers forward INVITE messages to the Redirect Server for routing information. The INVITE message contains data describing its origin and intended destination. The Redirect Server looks up the origin and destination on a table that includes the dialing plan and system features, and then generates a Redirect message that includes routing information.

#### Example - Call Blocking

If the calling user agent has call blocking enabled, the Redirect server instructs the User Agent Marshal Server to forward the INVITE message to the Call Blocking Feature Server. The Call Blocking Feature Server looks up the call destination on its table of forbidden destinations. If the call matches a forbidden destination, the Call Blocking Feature Server disallows the call by sending a 403 Forbidden, message back to the User Agent Marshal Server, which forwards this message back to the calling user agent.

If the call destination does not match a forbidden destination, then the Call Blocking Feature Server forwards the call to the Redirect Server for further routing.

### Diagram #1: Sending the INVITE

Figure 1-9 shows an INVITE message being sent to the VOCAL system.

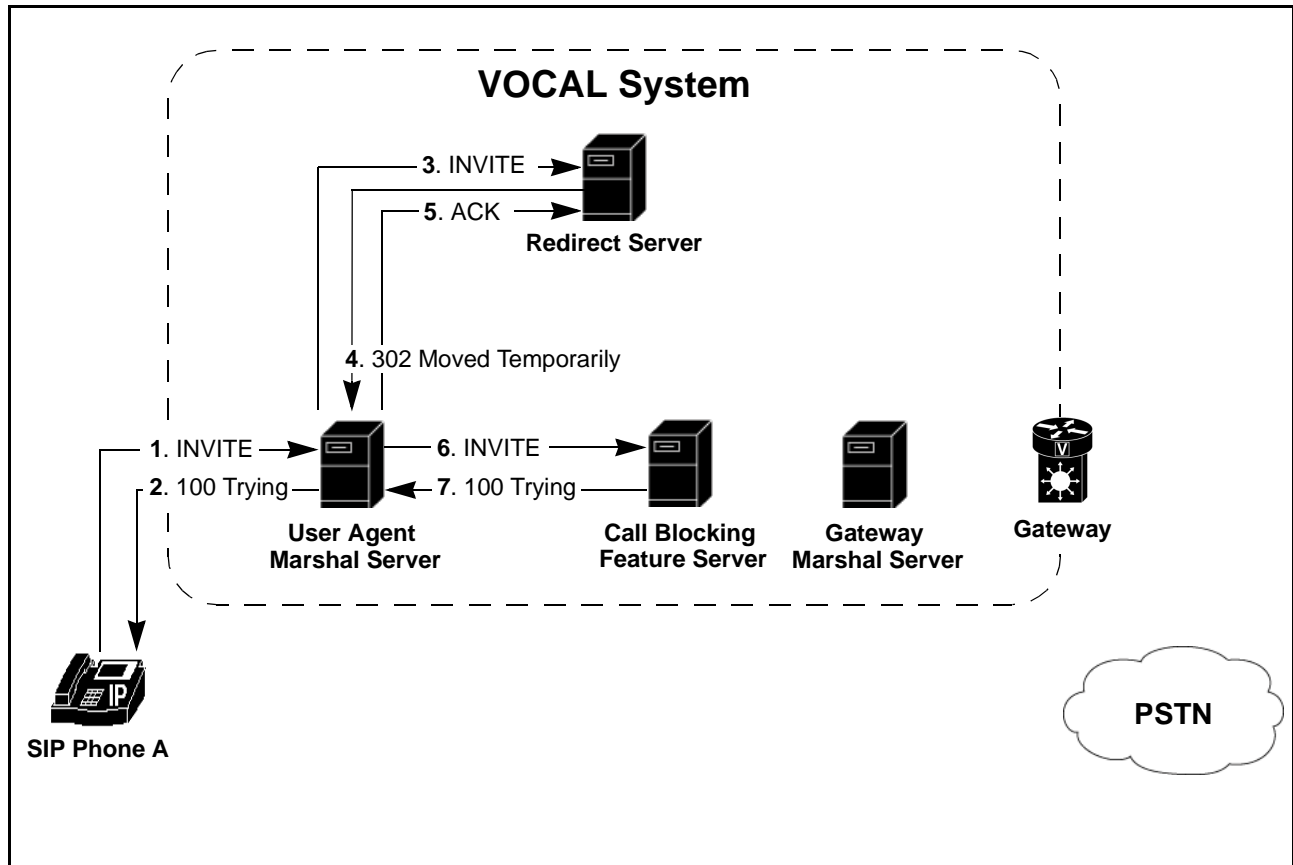


Figure 1-9. SIP Phone Sending an INVITE to the VOCAL System

**Messages 1 - 5 Described**

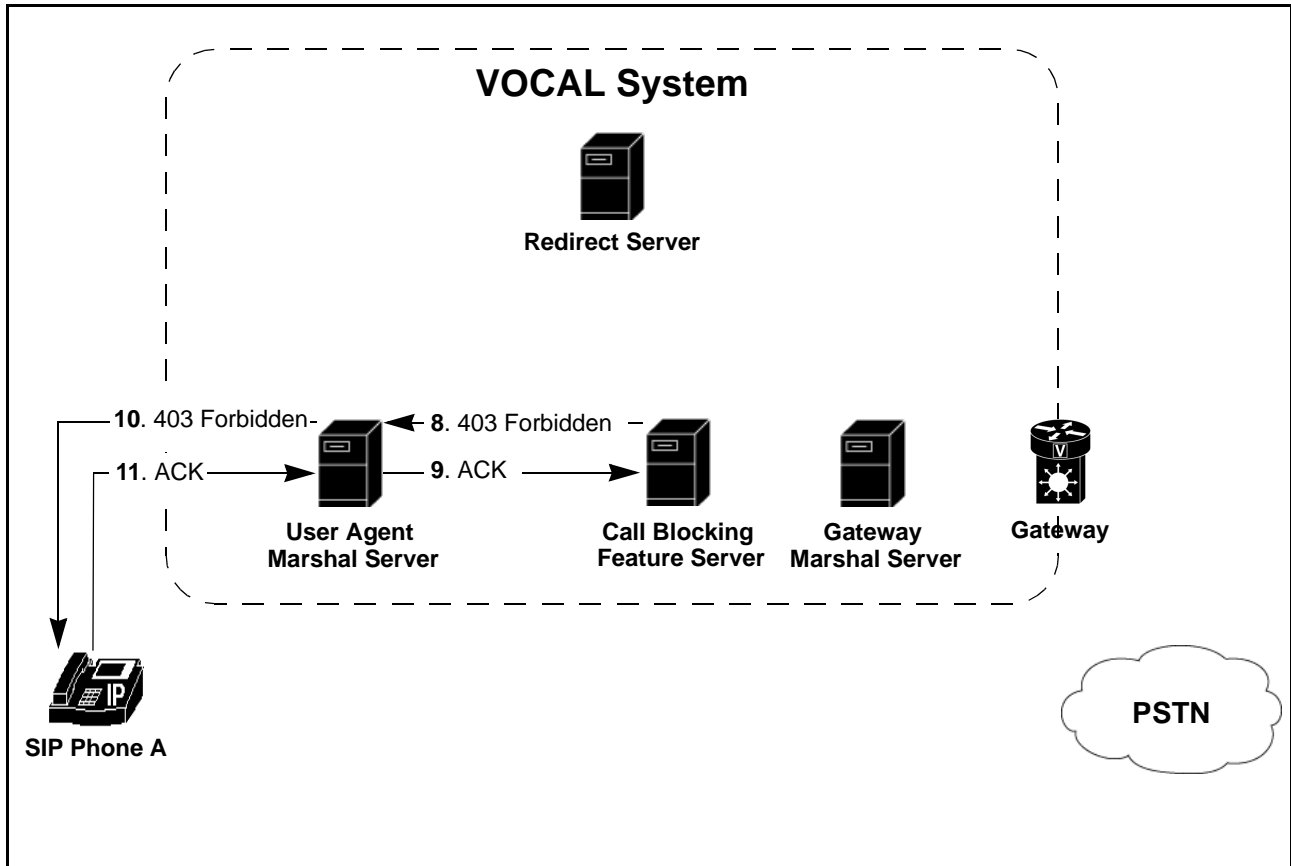
Table 1-13 describes the messages illustrated in Figure 1-9.

**Table 1-13. Interaction shown in Figure 1-9**

<i>Interaction</i>	<i>Step</i>	<i>Description</i>
SIP Phone A to the Redirect Server via the UAMS	<b>1 - 4</b>	SIP Phone A sends an INVITE message intended for a destination on the PSTN. The User Agent Marshal Server (UAMS) authenticates the message and forwards it to the Redirect Server (RS). The RS returns a 302 Moved Temporarily, message that provides routing information.
UAMS to the Call Blocking FS	<b>5 - 7</b>	The UAMS acknowledges receipt of the 302 message and forwards the INVITE to the Call Blocking Feature Server.

**Diagram #2:  
Blocking the Call**

Figure 1-10 shows the Call Blocking Feature Server preventing the call from going through to the PSTN.



**Figure 1-10. The Call Blocking Feature Server Blocks the Call**

**Messages 6- 8  
Described**

Table 1-14 describes the messages illustrated in Figure 1-10.

**Table 1-14. Interaction shown in Figure 1-10**

<i>Interaction</i>	<i>Step</i>	<i>Description</i>
The call is blocked	<b>8</b>	The Call Blocking Feature Server checks the calling destination against its list of forbidden destinations. The destination is forbidden, therefore, it sends a 403 Forbidden message back to the User Agent Marshal Server (UAMS).
	<b>9 - 11</b>	The UAMS acknowledges receipt of the 403 Forbidden message and forwards it to the SIP Phone, which acknowledges. The call has been blocked.

## Quality of Service

<b>Introduction</b>	This section describes how VOCAL has implemented Quality of Service (QoS) for calls transmitted over the Internet.
<b>What is QoS?</b>	Quality of Service (QoS) is, in theory, an effort to manage transmission and error rates, and to minimize latency, packet loss and jitter during internetwork calls. The purpose of this effort is improve the quality of internetwork calls. VOCAL does admission control based on resource availability. If resources cannot be allocated, VOCAL resorts to a “best effort only” delivery. Calls are still processed, but they may not be of the best quality.
<b>What is Policy?</b>	<p>“Policy” is a broadly used, and widely interpreted term, that describes the business rules of the organization applied to the operation of its telecommunications systems. The term stems from the same source as “corporate policy” meaning the rules that guide the behavior of those who work for or with a corporation.</p> <p>With respect to the practical application of QoS, policy is a combination of enforcement and decision making that permits calls to be initiated, established and torn down between networks over the Internet, or between managed IP networks. Enforcement and decision making are explained in detail in this section.</p>
<b>Function of the Policy Server</b>	<p>The Policy server is the key component used to achieve QoS. Service providers typically will only ensure QoS if authorizations and payments are guaranteed by a third party. The Policy server administers admission control for QoS requests and provides the Internetwork Marshal (policy client) with the information necessary to enforce the admitted QoS requests. The Policy server outsources the Authorization, Authentication and Accounting (AAA) requests to a third-party clearing house, which then acts as a trusted broker among a large number of network providers.</p> <p>The Policy server supports two protocols, Common Open Policy Service (COPS) and Open Settlement Protocol (OSP). It acts as a COPS server when it communicates with the network routers, and acts as an OSP client when it exchanges authorization requests and usage reports with the clearinghouse server.</p>
<b>QoS Protocols</b>	The QoS process works with the following protocols.

**Table 1-15. Protocols Used with QoS**

<b>Protocol</b>	<b>Description</b>
COPS	Common Open Policy Service Protocol (COPS) is a proposed Internet Engineering Task Force (IETF) standard for implementing QoS policies as an end-to-end service. It allows a Policy server to control devices on the network, such as routers and switches, whereby a consistent policy based on business priorities can be achieved. COPS is a companion protocol to Resource Reservation Protocol (RSVP).

**Table 1-15. Protocols Used with QoS**

<b>Protocol</b>	<b>Description</b>
RSVP	Resource Reservation Protocol (RSVP) allows paths on the Internet to be reserved so that voice conversations can be transmitted with minimal delays.

---

**PEP's** Policy Enforcement Points (PEP's) can be routers, gateways and other devices that transfer voice channel signals between subscribers and their calling destinations. When the call is initiated, the PEP's query the Policy server for authorization to reserve bandwidth. Regardless of whether the bandwidth is available or not, VOCAL allows the call to go through. When the call ends, the Policy server sends instructions to the PEP's to release the bandwidth.

---

**PDP** The Policy Decision Point (PDP) is the Policy server. When the PEP's query the Policy server for authorization, the Policy server makes a Policy Decision to either accept or reject the request.

---

### **Quality of Service Enabled**

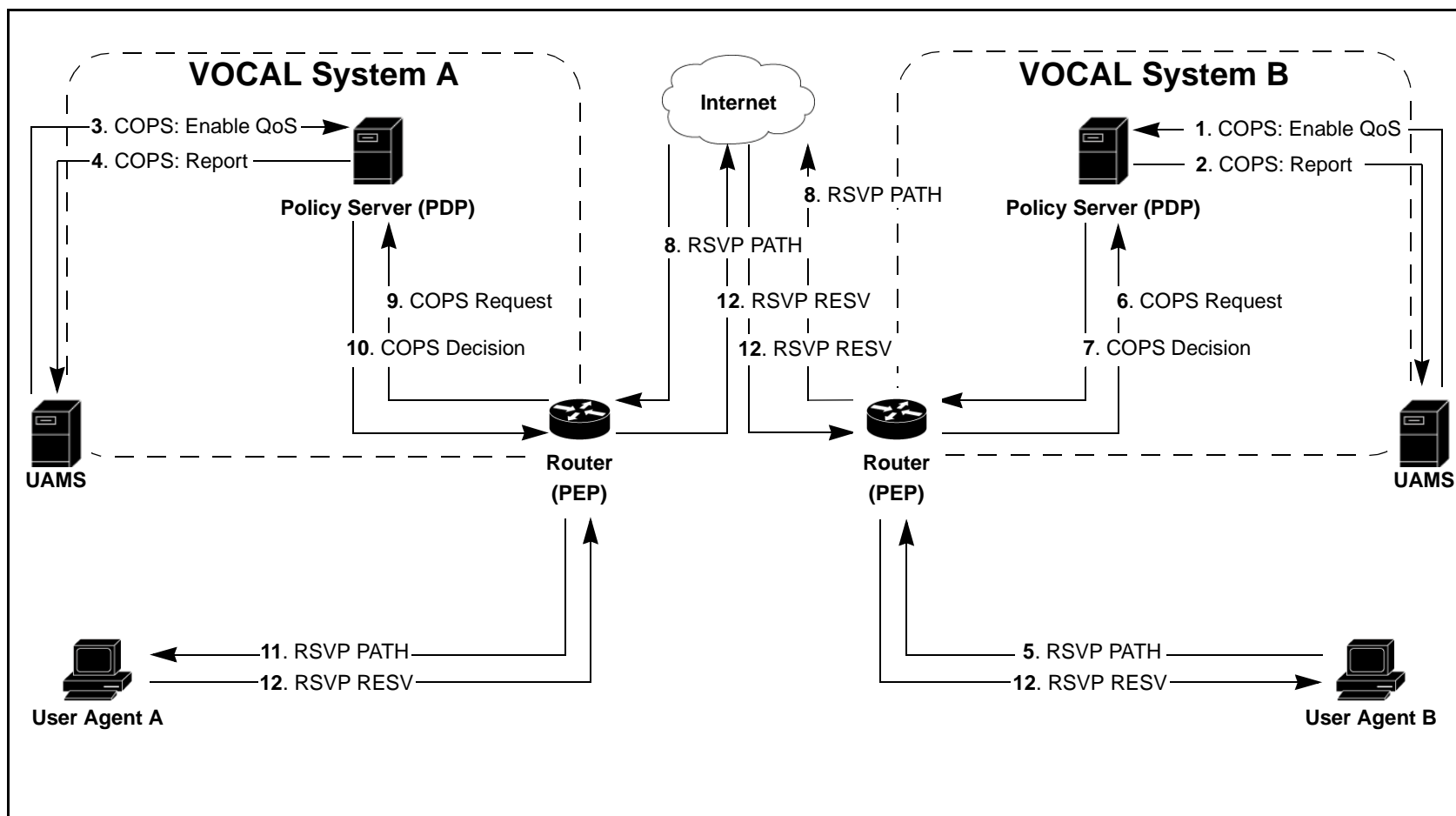
---

**Introduction** This section illustrates the messages exchanged to reserve bandwidth over the Internet, as well as the normal SIP messages used for call signaling.



**Suggesting A Bandwidth Path**

Figure 1-11 shows a request for bandwidth from User Agent B being processed through the networks. These signals are identified with letters, rather than numbers, because they are sent over the voice channel at roughly the same time that User Agent B sends a 180, Ringing, message, see [Figure 1-14](#). Their sequence does not necessarily follow the sequence of the SIP messages shown in Figures 1-12 through 1-14.



**Figure 1-11. Interactions: Suggesting and Reserving a Bandwidth Path**

**Messages A - F Described**

Table 1-16 describes the messages illustrated in Figure 1-11.

**Note**

These signals are identified with letters, rather than numbers, because they are sent over the voice channel at roughly the same time that User Agent B sends a 180, Ringing, message, see [Figure 1-14](#). Their sequence does not necessarily follow the sequence of the SIP messages shown in Figures 1-12 through 1-14.

**Table 1-16. Interactions Shown in Figure 1-11**

<i>Interaction</i>	<i>Step</i>	<i>Description</i>
Enabling QoS	<b>1-4</b>	At the time that the UAMS receives either a 180 or 183 message from the called party, it sends a COPS message to the Policy Server (PoS) requesting it to establish QoS.
Requesting Bandwidth	<b>5</b>	User Agent B sends a RSVP PATH request to suggest a bandwidth path to the on-network router.
Requesting a Decision from the PoS	<b>6-7</b>	The router generates a COPS-RSVP request and sends it to the PoS, which responds with a COPS decision, authorizing the request.
Sending the Request to System A	<b>8</b>	The router sends the RSVP PATH request to the router in VOCAL System A.
Requesting a Decision from the PoS	<b>9-10</b>	The router generates a COPS-RSVP request and sends it to the PoS, which responds with a COPS decision, authorizing the request.
Sending the Request to User Agent A	<b>11</b>	The router sends the RSVP PATH request to User Agent A.
Sending an RSVP RESV	<b>12</b>	UA A sends a RSVP RESV message to UA B, reserving bandwidth.

**Reverse Bandwidth Path**

In order to establish an RTP path going the other way, the UAMS in VOCAL System A initiates the same process as illustrated in Figure 1-11 except in the opposite direction.

**Open Settlement Protocol**

**Definition**

Open Settlement Protocol (OSP) is a product of the Telecommunication and Internet Protocol Harmonization Over Networks (TIPHON) project at the European Telecommunications Standards Institute (ETSI: [www.etsi.com](http://www.etsi.com)), and is a specification for providing interdomain authentication, authorization, and accounting (AAA) standards for IP Telephony.

**Diagram #1:  
Internetwork Calls  
From the calling  
party to the RS**

Figure 1-12 shows User Agent (UA) A initiating a call to User Agent B. In this scenario, the UA's are used together with basic analog phone sets, and are attached to different VOCAL systems, and each VOCAL system is known to the other. The call signal routing is carried over the Internet.

The call may be routed through one or more feature servers before it reaches the Internetwork Marshal (INMS). For the sake of brevity, the feature servers have been omitted from this scenario.

Version 1.4.0 of VOCAL supports multiple INMS's. Each of these servers will accept off-network INVITE messages from one other known SIP-based server. If an INVITE is received from any other off-network entity, it will be rejected regardless if it includes a clearinghouse token or not.

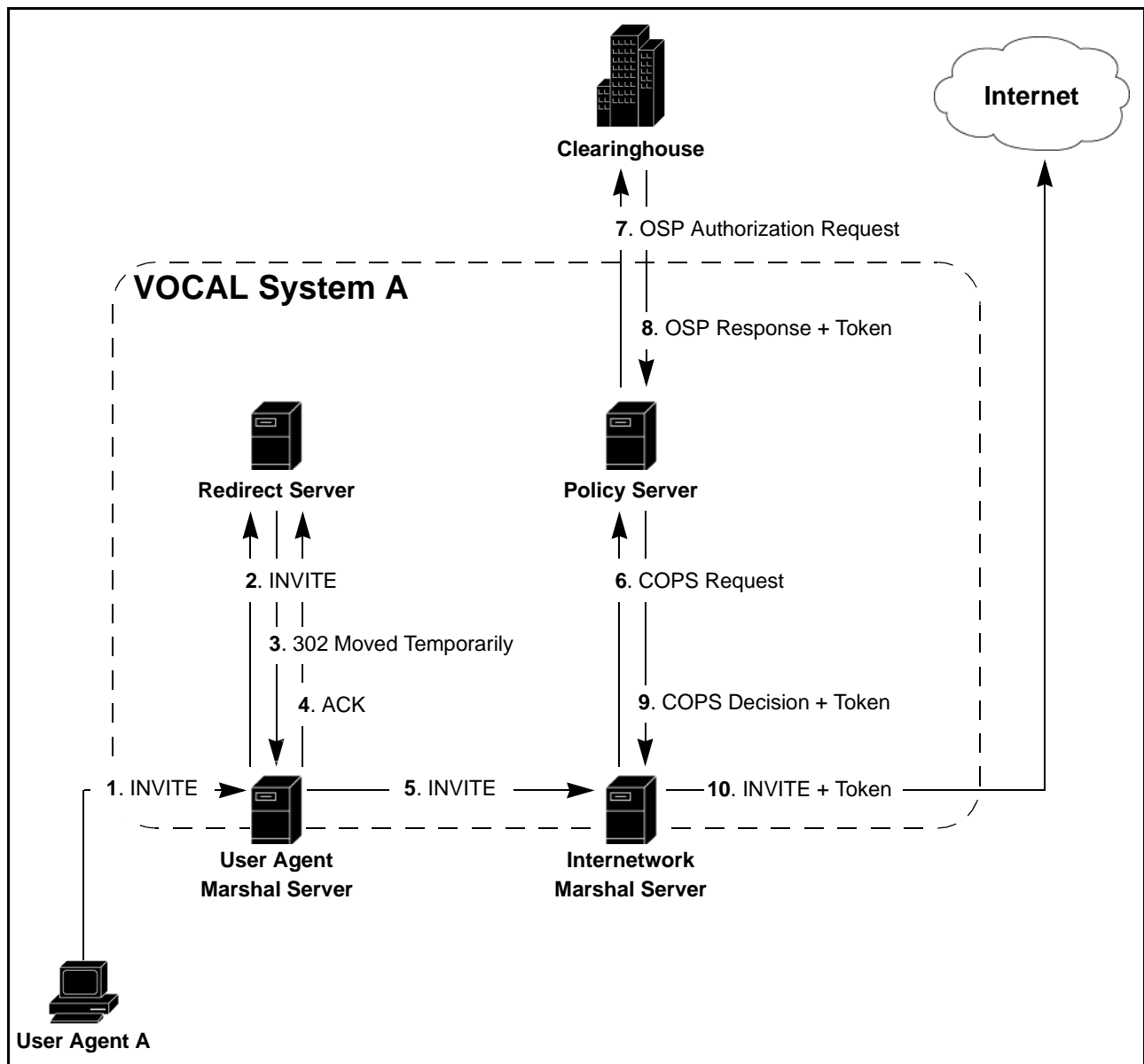


Figure 1-12. Transactions: Originating End

**Messages 1 - 10 Described**

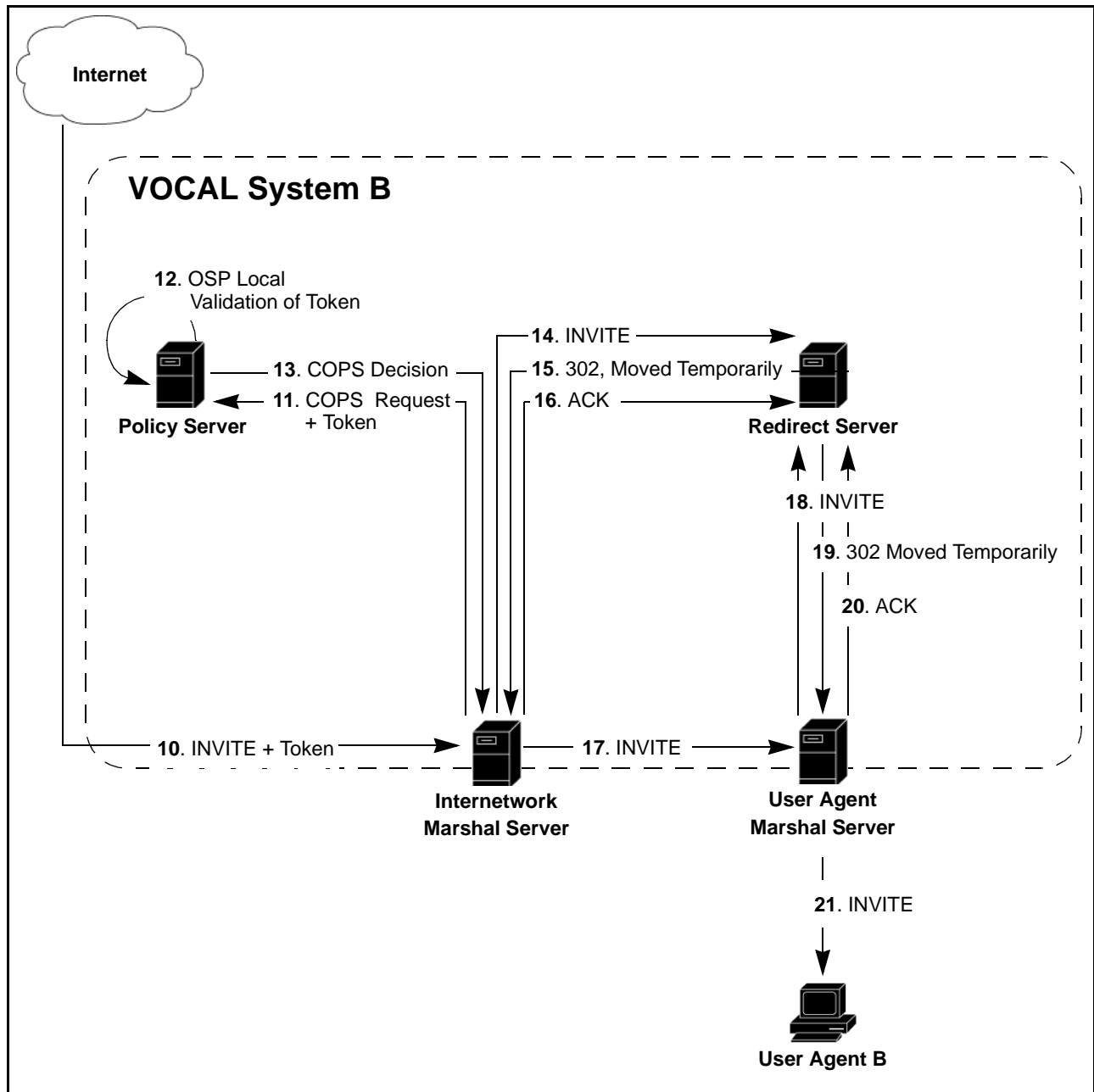
Table 1-17 describes the messages illustrated in Figure 1-12.

**Table 1-17. Interactions Shown in Figure 1-12**

<i>Interaction</i>	<i>Step</i>	<i>Description</i>
SIP phone to INMS	<b>1 - 3</b>	A call is initiated by an analog phone attached to User Agent A. The User Agent Marshal Server (UAMS) authenticates the message and forwards it to the Redirect Server (RS). The RS returns a 302 Moved Temporarily, message that provides routing information.
	<b>4 - 5</b>	The UAMS acknowledges receipt of the 302 message and forwards the INVITE to the Gateway Marshal Server (GWMS).
Requesting and Receiving an Internetwork Token from the Clearing House	<b>6</b>	The Internetwork Marshal Server (INMS) generates a COPS authorization request and sends it to the Policy Server.
	<b>7</b>	The Policy Server (PoS) composes an Open Settlement Protocol (OSP) authorization request and sends it to an internetwork clearinghouse and receives a response plus a token.
	<b>8</b>	The clearinghouse verifies the route, by confirming that the dialed digits are correct, and responds with an OSP Authorization plus a token.
	<b>9</b>	The PoS generates a COPS decision, which includes the clearing house's token, and sends it to the INMS.
INMS forwarding the INVITE Message Plus the Token	<b>10</b>	The INMS adds the token to the INVITE message and forwards it to the Internet via the router.

**Diagram #3: The INVITE Message is Received**

Figure 1-13 shows the receiving network processing the INVITE message and the token.



**Figure 1-13. Transactions: Terminating End**

**Messages 10 - 21 Described**

Table 1-18 describes the messages illustrated in Figure 1-13.

**Table 1-18. Interactions Shown in Figure 1-13**

<i>Interaction</i>	<i>Step</i>	<i>Description</i>
INVITE is received from known system	<b>10</b>	The INVITE message is received by the Internet Marshal Server (INMS).
The receiving INMS receives the INVITE and requests verification from the PoS	<b>11</b>	The INMS generates a COPS request and sends it, along with the token, to the Policy Server for verification.
	<b>12</b>	The Policy Server (PoS) verifies the token with its OSP client. The criteria for verification includes the source, the destination and the clearinghouse host name.
	<b>13</b>	The PoS strips the token from the message, generates a COPS Decision and sends it to the INMS.
The UAMS requests routing information from the RS.	<b>14 - 16</b>	The INMS strips the OSP token from the SIP INVITE header and forwards the INVITE message to the RS for routing. The RS returns a 302 Moved Temporarily and the INMS responds with an ACK message.
The INVITE message is sent to SIP Phone B.	<b>17 - 21</b>	The INMS forwards the INVITE to the UAMS, which forwards it, through the RS, to User Agent B.

**Diagram #4:  
Establishing the  
Audio Path**

Figure 1-14 shows the final series of SIP messages leading up the RTP audio path being established. Message 21, Ringing, is sent at roughly the same time that the RSVP PATH request is sent, see Figure 1-11.

**Figure 1-14. Interactions: Establishing the Audio Path**

**Messages 22 - 25  
Described**

Table 1-19 describes the messages illustrated in Figure 1-14.

**Table 1-19. Interactions Shown in Figure 1-14**

<i>Interaction</i>	<i>Step</i>	<i>Description</i>
Ringing	<b>22</b>	SIP Phone B starts ringing and sends a 180 Ringing message to SIP Phone A.
OK	<b>23</b>	SIP Phone B sends a 200 OK message to SIP Phone A confirming that it is ready for establishing an audio path.
Acknowledge	<b>24</b>	SIP Phone A replies with an ACK message.
Audio Path	<b>25</b>	SIP Phone B is answered and an RTP audio path is established.

## Operation System Support

---

**Introduction** This section describes how the system is managed and supported.

---

**What is OSS?** Operation System Support (OSS) includes methods that are used to monitor and maintain system performance. These methods include provisioning, authentication, billing and network management.

---

### Provisioning

---

**Introduction** Working with the Provisioning server is the subject of two chapters listed as hyperlinks below.

---

**What is Provisioning?** Provisioning is a method for adding and maintaining network users. Users include servers, User Agents and subscribers. Provisioning is divided into two interfaces, one for technicians and the other for system administrators. Each of these interfaces is a java based graphical user interface (GUI) that runs on a web browser.

#### Technician Interface

The technician interface works with maintaining the servers. This interface is described completely in [Chapter 3, Provisioning](#).

#### System Administrator Interface

The system administrator interface works with maintaining the subscribers. This interface is described completely in the System Administration Guide.

---

### Authentication

---

**Introduction** The Marshal servers authenticate every message that they receive. This section explains how.

---

**What is Authentication?** Authentication is the process that protects the system from unauthorized users. The marshal servers authenticate each call by checking the calling party's IP address against a master file. If the marshal server does not have the calling party's address on its list, it requests verification from the Provisioning server. If the Provisioning server does not verify the address, the marshal refuses to authenticate the call. The authentication method can be either Access List or Digest.

---

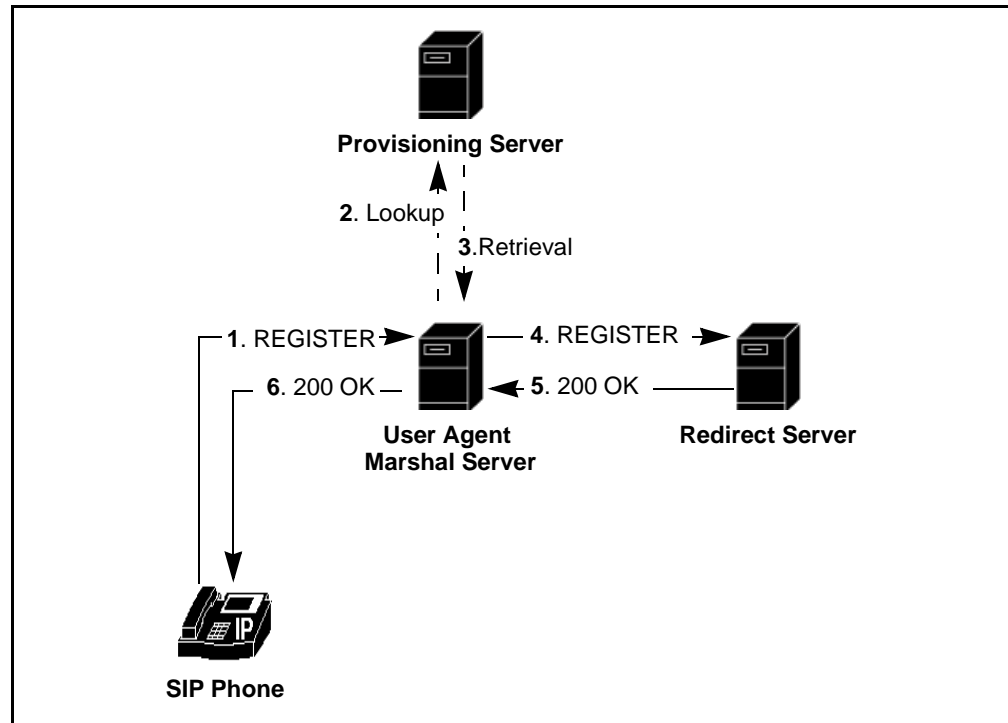
#### Access List

**Overview**

If the User Agent Marshal Server authenticates the user agent, it forwards the user agent's message through to the Redirect Server. If the message is REGISTER, the Redirect server registers the user agent, and returns a confirmation message back through the User Agent Marshal Server to the user agent.

**Diagram: calling party Authentication**

Figure 1-15 shows a SIP phone registering with the Redirect Server.



**Figure 1-15. Calling Party Registration: Access List**

**Messages 1 - 6 Described**

Table 1-20 describes the messages illustrated in Figure 1-15.

**Table 1-20. Interactions Shown in Figure 1-15**

<i>Interaction</i>	<i>Step</i>	<i>Description</i>
SIP Phone to UAMS	<b>1</b>	The SIP Phone is connected to the network and immediately sends a REGISTER message to the User Agent Marshal Server (UAMS).
UAMS to PS	<b>2 - 3</b>	The UAMS does not have a record of the SIP Phone's IP address in its database and it retrieves data from the Provisioning Server (PS) to validate the request. The UAMS adds the SIP phone to its list of authorized users.
UAMS to RS	<b>4</b>	The UAMS forwards the REGISTER message to the Redirect Server (RS).



Table 1-20. Interactions Shown in Figure 1-15 (Continued)

Interaction	Step	Description
OK Returned	5 - 6	The UAMS forwards the OK to the SIP Phone. The phone is registered in the system, and it will re-register every few minutes.

## Digest

### Overview

The Digest method for authentication and registration uses a password. This password is maintained in the Provisioning Server's database.

### Diagram: calling party Authentication

Figure 1-16 shows a SIP phone registering with the Redirect Server.

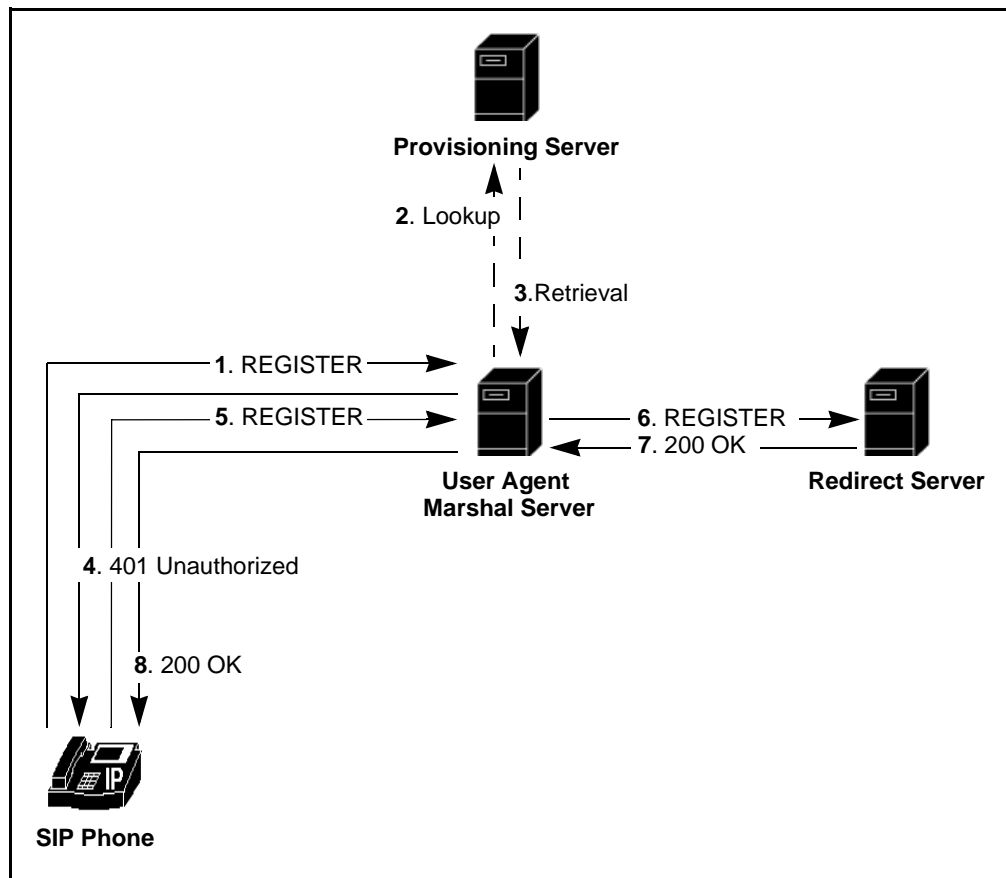


Figure 1-16. calling party Registration: Digest

**Messages 1 - 8 Described**

Table 1-21 describes the messages illustrated in Figure 1-16.

**Table 1-21. Interactions Shown in Figure 1-16**

<i>Interaction</i>	<i>Step</i>	<i>Description</i>
SIP Phone to UAMS	<b>1</b>	The SIP Phone is connected to the network and immediately sends a REGISTER message to the User Agent Marshal Server (UAMS).
UAMS to PS	<b>2 - 3</b>	The UAMS does not have a record of the SIP Phone's IP address in its database and it retrieves data from the Provisioning Server (PS) to validate the request. The UAMS adds the SIP phone to its list of authorized users.
Unauthorized	<b>4</b>	The UAMS returns a 401 Unauthorized message to the SIP Phone requesting a password.
New REGISTER message	<b>5</b>	The SIP sends a new REGISTER message that includes a password.
UAMS to RS	<b>6</b>	The UAMS authenticates the calling party and forwards the REGISTER to the RS.
OK Returned	<b>7 - 8</b>	The RS replies with a 200 OK message, which is forwarded to the SIP phone by the UAMS. The phone is registered in the system, and it will re-register every few minutes.

## Call Detail Records and Billing

**Introduction**

The VOCAL system has a Call Detail Record (CDR) server that receives time-stamped information about every processed call. This information can be forwarded to a third-party billing system by using a Remote Authentication Dial In User Service (RADIUS) stack.

### Call Detail Records

**How Does the CDR Server Receive its Data?**

The CDR server communicates with the marshal servers over TCP/IP. As it has been shown above under ["Call Control" on page 1-16](#), every call involves both incoming and outgoing marshal servers. At the time when a call starts and again when it ends, both marshal servers notify the CDR server. From this notification, the CDR server creates a new billing file, called billing.dat, with two Start and two End records, one of each from both marshal servers.

**What Defines the Start of a Call?**

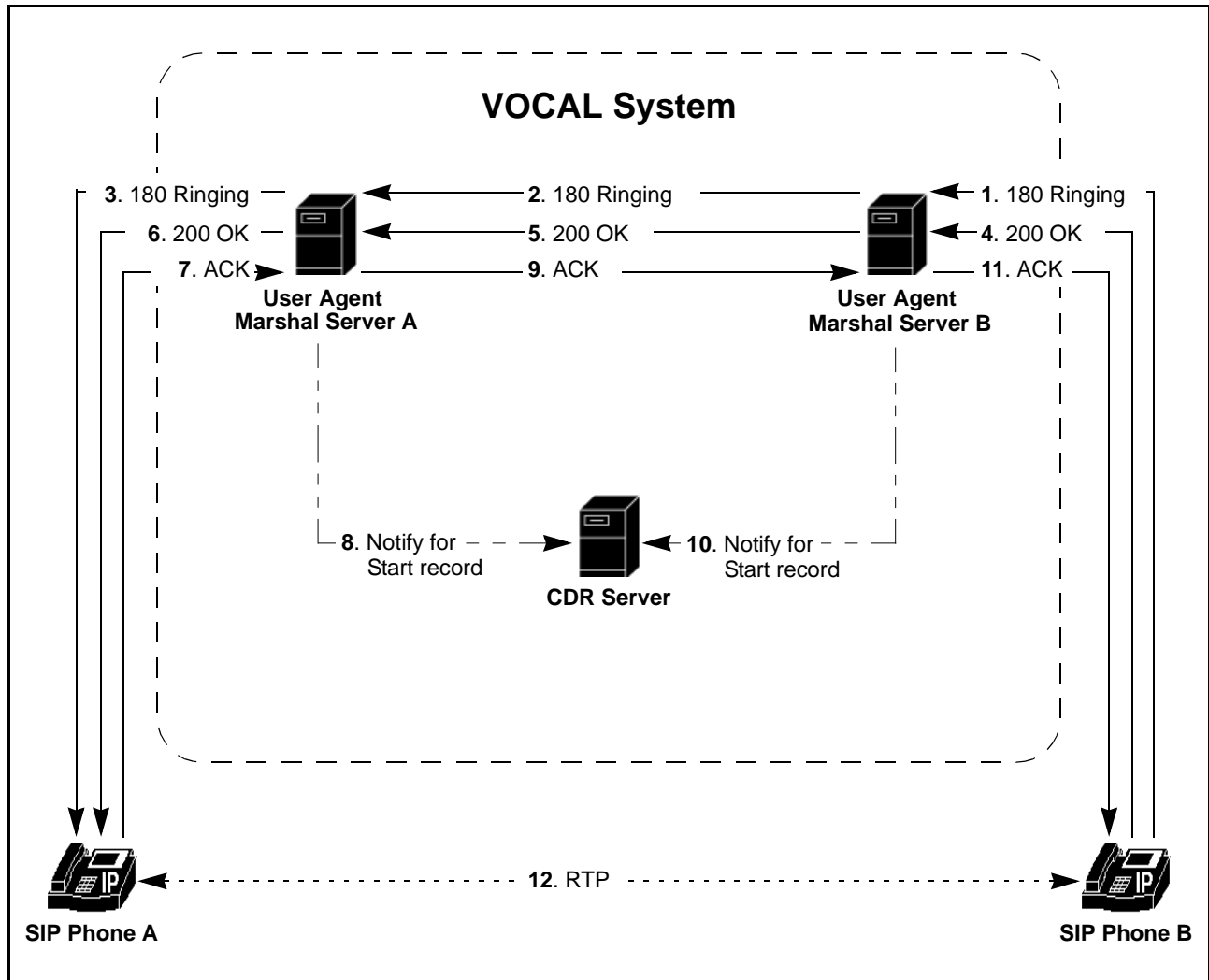
In a conventional setup, the start of a call happens when the voice channel is established. After the INVITE has been transmitted from the calling party to the called party, and the called party starts ringing, the called party picks up and thereby, transmits a 200, OK, message to the calling party. When the calling party replies with an ACK message, the marshal servers notify the CDR server to create a START record.

■ **Note**

You can provision the CDR server to bill for ring time. If you do, the marshals notify the CDR server to create a start record when they receive the 180, Ringing, message from the called party.

**Notifying CDR Server for START Record**

Figure 1-17 shows the SIP messages that lead up to the marshal servers notifying the CDR server to create a START record. In this scenario, the INVITE has already passed from SIP Phone A to SIP Phone B, as shown above in Figure 1-5.



**Figure 1-17. Notifying the CDR Server for the Start Record**

**Messages 1-12 Described**

Table 1-22 describes the message illustrated in Figure 1-17.

**■ Note**

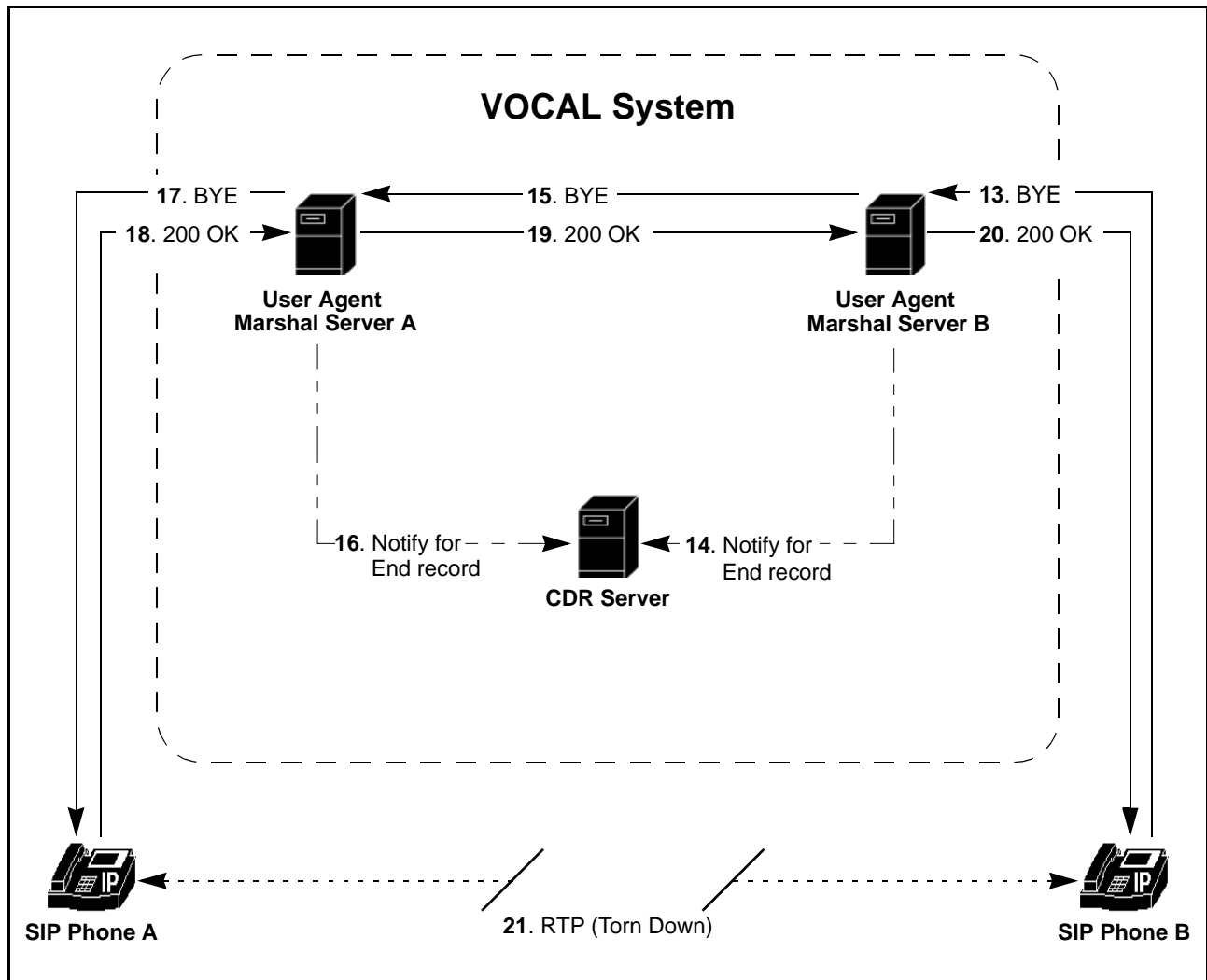
Message #1 in Figure 1-17 occurs after the INVITE has been passed from SIP Phone A, through the system to SIP Phone B. For more information, see Figure 1-5 and Table 1-9.

**Table 1-22. Interactions Shown in Figure 1-17**

<i>Interaction</i>	<i>Step</i>	<i>Description</i>
Ringling	<b>1 - 3</b>	SIP Phone B sends a 180 Ringing response to User Agent Marshal Server (UAMS) B, which is forwarded.
Pick-up	<b>4 - 6</b>	SIP Phone B sends a 200 OK response to the UAMS. This means that the phone has been activated and is ready to establish voice channel contact with SIP Phone A.
Pick-up acknowledged	<b>7</b>	SIP Phone A sends an ACK message to UAMS A confirming that it is ready to connect to a voice channel.
CDRS notified	<b>8</b>	UAMS A notifies the Call Detail Record Server (CDRS) that the call has started.
Pick-up acknowledged	<b>9</b>	UAMS A forwards the ACK message to UAMS B.
CDRS notified	<b>10</b>	UAMS B notifies the CDRS that the call has started.
Pick-up acknowledged	<b>11</b>	UAMS B forwards the ACK message to SIP Phone B.
A conversation takes place	<b>12</b>	The calling parties talk to each other using Real-time Transfer Protocol (RTP).

**What Defines the End of a Call?**

The end of a call happens when the first phone hangs up and, thereby, sends a BYE message to the other phone. Upon receiving the BYE message each marshal server notifies the CDR server to create an End record. This process is illustrated in Figure 1-18.



**Figure 1-18. Notifying the CDR Server for the End Record**

**Messages 13-21 Described**

Table 1-23 describes the message illustrated in Figure 1-18.

**Table 1-23. Interactions Shown in Figure 1-18**

Interaction	Step	Description
SIP Phone B Hangs Up	13	SIP Phone B sends a BYE request to User Agent Marshal Server (UAMS) B.
Notifying the CDRS	14	UAMS B notifies the Call Detail Record Server (CDRS) that the call has ended.

**Table 1-23. Interactions Shown in Figure 1-18 (Continued)**

<i>Interaction</i>	<i>Step</i>	<i>Description</i>
The BYE is forwarded from one UAMS to the other.	<b>15</b>	UAMS B forwards the BYE message to UAMS A.
Notifying the CDRS	<b>16</b>	UAMS A notifies the CDRS that the call has ended.
The BYE is received by SIP Phone A.	<b>17</b>	UAMS A forwards the BYE message to SIP Phone A.
SIP Phone A Hangs Up	<b>18 - 20</b>	SIP Phone A sends an ACK message, through the UAMs, to SIP Phone B.
The Voice Channel is torn down	<b>21</b>	The BYE and ACK messages trigger the voice channel to shut down.

## Billing

### Introduction

The section above shows how the CDR Server collects data about each call. This data collection occurs regardless if there is a third-party billing system attached to the network or not. This section explains how the call detail records can be used to generate billing.

### The Bill Record

After receiving notifications from the marshal servers about the start and end of each call, the CDR Server generates a Bill record that contains a duration field. This field is the calculated difference between the start and end times of the call. These Bill records can be sent from the CDR server to a third-party billing system on a regular schedule using RADIUS messaging over UDP.

New billing files, that have not been sent to the billing server, have a .unsent extension appended to their file name. Billing files are normally purged from the CDR Server after 72 hours.

### Sending Records with RADIUS

The CDR server uses a RADIUS stack to communicate with the billing system. In order to send records to the billing system, you must know which Vendor Specific Attributes are being used in the billing system's code, and modify the CDR server to accept those attributes. For more information, go to the [www.vovida.org](http://www.vovida.org) web site.

The billing data is not sent during real time. You must set up a transmission schedule for hourly, daily or for the frequency that best suits your needs. For more information about setting up the CDR Server and the billing transmission frequency, see "[CDR Servers, Data Entry Fields](#)" on page 3-40.

## **Network Management**

---

### **Introduction**

Network management is the subject of a chapter in the System Administration guide. This section provides a brief description and a hyperlink to the chapter.

---

### **How Does VOCAL Provide Network Management**

The VOCAL system uses Simple Network Management Protocol (SNMP) to control and monitor system processes. VOCAL provides a java-enabled GUI for the System Administrator to help him or her manage the system. Network Management is described in more detail in the System Administration Guide.

---

## Features

---

<b>Introduction</b>	Some features are provided by the VOCAL system regardless of the types of phones used by the calling parties. Other features are only available on certain IP phone sets. This section explains the differences between these types of features.
<b>What are Features?</b>	Features are the enhanced functions of the phone system that enable customers to do more than simply make and receive phone calls. Features are referred to as being either Core System or Set-based. Core System features are those that are provided by the VOCAL system. Some of these features are built-in to the SIP messaging such as, Calling Line Identification. Set-based features are those which are dependent on the design of the phone set such as, Transfer.
<b>What is CPL?</b>	The Call Processing Language (CPL) is used to describe and control Internet telephony services that are implemented on either network servers or user agent servers. CPL scripts are normally simple, extensible, and easy to edit. For more information about CPL see <a href="http://www.ietf.org/internet-drafts/draft-ietf-iptel-cpl-04.txt">http://www.ietf.org/internet-drafts/draft-ietf-iptel-cpl-04.txt</a> .

---

## SIP Messages and Feature Servers

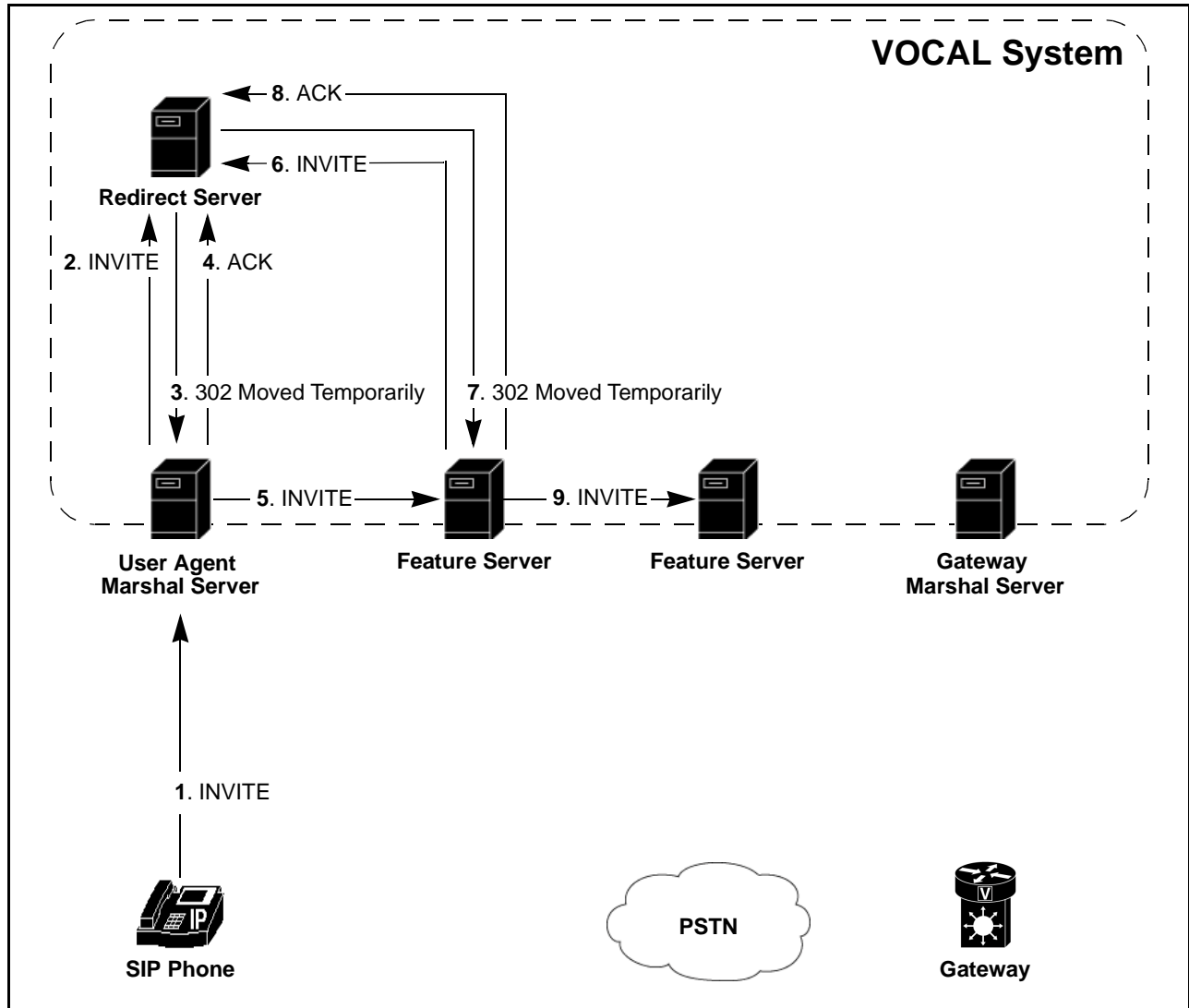
---

<b>Introduction</b>	This section illustrates how the VOCAL system routes calls to feature servers by using SIP messages. When the feature servers first come on-line, they download a register from the Provisioning Server but they do not download the file that controls the feature. It is not until the first time that the Feature Server runs a script, that it downloads the controlling file from the Provisioning Server.
---------------------	---



**Diagram #1: SIP Messages to the Feature Servers**

Figure 1-19 shows a Feature server receiving a message from a Marshal and then requesting routing information from the Redirect server. It is possible that a call signal may be routed to several Feature servers before leaving the VOCAL system. Some calls may not be routed to any Feature servers before going to the outbound Marshal.



**Figure 1-19. SIP Message Flow to the Feature Servers**

**Messages 1 - 7 Described**

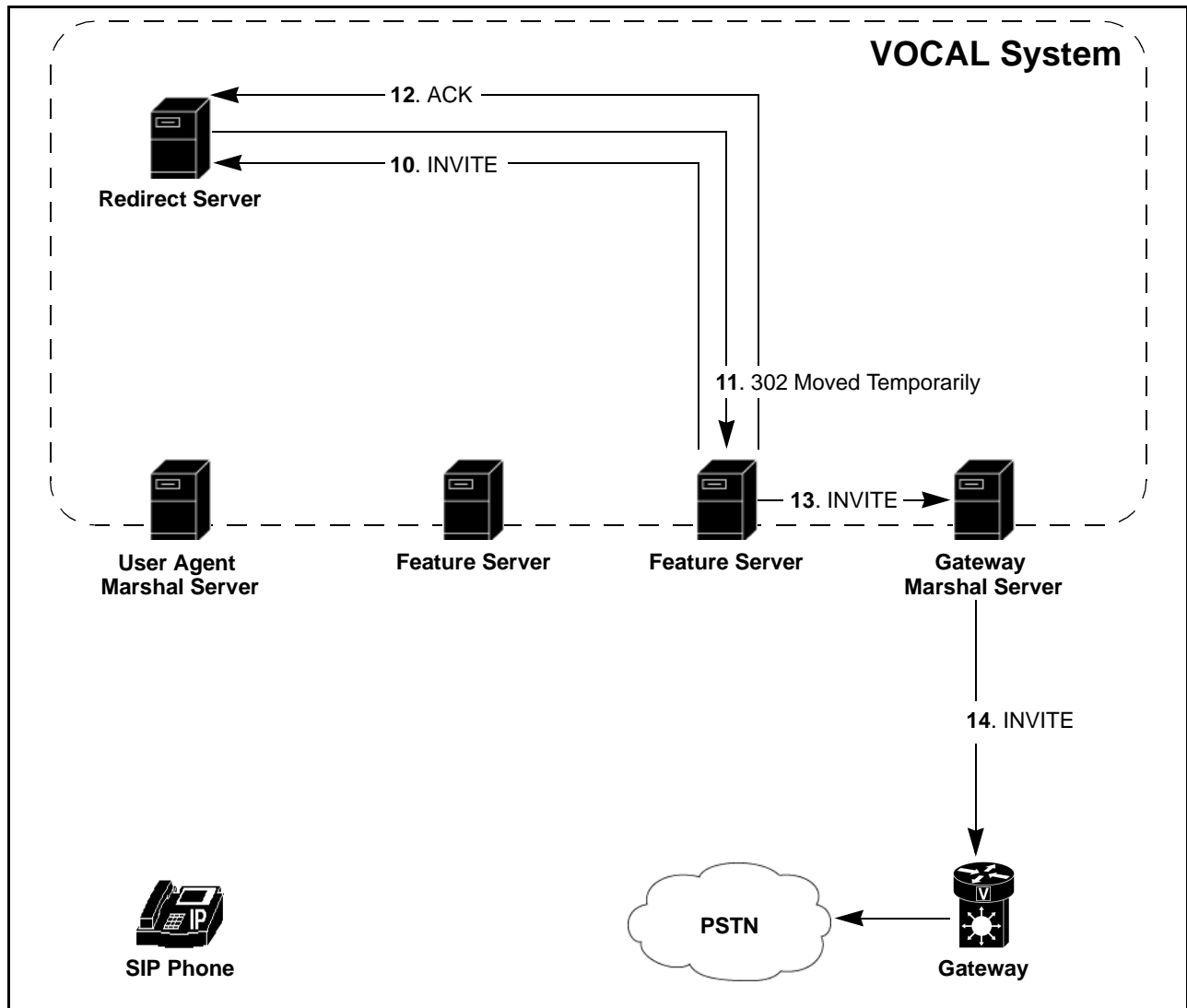
Table 1-24 describes the messages illustrated in Figure 1-19.

**Table 1-24. Interaction shown in Figure 1-19**

<i>Interaction</i>	<i>Step</i>	<i>Description</i>
SIP phone to UAMS	<b>1</b>	A call is initiated at one SIP phone to call a party attached to the PSTN. The SIP phone sends an INVITE message to the User Agent Marshal Server (UAMS).
UAMS to RS	<b>2 - 4</b>	<p>The UAMS authenticates the user and forwards the INVITE message to the Redirect Server (RS). The RS looks up the contact information for the calling user, which includes the Call Blocking and Calling Party ID Blocking features. The called party destination is on the PSTN, therefore the RS has no contact list for the called party, but through its dial plan, the RS can provide routing information. The RS writes the calling party feature and called party routing information to a 302 message and sends it to the Marshal server, which completes the transaction with an ACK message.</p> <p><b>■Note</b> The RS does not determine whether the called number is on the user's call blocking list. As long as the Call Blocking feature is assigned to this user, the RS will send every call from that user through the Call Blocking Feature server.</p>
UAMS to a feature server via the RS.	<b>5</b>	The UAMS generates a new INVITE message and sends it to the Call Blocking Feature Server (FS).
The message is redirected to a second feature server	<b>6 - 8</b>	The Call Blocking FS generates a new INVITE message and sends it to the RS. As it did earlier, the RS looks up the calling party's contact list and the called party's routing information. From the information provided in INVITE message, the RS knows that the message has come from the Call Blocking Feature server and provides routing information that will direct it towards the Calling Party ID Blocking FS. The RS writes this information to the 302, and sends it to the Call Call Blocking FS, which responds with an ACK to complete the transaction.
Feature server to Feature server	<b>9</b>	The Call Blocking FS generates a new INVITE message and sends it to the Calling Party ID Blocking FS.

**Diagram #2:  
Feature Servers to  
PSTN**

Figure 1-20 shows the INVITE message being redirected from the feature servers to the PSTN.



**Figure 1-20. Feature Servers to PSTN**

**Messages 8 - 12  
Described**

Table 1-25 describes the messages illustrated in Figure 1-20.

Table 1-25. Interaction shown in Figure 1-20

Interaction	Step	Description
Feature server to GWMS	10 - 12	<p>The Calling Party ID Blocking Feature Server (FS) generates a new INVITE message with calling party ID blocking instructions, and sends it to the Redirect Server (RS) for routing. The RS, once again, calls up the contact list for the calling party and the routing for the called party. The INVITE contains information telling the RS that the message has been routed through both Feature servers listed on the calling party's contact list. As the called party is on the PSTN, the RS does not have its contact list and therefore writes instructions to the 302 message to route the call to the Gateway Marshal server. This 302 is sent to the Calling Party ID Blocking Feature Server, which returns an ACK to complete the transaction.</p> <p><b>■ Note</b> If the called party had been a subscriber to this system, the RS would have been able to call up its contact list and would have sent the message through the listed Feature servers before sending it to the appropriate Marshal server.</p>
GWMS out to the PSTN	13	<p>The GWMS forwards the INVITE to the Gateway Marshal server, which forwards it to the gateway.</p> <p><b>■ Note</b> In version 1.4.0 of VOCAL, the GWMS does not forward INVITE messages back to the RS for final routing. This step was removed to speed up the call processing.</p>
	14	<p>The Gateway translates the message into a signaling format that is used on the PSTN and sends it out to the called party.</p>

## Core Features

### What's a Core Feature?

Core features are network features that operate independently of the User Agent appliance used by the customer. These features include calling line information features, call forwarding, call blocking and call screening.

### Calling and Called Features

Calling features are assigned to the call originator, and include Call Blocking, calling party ID Blocking and others. Called features are assigned to the calling destination, and they include Call Screening, Call Forward and others.

### Calling Line Information Features

#### Calling Number Delivery (CND)

*A calling feature:* Calling Number Deliver (also known as Calling Line Identification (CLID)) provides information to the line about where the call is to be terminated, the Directory Number where the call was originated as well as the date and time of the call.

### **Calling Name Delivery (CNAM)**

*A calling feature:* Calling Name Delivery (also known as Calling Party Name Delivery (CPND)) provides information to the line about where the call is to be terminated, the calling party's name as well as the date and time of the call.

### **Calling Party Identity Blocking (CIDB)**

*A calling feature:* calling party ID Blocking allows a subscriber to control whether or not their number (CND) or name (CNAM) is delivered when they place an outgoing call.

---

## **Call Forwarding**

### **Call Forward All Calls (CFA)**

*A called feature:* Call Forward – All Calls allows a customer to re-route all calls to an alternative number. When CFA is activated, a call to the listed number is redirected to a user selected alternative number or a voice messaging system.

### **Call Forward – No Answer Mode (CFNA)**

*A called feature:* Call Forward – No Answer Mode allows a customer to specify where an unanswered call should be routed. When CFNA is activated, a call to the listed number, that does not answer in a specified number of ringing cycles, will be forwarded to an alternative number selected by the user.

### **Call Forward – Busy Mode (CFB)**

*A called feature:* Call Forward – Busy Mode allows a customer to specify where a call should be routed when the listed number is in use. When CFB is activated, a call to the listed number, while it is in use, will be redirected to another number.

---

## **Call Blocking**

*A calling feature:* It prevents the customer from establishing connections to specified parties such as, 1-900 numbers.

#### **■Note**

For version 1.4.0 of VOCAL, long-distance call blocking only works for calls originating from the North American Numbering Plan (NANP). Calls cannot be blocked if they originate from Europe, Asia or other locations that are not part of the NANP. For more information, see [www.nanpa.com](http://www.nanpa.com).

---

## **Call Screening**

*A called feature:* It prevents incoming calls from specified parties to establish connections with the customer.

#### **■Note**

For version 1.4.0 of VOCAL, phone numbers entered for call screening must include the area code, regardless if they are local or long-distance phone numbers. Call Processing Language does not provide a pattern matching method that differentiates seven digit (local) phone numbers from ten digit (long-distance) numbers.

---

## Set Features

---

<b>What are Set Features?</b>	Set features are features that depend on the User Agent appliance. The VOCAL system supports transfer, call return and call waiting features.
<b>Transfer</b>	Call Transfer allows a user, on any existing two-party call, to place the existing call on hold and originate another call to a third party. The user may consult privately or connect the original call to the third party.
<b>Call Return</b>	Call Return allows the subscriber to place a call back to the last number that called him or her by dialing a special feature code. <b>■Note</b> Call Return can be either a Core System or a Set-based feature.
<b>Call Waiting (CW)</b>	Call Waiting notifies a telephone user, who is on an established call, that an additional external call has been presented and is “waiting to be answered”. The waiting call receives normal ringing until it is answered, the incoming calling party abandons the call, or the ringing cycle timer expires, and the call is given Call Forward-No Answer treatment (if applicable). Only one Call Waiting call can be present at a time. Additional calls that may be presented are provided with Busy Mode treatment (CFB, if applicable). <b>■Note</b> Implementation of Call Waiting requires support from the phone sets. <b>Cancel Call Waiting (CCW)</b> Otherwise known as “Do Not Disturb”, Cancel Call Waiting allows the subscriber to dial a feature activation code prior to making a call. For the duration of the subsequent call, the Call Waiting feature will be disabled for that line. The Cancel Call Waiting feature lasts only for the duration of one call and, when the subscriber goes on-hook again, their Call Waiting feature is re-enabled.

---

## Scriptable Feature Development

---

<b>What are Scriptable Features?</b>	Scriptable features are features that can be expressed in a scripting language such as, Call Processing Language (CPL). The VOCAL system supports new feature development through CPL scripts. For more information, see the System Administration Guide.
--------------------------------------	--

---

# Index

---

## A

AAA 1-25  
Authentication  
    defined 1-33  
    illustrated 1-34, 1-35  
Authorization, Authentication and  
    Accounting 1-25

## B

Busy Mode 1-48  
BYE  
    illustrated 1-19

## C

Call Blocking 1-47  
Call Control 1-16–1-32, ??–1-33  
Call Forward – Busy Mode 1-47  
Call Forward – No Answer Mode 1-47  
Call Forward All Calls 1-47  
Call Forwarding 1-47  
Call Return 1-48  
Call Screening 1-47  
Call Transfer 1-48  
Call Waiting 1-48  
Caller Identity Blocking 1-47  
Calling and Called Features 1-42  
Calling Name Delivery 1-47  
Calling Number Delivery 1-46  
Cancel Call Waiting 1-48  
CCW 1-48  
CFA 1-47  
CFB 1-47, 1-48  
CFNA 1-47  
CIDB 1-47  
CNAM 1-47  
CND 1-46  
Common Open Policy Service 1-9  
COPS 1-9  
    policy enforcement points 1-25  
Core Features 1-46–1-47  
CW 1-48

## D

DHCP 1-9  
Diagram 1-24  
DNS 1-9  
Domain Name System 1-9  
Dynamic Host Configuration Protocol 1-9

## F

Feature Server  
    Call Blocking 1-22  
    call routing 1-22–1-24

    defined 1-6  
Features 1-42–1-48  
    Call Blocking 1-47  
    Call Forward – Busy Mode 1-47  
    Call Forward – No Answer Mode 1-47  
    Call Forward All Calls 1-47  
    Call Forwarding 1-47  
    Call Return 1-48  
    Call Screening 1-47  
    Call Transfer 1-48  
    Call Waiting 1-48  
    Caller Identity Blocking 1-47  
    calling and called 1-46  
    Calling Name Delivery 1-47  
    Calling Number Delivery 1-46  
    Cancel Call Waiting 1-48  
    Do Not Disturb 1-48  
    scriptable feature development 1-48  
    set features 1-48

## G

Gateways  
    defined 1-5  
    PSTN gateway 1-5  
    residential gateways 1-5

## GUI

    defined 1-4

## H

Heartbeat Server 1-7  
HTTP 1-9  
Hypertext Transfer Protocol 1-9

## I

Internetwork Marshal  
    policy client 1-25  
INVITE  
    illustrated 1-16  
IP Phone 1-4

## J

JTAPI Server 1-6

## L

Location Server 1-10

## M

Marshal Server  
    defined 1-6  
Media Gateway Control Protocol 1-9  
MGCP 1-9

## Index (Continued)

---

### N

Network Management 1-41  
Network Manager 1-6

### O

Open Settlement Protocol 1-9  
Operation System Support 1-33–1-41  
OSP  
    defined 1-9

### P

PDP 1-26  
PEP 1-26  
Policy Decision Point 1-26  
Policy Enforcement Point 1-26  
Policy Server 1-7  
Provisioning 1-33  
Provisioning Server  
    defined 1-6  
Proxy Server 1-10  
PSTN  
    calling to 1-20–1-22  
    illustrated 1-21  
PSTN Gateway 1-5

### Q

Quality of Service 1-25–1-32, ??–1-33  
    illustrated 1-26–1-32, ??–1-33

### R

RADIUS  
    defined 1-9  
Real-time Transfer Protocol 1-9  
Redirect Server 1-10  
    defined 1-6  
Registrar Server 1-10  
Registration  
    illustrated 1-34, 1-35  
Remote Authentication Dial-In User Service 1-9  
Residential Gateway 1-5  
Resource Reservation Protocol 1-9  
RSVP  
    defined 1-9, 1-26  
    PATH 1-27  
RTP  
    defined 1-9

### S

Scriptable Feature Development 1-48  
Set Features 1-48  
Signaling 1-16

Request messages 1-12  
Response Messages 1-13  
Simple Network Management Protocol  
    Network Management 1-41

### SIP

basic call flow 1-11–1-12  
compatible protocols 1-9  
defined 1-8  
overview 1-8–1-9  
request messages 1-12  
response messages 1-13

### SNMP

    Network Management 1-41

Softswitch 1-16

### T

TCP 1-9  
Translators 1-4  
Transmission Control Protocol 1-9

### U

UDP 1-9  
User Datagram Protocol 1-9

### V

VOCAL  
    definition 1-3  
Voice Mail 1-6