

# VoiceMaster User Guide

Version 5.0



# Contents

## Preface

Disclaimer/Copyrights .....	3
Warranty and Limited Liability .....	3
SysMaster Technical Support and Services.....	5

## Chapter 1: VoIP Overview

In This Chapter.....	7
Prologue .....	7
VoIP Architecture and Operation.....	9
VoIP Devices and Roles.....	11
H.323 Protocol Architecture .....	15
Session Initiation Protocol (SIP).....	16
VoIP Performance Variables .....	19
VoiceMaster: A Comprehensive VoIP Solution.....	22

## Chapter 2: VoiceMaster Installation

In This Chapter.....	39
General Safety Warnings .....	39
Hardware Installation.....	40
VoiceMaster Initial Configuration.....	49

## Chapter 3: VoIP Service Configuration

In This Chapter.....	57
Overview .....	57
Configure Routing Tables (Routes).....	71
Billing Configuration .....	75
Activating VoIP Service: Linking Routes, Rates and Subscribers .....	80

## Chapter 4: VoiceMaster Administration

In This Chapter.....	87
Network Configuration.....	88
System Users Configuration.....	98
System Settings .....	103
Billing Settings .....	119
Payment Methods .....	124
Security .....	126
Fault Tolerance .....	137
Interface Customization.....	145
Miscellaneous Functions .....	166

## Chapter 5: Account Administration

In This Chapter.....	171
Overview .....	171
Administration Console Review.....	172
General Account Settings.....	173
Individual Accounts Administration.....	179

## Chapter 6: Event Monitoring

In This Chapter.....	199
----------------------	-----

VoiceMaster User Guide .....	
Call Calculator .....	200
System Alerts .....	204
Real-Time Stats.....	209
Real-Time Logs.....	216
Reports.....	219
 <b>Chapter 7: Route Management</b>	
In This Chapter.....	229
Console Overview .....	229
Routing Concepts And Configuration.....	230
Gatekeepers.....	240
Uniswitch.....	250
Special Routing Topics.....	250
 <b>Chapter 8: Rate Administration</b>	
In This Chapter.....	263
Overview .....	263
Rate Administration.....	265
Billing Rates Administration.....	273
 <b>Chapter 9: Batch Administration</b>	
In This Chapter.....	283
Overview .....	283
Configuring Global Batch Settings .....	284
Reseller Batch Administration .....	285
Corporate Client Batch Management.....	294
 <b>Chapter 10: Special Implementations</b>	
In This Chapter.....	299
Managed Services Configuration .....	299
ISP Billing .....	305
 <b>Chapter 11: Custom Modules</b>	
In This Chapter.....	311
Overview .....	311
Calling Plans Module.....	312
CDR Collection Module .....	317
Custom Maps Module .....	320
Custom Prompts Module.....	325
Custom Service Plans Module .....	329
Custom Tax Module .....	333
Discount Credit Time Module .....	336
Exception Numbers Module .....	339
Flag Fall Billing Module .....	343
Multi-Level Marketing Plans Module .....	347
Progressive Billing Module .....	350
Provider Time Interval Module .....	354
Rate Switching Module.....	359
Softphone Profiles Module .....	362
Special Numbers Module .....	365
Time Interval Module.....	371

# Preface

## **Disclaimer/Copyrights**

Copyright 2005 SysMaster Corporation. All Rights Reserved.

This User Guide and the products described within are the sole property of SysMaster Corporation. No part of this guide may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into another language for any purpose except documentation archiving without the express written permission of SysMaster Corporation.

SysMaster provides this guide ‘as is’, without warranty, express or implied. In no event shall SysMaster, its officers, directors, employees or agents be liable for indirect, special, incidental or consequential damages (whether for loss of profits, business, use or data, or interruption of business), even if SysMaster has been advised of the possibility of such damages arising from defect or error in this documentation or the product described.

The specifications and information contained within this guide are provided for informational use and are subject to change at any time without notice. Statements of specifications are intended for informational purposes. SysMaster does not commit to the accuracy of such information. Neither does SysMaster assume responsibility or liability for errors or inaccuracies that may appear in the manual, including hardware and software described.

Products and corporate names appearing in this guide may or may not be registered trademarks or copyrights, and are used for identification or explanation purposes, without intent to infringe.

Product Name: VoiceMaster and VoiceMaster User Guide

VoiceMaster User Guide Version: Version 2.0

Release Date: **Nov 2005**

## **Warranty and Limited Liability**

**Six Months**

SysMaster warrants supplied hardware for one hundred eighty days (180) from shipment. SysMaster will refund the cost of defective hardware for the first thirty (30) days of this period. Between 30 and 180 days from the shipment date, defective hardware may be exchanged. After 30 days has expired, no refund is available. After 180 days, no exchange is provided.

SysMaster's sole obligation under this express warranty shall be, at SysMaster's option and expense, to repair the defective product or part, deliver to Customer an equivalent product or part to replace the defective item, or if neither of the two foregoing options is reasonably available, SysMaster may, *in its sole discretion*, refund to Customer the purchase price paid for the defective product. All products returned for replacement become the property of SysMaster.

Replacement products may be new or reconditioned.

## **Warranty and Limited Liability**

---

In no event will SysMaster's liability for any damages, losses and causes of actions whether in contract or tort [including negligence or otherwise] exceed the purchase price paid for the device covered by this warranty.

### **Software**

SysMaster provides licensed software to the customer, the exact configuration to be determined before shipment of same. Customer assumes responsibility for the selection of the appropriate applications program and associated reference materials.

As described, all software sold as part of the VoiceMaster system is licensed and accessed through a key supplied by SysMaster. The decision to purchase and integrate additional VoiceMaster software modules is at the customer's discretion. It is similarly supplied with a license, and can be purchased from SysMaster separately.

SysMaster makes no warranty or representation that its software products will work in combination with any hardware or applications software products provided by third parties, that the operation of the software products will be uninterrupted or error free, or that all defects in the software products will be corrected. For any third party products listed in the SysMaster software product documentation or specifications as being compatible, SysMaster will make reasonable efforts to provide compatibility, except where incompatibility is caused by a "bug" or defect in the third party's product or from use of the software product not in accordance with published specifications or user documentation.

### **Obtaining Warranty Service**

Customer must contact SysMaster or an Authorized SysMaster Service Center within the applicable warranty period to obtain warranty service authorization. Dated proof of purchase from SysMaster or its authorized reseller may be required. Products returned to SysMaster's Corporate Service Center must be pre-authorized by SysMaster and sent prepaid and packaged appropriately for safe shipment, and it is recommended that they be insured or sent by a method that provides for tracking of the package. The repaired or replaced item will be shipped to Customer, at SysMaster's expense, not later than thirty (30) days after SysMaster receives the defective product.

### **Dead- or Defective-on-Arrival**

In the event a product completely fails to function or exhibits a defect in materials or workmanship within the first forty-eight (48) hours of installation but no later than 180 days after the date of purchase, and this is verified by SysMaster, it will be considered dead- or defective-on-arrival (DOA) and a replacement shall be provided by advance replacement.

The replacement product will normally be shipped not later than three (3) business days after SysMaster's verification of the DOA product, but may be delayed due to export or import procedures. When an advance replacement is provided and Customer fails to return the original product to SysMaster within fifteen (15) days after shipment of the replacement, Customer is charged for the replacement product at list price. SysMaster shall not be responsible for any software, firmware, information, or memory data of Customer contained in, stored on, or integrated with any products returned to SysMaster for repair, whether under warranty or not.

### **Force Majeure**

SysMaster shall not be liable for failure or delay in performing its obligations hereunder if such failure or delay is due to circumstances beyond its reasonable control, including, without limitation, acts of any government body, war, insurrection, sabotage, embargo, fire, flood, strike or other labor disturbance, interruption of or delay in transportation, unavailability of or interruption or delay in telecommunications or third party services, failure of third party software or inability to obtain raw materials, supplies, or power used in equipment needed for provisions of the service.

### **Governing Law**

The validity, interpretation, enforceability and performance of this Agreement are governed by and construed in accordance with laws in the State of California.

## FCC/CDC Statements

### Federal Communications Commission Statement

This device complies with FCC Rules Part 15. Operation is subject to these conditions:

- This device may not cause harmful interference;
- This device must accept any interference received including interference that can cause undesired operation.

This equipment has been tested and found to comply with limits for a Class B digital device pursuant to Part 15 of the FCC rules. Such limits are designed to provide reasonable protection against harmful interference in a network installation. This equipment generates, uses and may radiate radio frequency energy and - if not installed and used according to instructions here and in related documentation - may cause harmful interference to radio communications.

There is no guarantee that interference will not occur in a given installation. If such interference to radio or television reception should occur (this can be determined by turning the equipment off and on), the user can try to correct interference by:

- Reorienting or relocating the receiving antenna
- Increasing the separation between equipment and receiver
- Connecting the equipment to an outlet on a circuit different from that to which the receiver is connected
- Consulting the dealer or an experienced technician.

### Canadian Department of Communications Statement

This digital apparatus does not exceed Class B limits for radio noise emissions from digital apparatus set out in the Radio Interference Regulations of the Canadian Department of Communications.

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

## SysMaster Technical Support and Services

Product information, Frequently Asked Questions, a Knowledge-base and other support are available through the SysMaster World Wide Web site at <http://www.sysmaster.com>.

SysMaster also offers toll-free 1-877-900-3993 (US only) and 1-510-420-8837 (International) direct phone support during normal business hours.

#### Sales and Ordering Information

For sales information, send an electronic mail message to [sales@sysmaster.com](mailto:sales@sysmaster.com) or call our toll-free number 1-877-900-3993. International customers, please dial 1-510-420-8837.

#### Feedback on this Manual

Your feedback is welcome. If anything in the guide seems unclear, please let us know by sending e-mail to [support@sysmaster.com](mailto:support@sysmaster.com).



# Chapter 1: VoIP Overview

---

## In This Chapter

This chapter includes the following topics, by section:

- A Prologue that presents the benefits of migration to Voice Over IP
- A discussion of VoIP architecture and operation
- A look at critical VoIP devices and their roles
- A survey of the two key VoIP protocols or protocol suites - H.323 and SIP
- A survey of VoIP performance variables
- Finally, a full study of VoiceMaster as a comprehensive VoIP solution, including:
  - VoiceMaster entities
  - VoiceMaster-supported business models
  - VoiceMaster components and (call) operation basics
  - A tutorial that introduces the VoiceMaster Administration Console

## Prologue

The transfer of voice traffic over packet networks, and especially voice over IP, is rapidly gaining acceptance as an alternative to standard voice networks. The use of digital data channels to transport voice traffic is now becoming widespread.

Calling customer migration from traditional switched telephone circuits to Voice Over IP (VoIP) is accelerating. The Telco/PBX world is wire-based and expensive. Maintaining physical circuits is costly, while these networks are vulnerable to natural equipment degradation and connection interruptions. These system stresses are passed on to the customer in the form of frustrating calling experiences and higher costs.

The VoIP solution is largely free of physical drawbacks and limitations. Use of public data lines and minimal or no use of physical circuits (depending on call origination gateway location) combine to boost network reliability. There are few physical maintenance requirements within such networks. Though data lines that carry VoIP calls can become congested, only rarely do they experience breakdowns.

Service may slow during peak usage patterns or if routing configuration is not optimized. Yet, these are problems that lend themselves to resolution through freeing up of available bandwidth or the coherent application of network planning (especially routing). Improvements can be implemented by contracting with additional network service providers or using administrative software tools to improve traffic results.

The reliance on the Internet (the ‘IP’ in VoIP) is an enormous advantage over traditional telephony logistics. The increasingly attractive low-cost, flat-rate pricing of the public Internet drives down prices for suppliers and users alike. This potentially enables large volumes of inexpensive long-distance calls and opens up the VoIP market to consumers who would otherwise shy away from voice-only long-distance services.

Quality of Service issues, while still a concern, no longer weigh on potential customers. Improved technologies to address issues such as call compression and delay put the cost/benefit equation squarely on the side of VoIP over traditional switched-network telephone services.

## VoIP Benefits

VoIP service implementation benefits can be divided into three general categories:

- **Cost Reduction and Availability**—IP has reached a level of availability that includes the desktop. The combination of network technologies, increased bandwidth availability and proliferating network devices (switches, routers, gatekeepers, gateways) reduce costs significantly. Businesses and individuals can access effective, inexpensive services by subscribing to IP-based services. It becomes a question of not ‘if’ but when and how to switch.
- **Simplification and consolidation**—An integrated infrastructure is evolving. The industry is moving towards the consolidation of different protocols and communication methods. This translates into technology standardization and a reduction in total equipment needs (greater *interoperability*). Strategic integration of voice and data functionality will yield useful long-run returns for businesses of different sizes. All of this makes the VoIP realm simpler, more flexible and cheaper to use.
- **Advanced applications**—Basic telephony and facsimile were the initial applications in VoIP, but multimedia and multiservice applications are increasing. The convergence of Internet and voice traffic creates new network design possibilities. Solutions such as voice call button customer access to call center agents are growing. Then add in novel implementations such as interactive shopping, streaming audio, electronic white-boarding and stereo conference calls.

## Technology Challenges

Prospective VoIP customers do have legitimate concerns when considering migration from PSTN. These include possible degradation in voice quality that results when voice is carried over packet networks. VoIP service providers and administrators should consider factors that may impact call quality:

- Compression. Data compression for the IP segment of a VoIP call is an inherent function. It is the means by which analog voice data is converted into digital data and compressed for the major IP call portion (at the IP endpoint, data is decompressed and sent in analog form to the receiving device). Though compression is often highly sophisticated, it can affect voice quality and also cause data transfer delays.
- Delay. Delays may result from data compression/expansion, as well as from intermittent bandwidth congestion. These delays can reduce call efficiency and user comfort, leading to customer dissatisfaction.

- **Echo.** Just as in traditional PSTN networks, voice echo can occur in VoIP calls. Despite the incorporation of anti-echo mechanisms into network functionality, echo may periodically occur in VoIP calls.

---

**Note** Network administrators should obtain tools that measure potential problems and optimize their implementations to avoid them. To learn more of these challenges, see [VoIP Performance Variables](#) later in this chapter.

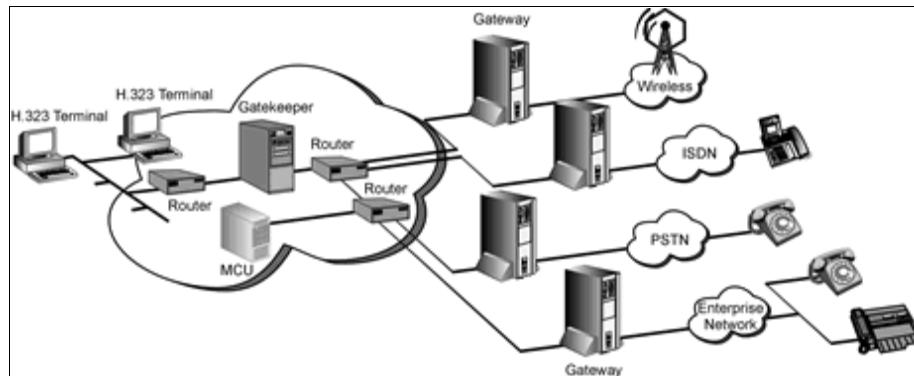
---

## VoIP Architecture and Operation

VoIP services must have access to traditional circuit-switched voice networks so that VoIP calls can be successfully routed. The technology assumes a traffic pattern of voice-data-voice; that is, the first and last call links are always (analog) voice links.

In VoIP technology, a digital signal processor (DSP) typically segments the voice signals into frames and stores them in packets. Packets are typically transported using the internet protocol (IP) that complies with the International Telecommunication Union-Telecommunication Standardization Sector (ITU-T) specification (H.323) for packet-based multimedia (voice, video, and data) networks.

The basic elements of an H.323 network are shown here: H.323 terminals such as PC-based phones on one side connect to existing ISDN, PSTN and wireless devices on the other side:



**Figure 1-1 Sample VoIP Network Configuration (Generic)**

---

**Note** VoIP traffic can be carried using either the H.323 protocol (stack) or the Session Initiation Protocol (SIP). Though H.323 is the first VoIP protocol and remains in wide use, it is increasingly eclipsed by SIP's modular design, which includes greater extensibility. We cover both protocols in greater depth later in this chapter.

---

The general architecture by which VoIP calls are processed is fairly basic. A customer uses a telephone device to initiate a call. If authorized, that call travels over a traditional PSTN network link to a (gateway) origination device, which translates the call data into digital format and compresses it for transmission over the IP network to a terminating device. This IP endpoint then decompresses the digital packets into analog format and sends the data on the final PSTN link to the receiving telephone device.

Let's take a closer look at these call phases and the devices used to enable them:

- *Call origination device to origination gateway.* This is a pure voice (analog) segment. The voice line used can be of any type, including T1 lines with multiple circuits. The gateway receives the voice segment, uses RADIUS to authenticate and authorize the source and the call, then begins to receive and prepare the data for digital transmission over the IP link.
- *Origination gateway to termination gateway.* The gateway sends the translated, compressed data, over public Internet (IP) lines to the termination gateway. The gateway must be linked to an ISP; its physical location is variable, ranging from an ISP Point of Presence to the caller's site (specially if the call originates from a business).
- *Termination gateway to receiving device.* The termination gateway receives the digitized (compressed) signal over the IP network, decompresses it and sends it in analog (voice) format to the destination telephone device.

---

**Note** In this guide we refer to *endpoints* as well as *originating* and *termination devices*. These are the gateways and gatekeepers that 'bookend' the IP call portion also communicate with their respective telephone devices. (A telephone is not an endpoint.) Routing configuration and administration are expanded later in this Guide.

---

## A VoIP (Calling Card) Call, Step by Step

A VoIP call, based on a calling card model, includes the following events:

- Step 1** The caller dials the destination number.
- Step 2** The call attempt reaches the origination gateway. The gateway recognizes that a call has been initiated and begins caller authentication.
- Step 3** The caller hears a Welcome prompt (assuming the gateway includes Interactive Voice Response [IVR] functionality).
- Step 4** The message instructs the caller to enter a Personal Identification Number (PIN). The caller does so.
- Step 5** Authentication. The gateway checks its database (user table) to match the PIN entry with a known user.
- Step 6** If the user's identity is confirmed, a message prompts entry of a destination (country code) if the user has not entered it (for international calls).
- Step 7** The system checks the verified user's account balance and calculates maximum call time.
- Step 8** The IVR informs the user of maximum allowable call time. (The IVR call time announcement may reflect actual time or not, depending on management software capabilities and configuration).
- Step 9** The call is authorized.
- Step 10** Routing occurs. The system gatekeeper accesses stored route tables and calculates a route on the basis of current information and administrator-configured routing policies.
- Step 11** The call is established, using signaling protocols in accord with H.323 or SIP configuration. The gateway compresses the first analog voice stream to digital form and passes it over the Internet data lines to the termination gateway.
- Step 12** The termination gateway decompresses the data stream and translates it into analog form for the last leg to the receiving device.

- Step 13** The call continues, all voice data following the voice-data-voice pathway until the call is completed. The same inherent protocol functionality that established and maintained the call now ‘tears it down.’

---

**Note** Route failover is commonly configured in VoIP. If a primary route fails, the system will automatically shuttle the call onto a backup path for a designated period. Your system must include the Route Failover module for your VoiceMaster to be configured to implement this functionality.

---

### VoIP and the E.164 Numbering Scheme

The standard Public Switched Telephone Network (PSTN) uses a specific numbering scheme to comply with the ITU-T international public telecommunications numbering plan (E.164) recommendations. Every nation is assigned a one-to-three digit country code; specific national dial plans are based on that code. For example, in North America, the North American Numbering Plan (NANP) uses an area code (assigned geographically), an office code (assigned to actual switches) and a station code (identifying switch ports).

VoIP relies on and uses these standards; it does not use a unique, VoIP-specific numbering scheme.

## VoIP Devices and Roles

As you can see, VoIP networks rely on a combination of devices and protocols to enable and configure routes and manage call flow along these routes. In the following sections, we describe these devices and the role they play in making VoIP calls happen.

### Gatekeepers

Gatekeepers are optional but important entities in a VoIP network. A gatekeeper works with multiple providers and destinations to perform intelligent routing. Its capabilities combine with human administrative configuration decisions to select the best route between gateways.

A gatekeeper manages call routing within its assigned zone and shuttles calls to and from neighboring zones. Gatekeepers monitor neighboring zones and forward calls accordingly. Depending on the active routing mode used, a gatekeeper assimilates routing priority data and routes accordingly.

The importance of gatekeepers is related to the proliferation of gateways and endpoints. As devices and possible routes increase, so does the need for intelligent routing and network management. Routing tables and reports, often dynamically updated, provide information about network status, device load and overall traffic flow/congestion.

In many network designs, the presence of a gatekeeper enables a division between intelligent network control and routing functions and processing requirements. Within a system such as VoiceMaster, the gatekeeper selects the best path on the basis of parameters such as endpoint priority or best cost. Calls are typically delivered to origination and termination gateways that handle tasks like data compression that make VoIP traffic function.

Gatekeepers are often platform/software solutions within servers, while gateways are manifested as proprietary hardware platforms. However, gatekeepers can also be purely physical devices, as with Cisco gatekeepers.

Each gatekeeper has responsibility for a finite number of gateways and endpoints within its area or *zone*. Gatekeepers can recognize when new devices seek to join the network, then qualify or disqualify them accordingly. This is called *device registration*. Once these devices join the network, the gatekeeper manages them. This is the reason for the name *gatekeeper*: it is the guardian and regulator of a specific Internet zone and the devices that reside and function within it.

Gateways and endpoints will often register themselves to a zone (self-register). This will depend on a combination of their own configuration and that of the zone's gatekeeper. (It is up to the Administrator who controls the gatekeeper to structure and manage networks to grow coherently.)

---

**Note** If a centralized gatekeeper is present, it will manage a registry of different zones and coordinate LRQ-forwarding.

---

Specific Gatekeeper functions include:

- Address translation
- Admission control
- Bandwidth control
- Zone management

---

**Note** For example, address translation involves mapping between internal and external numbering systems. Admission control specifies permitted call destinations for specific devices.

---

Optional gatekeeper functionality includes:

- Call authorization
- Call management
- Bandwidth management
- Call Control signaling

During call setup procedure, the Gatekeeper acts as a management control station. Customer entry of authorization data and country/area code (destination gateway) triggers a call routing request. The Gatekeeper sets a best path based on standard routing protocols and software configuration settings.

---

**Note** Gatekeeper functionality is usually an inherent part of a VoiceMaster VoIP solution. Combined with software routing and billing functionality, it creates an integrated and powerful VoIP service.

---

### Gatekeeper Zones

Each gatekeeper is responsible for a zone in which gateways and endpoints operate. A zone is a portion of virtual VoIP network geography containing devices that use the gatekeeper's service for VoIP calls. When endpoints outside a gatekeeper zone want to communicate with endpoints *within* the zone, they effectively request permission from the gatekeeper to establish endpoint-to-endpoint contact.

---

**Note** Voicemaster defines its own gatekeeper zone. Gateways and gatekeepers registered to it can be used in configuring routes for calls. The association of destination area codes with termination devices enables the creation and assignment of routes.

---

In a real-world VoIP network scenario, gatekeepers make note of neighboring gatekeepers and their gateways. Each gatekeeper incorporates information about adjacent zones into the routing tables.

For instance:

Gatekeeper1 has a collection of 30 gateways that terminate area codes 1, 2, 3

Gatekeeper2 has a collection of 10 gateways that terminate area codes 6, 7, 8

The routing table of Gatekeeper3 will be:

- 1 GK1
- 2 GK1
- 3 GK1
- 6 GK2
- 7 GK2
- 8 GK2

All area codes associated with neighboring gateways are stored in the routing table.

---

**Note** For more on Gatekeeper zones, refer to Cisco documentation on the subject. An example is:

<http://www.cisco.com/warp/public/788/voip/understand-gatekeepers.html>.

---

## Gatekeeper Signaling

Typically, however, the a VoIP network with an active gatekeeper implies the presence of a routed call signalling model. All call signalling passes through the gatekeeper, while the media (call data) is transferred directly back and forth between endpoints. This is known as *routed mode* in the context of VoiceMaster operations.

---

**Note** VoIP call signaling protocols and uses are discussed a bit later in this chapter.

---

An alternate, direct signaling model can trigger the exchange of messages without a gatekeeper. All signals and call data are routed directly between end points through associated gateways. If a gatekeeper is present, it is simply bypassed.

## Gatekeeper Working Modes

Gatekeepers can function in different modes. One such mode (routed) was just discussed. Static mode is one in which routes are preset and routing tables are not updated dynamically. In this mode, a gatekeeper lacks any ability to configure routes. Routed mode gives the gatekeeper control over call signaling. Proxy mode is one in which the gatekeeper controls both call signaling and media transport.

## Gateways

VoIP gateways bridge different types of networks. There are many types of gateways in existence today, ranging from support of a dozen or so analog ports to high-end gateways with simultaneous support for thousands of lines.

Typically, a gateway in a VoIP setting connects the IP data network with the PSTN voice link. On one side, it interacts with its associated endpoints (telephone devices) through standard analog communication. On the VoIP side, it communicates with IP-fluent devices (gatekeepers, gateways), sending and receiving digital data.

The gateway must be able to do more than compress and decompress data. It also must handle associated signaling for establishing, maintaining and breaking down active calls.

---

**Note** Depending on the network configuration, a gateway may originate and terminate VoIP calls for many telephone devices.

---

Possible gateway *bridging* modes include:

- PSTN-IP (just described)
- PSTN-PSTN
- IP-IP

Gateways carry out additional essential functions:

- Authenticate calls using in-built RADIUS functionality
- Provide an IVR (Interactive Voice Response) platform by which a VoIP service informs prospective callers of account and call status
- Record call data and passing it on to the managing gatekeeper for processing and administration. This is an ‘agent’ role.

## H.323 Terminals

H.323 terminals are LAN-based end points for voice transmission that support the H.323 signaling functions. These protocols provide mechanisms for call setup, transmission and call dissolution. H.323 terminals implement voice transmission functions and include at least one voice CODEC that compresses and decompresses packetized voice.

---

**Note** The definition of all the H.323 network entities is purely logical. No specification has been made on the physical division of the units, which can be configured in different ways.

---

Specific Session Initiation Protocol (SIP) entities also exist:

- SIP Registrar
- SIP Proxy
- SIP Gateway

SIP-based VoIP will soon be elaborated in its own section.

# H.323 Protocol Architecture

H.323 is a protocol suite that has been a standard for communications over IP-based networks. Advantages include the powerful combined functionality deriving from the integration of its individual components.

H.323 specifies techniques for compressing and transmitting real-time voice, video, and data between a pair of video conferencing workstations. It includes signaling protocols for managing audio and video streams.

The H.323 suite also includes specific guidelines for breaking data into packets and synchronizing transmissions across communications channels. It uses the RTP protocol to carry the actual media and RTCP for status and control information.

## Signaling Protocols

Signalling is transported reliably over TCP using the signaling protocols:

- **RAS (Registration, Admission, Status).** RAS enables connection between terminals and gateways and a gatekeeper. It is the first signal channel opened and remains independent of call setup and media transport channels. RAS uses UDP ports 1719 and 1718, respectively, for H.225 messages and gatekeeper discovery.

Registration refers to the process by which gateways and terminals join a zone and transmit IP and alias addresses to the gatekeeper. Registration occurs after discovery.

Gateways search for the responsible Gatekeeper one of two ways:

- **Unicast discovery.** Using port 1718, endpoints are configured with the gatekeeper IP address and attempt registration. If the zone gatekeeper responds with a confirmation message, the gateway is added to the zone registry.
- **Multicast discovery.** The gateway uses a special multicast address and to broadcast to all gatekeepers. The appropriate gatekeeper replies with a confirmation message or remains silent to bar the endpoint's addition to the zone.

---

**Note** A gateway that does not find a gatekeeper can make periodic discovery attempts. There is no limitation in the number.

---

Additional RAS messaging includes:

- *Admission messages* that enable call admissions and bandwidth control. A gatekeeper accepts or denies endpoint network access requests. Message types are requests (ARQ), confirmations (ACF) and rejections (ARJ).
- *RAS Endpoint Location.* Gatekeepers communicate with each other to locate IP addresses for various zone endpoints.
- *RAS Status Information.* A gatekeeper obtains online/offline endpoint status information.
- *RAS Bandwidth Control.* This specialized message type is sent to request an increase or reduction in utilized bandwidth during a call.
- **Call Control Signaling.** H.225 sets up connections between H.323 endpoints using Q.931 signaling messages. Port 1720 is reserved for call control messages that connect, maintain and disconnect calls.

- **Media Control and Transport (H.245)** used to exchange capabilities such as compression standards between H.323 entities. H.245 establishes logical channels for multi-media transmissions.

### CODECS

Also included in the H323 protocol stack are the audio/video Codecs:

- audio codecs (G.711, G.723.1, G.729)
- video codecs (H.261, H.263)

Codecs are standards for the compression and decompression of data/media streams. Codecs differ in CPU and bandwidth requirements, in voice quality and processing delay. We address codes in depth in VoIP Performance Variables.

## Session Initiation Protocol (SIP)

The Session Initiation Protocol is an Internet Engineering Task Force (IETF) standard protocol for establishing, maintaining and ‘tearing down’ an interactive user session. Such sessions may include multimedia elements such as audio, video and instant messaging, or other real-time data communications. SIP is an emerging alternative to the H.323 protocol set and is increasingly used in VoIP implementations.

As an application-layer protocol, SIP will work with many other protocols. It requires only datagram service and is independent of the packet layer. SIP cooperates with other call setup and signaling protocols. It can detect address and protocol information from protocol-independent source addresses.

Though it normally runs over UDP or TCP, SIP can ‘sit’ over other protocols such as IP, ATM, or X.25. It also provides out-of-band call setup services in which SIP exchanges take place over UDP or TCP, but actual data transmission takes place over the public telephone network.

---

**Note** The ability to decipher protocols used by participating endpoints is a great benefit. If it sees an endpoint expects H.323, SIP is able to call upon H.323 sub-protocols - H.245 and H.225.0 - to establish the call.

---

SIP session invitations contain session descriptions that facilitate participant agreement on compatible media types. Session members communicate using multicast or a mesh of unicast relations, or a combination of both. SIP can also initiate multi-party calls using a fully-meshed interconnection. It also supports call forwarding.

SIP is based on HTTP architectural design. SIP addresses are URLs and therefore can be integrated into far-reaching Web applications and implementations.

One of the key SIP advantages lies in support of user mobility. It can accept proxy and redirect requests from any current location by using name mapping to identify and authorize a known user. By relating to the unique identity and not the machine location, it supports mobile-dependant subscriber services.

In all, SIP supports five mechanisms for establishing and terminating multimedia communications:

- User location: SIP supports address resolution, name mapping, and call redirection.
- User capabilities: SIP determines the lowest level of common services between the end points. Conferences are established using only the media capabilities that can be supported by all end points.

- User availability: If the target end point is unavailable, SIP determines whether the called party is on the phone or did not answer in the allotted number of rings. It then returns a message that includes the cause of unavailability.
- Call setup: If the call can be completed, SIP establishes a session between the end points. SIP also supports mid-call changes, such as the addition of another end point to the conference or the changing of a media characteristic or CODEC.
- Call handling: SIP supports the transfer of calls from one end point to another. SIP simply establishes a session between the transferee and a new end point and terminates the current session. At the end of a call, SIP terminates sessions between all parties.

A comparison between SIP and H.323 is shown below, illustrating the advantages and disadvantages of the two systems:

**Table 1-1 SIP/H.323 Comparison**

H.323	SIP
Robust but consumes more call set up time	Simple, scalable and extensible
Requires about twelve packets for call-setup	Requires about four packets for call-setup
Provides floor control within a session	Cannot provide
Has more elaborate capability exchange (H.245)	Minimal capability exchange, enough for IP telephony
Provides a multipoint controller for conferences	Multipoint controller not needed for SIP multicast conferences
Requires both TCP and UDP during the call-setup	Runs on UDP, achieves reliability through retransmissions. Employs TCP when UDP is not supported.
Implementation is relatively complex	Easy to implement

## SIP Architecture

SIP architecture is based around two essential components:

- SIP User Agent (UA) - the endpoint component, which can be a hardware or software device implementing SIP (e.g., an IP phone), and consists of two main components:
  - A User Agent Client (UAC) that initiates calls
  - User Agent Server (UAS) that answers calls
- SIP Network Server - handles signaling associated with multiple calls. It provides name resolution and user location.

In reality, three separate servers combine functions:

- A SIP Register Server receives registration messages from endpoints regarding current user location and maps SIP addresses to the endpoint's physical location(s). Mapped data is stored in a database that can reside on the same machine or on a remote server.
- An IP Proxy Server forwards SIP messages to multiple proxy servers. It builds a search tree, that guides SIP messages to their destinations. Proxy servers have two distinct operating modes:

Stateless - the server forgets all data once the request is sent

Stateful - the server exploits stored routing information to improve route efficiency and message transmission

- A SIP Redirect Server redirects endpoints to alternate servers to locate desired addresses. If a call is to be routed through a number of different Proxy servers, the Redirect server is used:
  - A caller sends an INVITE request to the redirect server
  - The redirect server contacts the location server to determine a path to the called party
  - It then sends the path information to the caller
  - The caller acknowledges receipt of the information
  - The caller sends a request to the destination specified - whether the receiving telephone device or a server designated to forward the request
  - The request reaches the called station, which acknowledges its reception.

---

**Note** RTP is the protocol used for communication between the callers.

---

SIP messages can be request messages or response messages and can be transmitted either over TCP or UDP. The message/signaling contents include:

- The protocol format, consisting of a start line, message header, an empty line and an optional message body
- The Request packet header format
- The method to be performed on the resource. (INVITE, ACK, etc.)
- A SIP URL or a general Uniform Resource Identifier (the user or service to which the request is addressed)
- The SIP version being used
- The format of the Response message header, and the relevant response codes
- Status-code: a three-digit integer result code of the attempt to understand and satisfy the request
- Reason-phrase. A text description of the status code.

## SIP Applications

SIP addresses major issues in the development of Internet telephony, and enables an impressive range of power applications:

- **Unified Communications.** A SIP session can contain any combination of media (voice, data, video, etc.). These sessions can be modified at any time by adding new parties or by changing the nature of the session. SIP enables the augmentation of multimedia capabilities to browsers. User profiles can be managed through a web interface and voice plug-ins are incorporated into browser technology

---

**Note** SIP uses MIME, the *de facto* standard for describing content on the Internet, to convey session protocol information. It uses the Domain Name System (DNS) to deliver requests to a server that can handle them.

---

- **Unified Messaging.** E-mail, voice-mail, faxes, and phone messages are accessible from one system. Yet, the support of user mobility means that people can use multiple communication devices for the same purposes.
- **Directory Services.** Directory services are to a network what white pages are to the telephone system. People can use the SIP-based service to look up objects by name or service type. Network managers use directories to manage user accounts and network resources. It is a network device inventory that is opened using a graphic interface or by name and properties searches.
- **IP-PBX functionality** - Software based IP-PBX that is compliant with the SIP standard can be utilized in a single office setting or multiple office locations, offering flexibility and options for future expansion.
- **Voice-enhanced e-commerce** - A website contains click-to-dial links that establish a session between the end-user and the website owners.
- **Web Call Centers** - A web page may be opened when a particular number is called (with SIP, it is just as easy to direct an user to a web page as it is to a telephone). SIP supports IVR (Interactive Voice Response) features, navigating users through options and providing auto-responses to common requests. SIP offers a forking facility perfect for fulfilling the ACD (Automated Call Distribution) functionality.
- **Instant Messaging (IM) and Presence.** SIP's ability to underpin any form of communication, lets it run an IM session to a telephone call or a whiteboard or video session at the click of a button. It is also easy to monitor the status of multiple invitees to a call, then connect available parties to a conference bridge. This creates near-spontaneous conference calls.
- **Mobile phones and PDAs** - Because SIP client software is lightweight, it can be embedded in mobile phones and PDAs. These services can cross all platforms, since SIP is able to negotiate different media (transmission) facilities. PDAs and related devices becomes means of accessing services, breaking from their proprietary-systems roles.
- **Wireless LAN VoIP Telephone Handsets** - Dedicated, VoIP supporting portable telephone handsets on a wireless LAN connection can use SIP and other proprietary protocols.
- **Desktop Call Management** - SIP enables a convergence at the desktop. Voice services can be assimilated into other applications. Using SIP features such as user profiling, presence management and instant messaging, third party call control and integration with media, service providers can create multiple services. And all the advanced telephony services are supported by SIP, including call forwarding, call hold and call waiting.

## VoIP Performance Variables

The limitations of analog transmission helped push the telephony industry to migrate to digital transmission using pulse code modulation (PCM) or the derivative PCM (ADPCM). Either technology converts analog into digital form by sampling the analog sound 8000 times per second and converting each sample to a numeric code.

The use of digital transmissions and signals, though a powerful antidote to analog communication limitations, has its own challenges. Digital signals solve the problem of degradation of analog voice over distance through amplification, which creates ambient line noise. This becomes a consideration for subscribers and therefore for VoIP service providers as well.

By definition, the translation of analog to digital compresses data. The smaller the digital data component, the faster the packets are likely to travel along the IP portion. The greater the compression, the greater the resultant voice distortion.

At both IP endpoint devices (gateways) compression/decompression functionality is implemented through Codecs that can also vary by type and inherent efficiency.

Another factor in network performance is the processing load on the gateway (or gatekeeper) itself. Powerful compression protocols will tax the device's processor, adding a factor to call time variables. Lighter Codecs ease the processing burden but may add time on the IP call portion due to larger packet size.

Among the specific performance variables that impact VoIP performance are:

- Compression (CODEC)
- Delay
- Echo

## CODECs

Over the years, improved (CODEC) compression techniques have reduced required bandwidth while preserving voice quality. Most H.323 devices used in VoIP networks employ CODECs standardized by the ITU-T to facilitate interoperability (cross-vendor functionality).

PCM and ADPCM are examples of *waveform* CODECs that compress data using waveform redundancy.

*Source* CODECs compress speech by sending simplified parametric information about voice transmission. These require less bandwidth and use predictive coding and multipulse technologies.

Different compression schemes can be compared based on these parameters:

- **Compressed Voice Rate.** Codecs compresses voice from 64 Kbps to a specified bit rate for data transport. Each Codec compresses data to different, multiple target rates such as 8, 6.4 and even 5.3 Kbps (audio rates). However, some can handle more intense compression 'translations' than others, a factor in network designs where reducing bit rates is a priority.

---

**Note** When transmitting packetized voice over the network, protocol overhead (RTP/UDP/IP/Ethernet) is added to this audio bit rate, resulting in a higher actual data rate.

---

- **Complexity.** The more complex the Codec implementation requirements, the more CPU resources are required. The best quality of sound and speed is a compromise - best sound quality slows transmission, while the fastest packet rates correspond to lowered voice quality.
- **Voice quality.** Some Codecs are inherently better at compressing voice to data and preserving sound quality than others.
- **Digitizing delay.** Each CODEC uses an algorithm that specifies different quantities of voice data for buffering. It can compress a certain block of data at a time, while the remainder is buffered, or queued. This adds to the overall end-to-end delay (next section).

---

**Note** Networks with excessive end-to-end delay can lead to chopped, half-duplex conversations in which callers pause in order to mitigate the effects of delay.

---

The choice of compression scheme depends on which scheme better fits a specific VoIP installation and network needs. G.723 and G.729 are two of the most widely used compression protocols.

## Delay

One of the most important VoIP design considerations is minimizing one-way, end-to-end delay. Long packet delivery delays may cause nonsensical speech and force callers to improvise unwanted pauses. (An acceptable delay is less than 200 milliseconds.)

Two kinds of delays exist:

- Propagation delay caused by the characteristics of the speed of light traveling via a fiber-optic-based or copper-based medium;
- Handling delay (*serialization delay*) by devices that handle voice information. These can significantly impact voice quality.

A good network administrator accounts for end-to-end signal paths/data paths, Codec performance characteristics, and packet payload size when estimating:

- Delays from endpoints to CODEC processing (queuing)
- Encoding delay on compression/decompression
- Packet delay
- Fixed network portion delay

The aggregate of these factors forms the potential end-to-end delay. Reducing their combined effect results in a VoIP service network where the advantages of digital transmission are maximized.

## Echo

Echo is the phenomenon of hearing your own voice in the telephone receiver while you are talking. It is a signal bouncing off the receiving endpoint. Properly timed and contained echo does not distract the caller. It may even provide functional feedback or confirmation.

Echo cancellers are often built into the low bit-rate codecs and operate on each digital signal processor. They work by generating an *antisignal* that cancels the echo. Echo cancellers are intentionally limited by the time - *echo trail* - they wait for reflected speech to be received. This is normally 32 milliseconds but can be set to 8, 16, or 24 milliseconds. (A time over 24 milliseconds can be audibly distracting.)

This technology is also used to overcome speakerphone feedback and even in environmental scenarios where digitally produced ‘anti-noise’ may be applied.

(Packet loss and jitter are additional issues for VoIP service. These will be addressed in more detail in the final version of this Guide.)

## Fraud Prevention

Fraud is an important issue in VoIP communications. Defrauding of VoIP service providers and customers alike adds up to a multibillion dollar business. Just five years ago, estimates of direct damages resulting from fraud ranged from \$30 to \$40 billion or more, an annual loss of between 3 and 8% to an average VoIP service provider.

Next generation networks (NGNs) like those that VoIP services employ and depend upon prove to be fertile ground for sophisticated criminals. Unauthorized users employ improvised, clever methods (often with the assistance of hackers) to steal information, invade accounts, and damage networks and their resources. At the same time, ‘entrepreneurs’ working on their own cause damage if their hacking skills are adequate. Modern communication techniques like Internet Relay Chat (IRC) let purveyors of mischief transmit illicit insights rapidly, almost instantly.

All of this can create network downtime and service malfunction, and heightens the importance of security and fraud detection functional implementations in VoIP service networks. (Such security measures are an integral part of a typical VoiceMaster-centered VoIP service.)

Traditionally, network administrators dealt with network intrusions via access-control devices such as firewalls and radius and authentication servers. A firewall provides preliminary filtering of unauthorized traffic to specific resources or network segments. Authentication and authorization mechanisms (AAA servers, radius) restrict access to the network and its resources, enabling usage only when provided with a legal user identification and password. They must respond to efforts to alter IP addresses and abuse user accounts in a timely way, before imaginative unauthorized users move on to more fertile territory.

VoiceMaster provides extensive security and fraud protection options, implemented in different modules available to all customers. In the next major section, we present VoiceMaster as a comprehensive VoIP solution.

## VoiceMaster: A Comprehensive VoIP Solution

The SysMaster VoiceMaster is a modular system that facilitates operation and management of a VoIP service. When combined with a VoIP gateway, VoiceMaster creates a robust and integrated VoIP solution. In a typical customer configuration, VoiceMaster contains gatekeeper, routing and billing functionality. It is this suite of tools that enables network planning and configuration, as well as event monitoring and system administration (most or all of this in *real time*).

Gatekeeper functionality is at the heart of VoiceMaster's routing intelligence. This is complemented by software modules that facilitate dynamic routing configuration, and additional modules for configuring fluid, flexible and comprehensive billing solutions. A SysMaster customer's VoiceMaster is the core of his VoIP operations, a nerve center that can respond to system events with adaptive policy administration.

The VoiceMaster Administration Console is the administrator's tool for creating, monitoring and managing an effective VoIP service. This user interface incorporates and displays all implemented modules in a given VoiceMaster and lets the Administrator remotely configure and maintain his network.

---

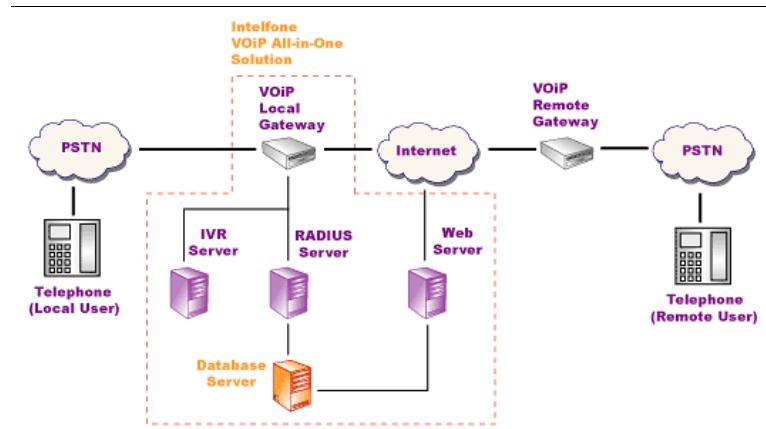
**Note** See [Using the Administration Console](#) later in this chapter for more on this critical configuration and management tool.

---

On the practical level, VoiceMaster offers a comprehensive solution for services based on pre-paid, post-paid or wholesale calling cards. It supports phone-to-phone, PC-to-phone and PC-to-PC voice calls. Containing a set of CRM site management options, including special templates, it facilitates web-based customer registration for VoIP service in an "e-tailing" (retail) business model.

VoiceMaster implementation options also include special scenarios such as Managed Services and ISP Billing. (The use of VoiceMaster for ISP services illustrates that system architecture and functionality is versatile and extends beyond the VoIP world.)

This illustration provides a graphical view of a VoIP network operated and enabled by a VoiceMaster:



**Figure 1-2 VoIP Design**

The following sections describe the VoiceMaster concept, architecture, functions and practical applications.

## VoiceMaster Entities

In a VoIP network or system, a range of different entities participate. Each entity has its own role to play in the system, and VoiceMaster (and Administrator) ‘relates’ to each through the Administration Console. In fact, the Console is designed to allow the configuration and management of these entities. The roles they play, and their relationships to one another, are at the core of the VoIP service itself.

---

**Note** The extent of an Administrator’s capabilities depends as well on the presence of VoiceMaster add-on software modules. In any VoiceMaster implementation, an Administrator’s range of actions is related to the robustness of the specific VoiceMaster configuration. Every customer (VoIP service provider) will have consulted with SysMaster sales personnel before purchase and installation. System capabilities can be upgraded at any time.

---

This is a list of the different entities that exist within the system:

- **VoIP Service Provider.\*** The VoIP Service Provider is the VoiceMaster purchaser who sets up, configures and manages a VoIP service. Where other entities may be either purely *managed* or may both manage and be managed (a client in a Managed Services implementation, for instance), the VoIP Service Provider is the overarching managing entity. The person carrying out the management functions is the Administrator who uses the Administration Console to accomplish this. This Administrator, whether the owner of the business or someone else, is the principal audience for this User Guide.

\*The asterisk is here to point out that the Service Provider is a unique entity that acts on the remaining entities.

- **Network Provider.** This is the entity that provides essential infrastructure - bandwidth and termination devices - to the VoIP Service Provider. The latter contracts with network providers to obtain rights to use IP bandwidth for the major, Internet portion of VoIP calls. In addition, the network provider provides access to termination devices (gateways and/or gatekeepers) that receive packetized voice data (originating from the VoIP Service Provider’s customers). It is these termination devices (‘endpoints’) that decompress the digital data, translate it to analog and send it to the receiving telephone device.

The relationship between the VoiceMaster owner and his providers is a symbiotic one. The provider's bandwidth and network devices are required to enable call service to desired destinations, while the needs of VoIP services create business for the network provider. The VoiceMaster Administrator incorporates the various network provider data (and billing rates) into his call network. The provider devices play a critical role in routing configuration, while the provider rates are at the core of the VoIP service's billing management. They become an expense that is the starting point for calculating billing rates charged to customers. Provider rates are the effective basis for the calculation of business costs, revenues and profits.

- **Resellers.** These are VoIP service dealers/retailers who use preset negotiated rates for charging their own users or subscribers. Resellers are effectively agents for the VoIP service business. The VoiceMaster owner provides infrastructure and, potentially, administrative support to resellers. The resellers benefit from and use this infrastructure, including provider bandwidth and termination devices. One expression of the VoIP service provider-reseller relationship is in the Managed Services implementation. More on this is available in [Chapter Ten: Special Implementations](#).
- **Corporate Clients.** Similar to Resellers, Corporate Clients are treated as single account-users, a sort of super-customer that includes (hidden) individual users. In other words, the VoIP service provider, using VoiceMaster, registers a corporation under one account, and this client then distributes VoIP access to employees. VoiceMaster relates only to the single (corporate) client, which is responsible for managing access to the VoIP service. Corporate clients are likely to assign their own 'administrators' to regulate VoIP use. The VoiceMaster will only relate to a single client and his account.
- **Wholesale Clients.** Wholesale clients can be telephone or other telecommunication companies employing VoiceMaster as a functional backbone. While resellers are tied to the VoIP service billing rates, wholesalers have this additional management capability - and responsibility. Wholesalers also manage their own gatekeeper and/or gateways.
- **Customers.** A customer is anyone who uses the VoIP service provider's infrastructure and billing system, that is, any calling customer who has established an account, directly or indirectly. Customers can be of these types:
  - **Direct - Active Users.** These are customers who contract directly with the VoIP service and are authorized for calls based on rates that you configure. Their calls are routed according to routing policies set by the VoiceMaster Administrator, who can set different rules for different customer groups or for individual customers.
  - **Customers belonging to a Reseller.** These are customers that use VoIP infrastructure and services but are charged by rates set for the respective reseller to which the customers are linked;
  - **Customers belonging to a Corporate Client.** These are customers that use VoIP services but are charged as a block at rates set by their associated corporate client.
  - **Customers Tied to Wholesalers.** (See Wholesale Clients definition above.)

## VoIP/Voicemaster Business Models

Different kinds of businesses models can be constructed and operated using a VoiceMaster. A VoiceMaster is not a static entity tied to a predefined way of establishing and running VoIP service. Rather, it is an infrastructure 'template' that permits the creation of different business models and their related implementations.

Before purchasing a VoiceMaster, a customer will consult with SysMaster sales and technical personnel to best identify his purpose in using VoiceMaster as a VoIP service infrastructure and administration facilitator. Customers have different needs and goals, inevitably. The inherent power and flexibility of VoiceMaster facilitates these different uses, each of which will correspond to a business model.

---

**Note** Individual VoiceMaster customers, though guided by particular model, may also create unique implementations that reflect their particular situations. Nonetheless, the business models we discuss here are valid starting points. Every VoIP service will either follow a model closely or be variant of one model or the other.

---

## Calling Card Provider

The calling card business model uses physical calling cards and access to a large market of potential local subscribers. Such potential VoIP service (calling card) customers are a natural and eager market for potential VoIP service providers with a natural connection to the subscriber base.

These prospective VoIP service providers require a physical infrastructure, including trunk lines so their customers can connect to an origination gateway (also required). They use a VoiceMaster to configure and manage the service, and contract with network service providers for essential access to IP bandwidth and termination devices. Frequently, such businesses use 800 numbers as well.

A business using this model usually requires an independent Administrator to run the VoiceMaster. Additionally, he must create and distribute physical calling cards with specified balances (and PIN numbers) to his customers. This information is used by the origination device to validate caller identities and authorize a call.

Thus an entire VoIP call infrastructure is in place, managed through the VoiceMaster:

- An expansive physical infrastructure includes the customer calling devices, origination gateway, the VoiceMaster with its contained gatekeeper, routing and billing functionality, and Internet bandwidth and termination devices.

---

**Note** Typically, such a VoIP service requires access to a physical location where the VoiceMaster and gateway(s) are installed and operated. This may mean leasing rack space from a Telco or other supplier of network infrastructure.

---

- The management capabilities of the VoiceMaster, split into routing and billing configuration and administration, and run by an Administrator.
- The various entities:
  - The VoIP Service Provider, in this case the merchant who sets up the calling card service.
  - Network providers, supplying IP bandwidth and termination devices.
  - Customers who use the VoIP service infrastructure (VoiceMaster, trunk lines, gateways, provider bandwidth and devices) to make calls.
- Merchant/billing processing is also required. The VoIP service must have a merchant account to physically accept the customer's credit card payment. Authorize.net passes customer credit card information to the various credit card companies to authorize customer payment.

### E-Commerce Variation (Retail)

Here the same basic (calling card) model exists, but with a twist. Interaction with the customer is handled not through physical sale of a tangible calling card in a store, but remotely through a CRM site. The Internet becomes the means of contact and the customer subscription and account maintenance gateway.

The basic infrastructure requirements and participating entities are the same. The VoIP administrator sets up a website on behalf of the VoIP service business. Prospective customers are directed to a URL by advertising. The would-be customer must have computer and Internet access. He navigates to the VoIP service website, built by the Administrator, surveys the service offerings, and registers as a subscriber.

Following registration, the subscriber/user can track his account through the interface, refill account balances, change preferences and so on.

To establish this business model, the E-Commerce VoIP service provider requires, in addition the gatekeeper/billing functionality:

- A payment gateway, such as authorize.net, that passes customer credit card information to the appropriate credit card company
- A merchant account that accepts the customer payments on behalf of the VoIP service.

The Administration Console has a full range of functionality to allow configuration and management of the CRM sites that enable customer-service interaction. This functionality is described in [Chapter Four: VoiceMaster Administration](#).

The E-Commerce model is a potentially lucrative and easily administered form of VoIP service. It caters to the proliferation of computers and today's easy state of Internet access, while preserving the essence of the Calling Card business model.

### Wholesaler

This next model refers to a largely independent VoIP service provider that implements the VoiceMaster as a management/billing application for an independently established network and customer base. The wholesaler uses his own network infrastructure to carry traffic, and uses the VoiceMaster billing modules to configure rates and bill groups of customers for VoIP service.

---

**Note** A typical VoiceMaster-based wholesaler is a Telco that is either entering the VoIP service world for the first time or looking to improve his existing VoIP infrastructure and administrative capabilities.

---

### Managed Services

In this model, an agent uses VoiceMaster to provide VoIP administrative services to subscribers. This agent is typically either a reseller or wholesaler, and is essentially leasing the network infrastructure for his purposes.

Effectively, two administrative layers exist in a managed services solution. The VoiceMaster owner effectively assigns the agent finite permissions used for essential administrative functions. The agent (reseller/wholesaler) partially manages his subscribers, but 'sees' only revenue collected from his subscribers and expenses owed to the 'global Administrator' (the actual VoiceMaster system owner). The VoiceMaster owner is responsible for the rest.

The system owner defines expenses to be charged the agent, using a ‘dummy provider’ billing template, or base. He sees the whole rate structure in operation - agent costs and revenues and overall system costs and revenues.

---

**Note** Each prospective VoIP service provider should create and analyze a business plan, then adapt VoiceMaster use to best execute that plan. It is always possible to adapt and evolve business models, and then purchase additional modules to implement such changes.

---

## VoiceMaster Components

The VoiceMaster combines hardware and software modules to create a flexible, extensible VoIP solution. Individual customer configurations will vary based on need, budget, targeted customer base and so on. The component descriptions here reflect a basic configuration.

The vast majority of VoiceMaster customers (VoIP service providers) utilize a combination of gatekeeper, routing and billing functionality. Certain customers may employ only a portion of this functionality package while many others will implement additional modules.

---

**Note** SysMaster uses the term *modules* in different ways. The core functionality just described includes modules. Custom Routes is needed to create routes other than the system route. Other add-on modules accomplish specific purposes. An example is Fraud Detection. Besides these add-on module there are Custom Modules, many of them tailored to billing management.

---

Key VoiceMaster components are described in the following sections.

### Hardware

All software modules are integrated into various VoiceMaster hardware configurations. At least five levels currently exist. The customer (VoIP Service Provider) selects the desired configuration during the pre-sales process.

The chosen configuration is then installed in one of two Framework Enclosures. One is a horizontal profile 2U Framework Enclosure that accepts a Level 1 VoiceMaster system. The second is a larger 6U enclosure that houses any of the various VoiceMaster hardware.

See [Chapter Two: VoiceMaster Installation](#), for more on these hardware configurations, and for installation instructions.

### IVR Server

The VoiceMaster includes a full-scale TFTP IVR (Interactive Voice Response) server that provides storage for audio playback files required for all pre-paid and post-paid calling card applications. Like the RADIUS component, IVR is a turnkey solution. No modifications are needed to make it function.

What does IVR really do? An IVR server is really a TFTP (Trivial FTP) server. Trivial FTP is FTP that lacks authentication functionality. (A gateway must have RADIUS for authentication, and RADIUS helps to trigger IVR messages.)

### RADIUS Server/AAA

The RADIUS (Remote Authentication Dial-In User Service) protocol is an industry standard widely used by billing and other management applications to control network access. This process is often referred to as authentication, authorization and accounting (AAA).

RADIUS is typically implemented through a server that responds to standardized message formats for transmitting and receiving keypad input, account data, authorization codes and other information between access gateways and billing servers. Each time RADIUS is invoked, it carries out the AAA functions.

- **Authentication.** The user enters this information and RADIUS authenticates (or denies) his identity. Typically, once authentication is performed, an IVR message informs the caller of account balance status.
- **Authorization** of destination phone number. RADIUS confirms the destination number and IVR is invoked to supply remaining calling time to the user.
- **Accounting.** Once the call begins, RADIUS functionality triggers real time call record monitoring. This is immediately reported to the management station (VoiceMaster Administration Console) as both total calling time and as specific call aspects (configurable parameters).

## Database

The Sybase 11.0.3 database server provides robust industrial database storage and support for multiple concurrent connections with complete database backup and recovery functionality. A comprehensive VoIP schema is developed that supports call network functionality. Updates to the database are dynamic. Administrator actions taken through the VoiceMaster Administration Console are reflected almost immediately in the relevant database tables.

The operating system on which the entire system runs is Linux-based. All RADIUS calls are executed on a database level to provide current account balance and user authentication information. It stores call history and call audit information as well as user profile and credit card information.

---

**Note** The number of concurrent phone calls supported depends both on hardware capabilities and VoiceMaster configuration level.

---

## Gateways

SysMaster offers a separate gateway. In addition, VoiceMaster supports a wide range of H.323 and SIP-compliant gateways from companies like Cisco, Lucent, Quintum, etc.

---

**Note** A complete VoiceMaster-based VoIP solution assumes the presence of a working gateway to handle the PBX portion of VoIP calls. A VoiceMaster that includes gatekeeper functionality will also ‘relate to’ multiple gateways throughout the call network. Route configuration must take into account various provider gateways, also referred to as *termination gateways*.

---

## Dynamic Gatekeeper

The VoiceMaster gatekeeper offers functionality that manages calls dynamically and in real time. For VoiceMaster configurations that include gatekeeper functionality, dynamic call management is enabled. Gatekeeper operates in a (dynamic) routing mode to provide real-time call control and call termination services. Routes are built that reflect changing network factors from architecture to traffic patterns.

The Gatekeeper is functionally and fully integrated into the VoiceMaster platform to provide call management for services such as least cost routing and dynamic gateway call distribution. Using the Administration Console, the VoIP service administrator can track route usage, identify gateway burdens, and shift traffic to reflect such patterns.

This features list provides an idea of VoiceMaster's gateway capabilities:

- **Optimized Routing.** VoiceMaster enables dynamic selection of a least expensive termination provider/route for subscriber calls. Based on an algorithm that works from user-defined parameters to select the most cost efficient termination point or provider.
- **Wholesale and Network Billing Support** VoiceMaster offers dynamic call management for real-time call termination in case of balance depletion. Concurrent billing of concurrent interdependent sessions is provided. PC VoIP clients authenticated and authorized for billing in real-time. Custom modules available to set billing rates by custom monthly plans, time intervals, apply custom taxes, etc. SMS and SMS callback billing support, universal H323 gateway billing.
- **Centralized Call Management.** Real-time call control and termination integrated into VoiceMaster. Call handling, dynamic gateway call distribution, and preferred vendor call routing. Single point-of-entry into the VoIP infrastructure for wholesale resellers and providers; PC-to-gateway and gateway-to-gateway Support.
- **Flexible Call Authentication Procedure.** VoiceMaster is the only gatekeeper solution that allows PIN prefix, account name, and ANI authentication.

## Gatekeeper Working Modes

The Voicemaster can function in one of several available (configurable) working modes when implementing its gatekeeper role. The active working mode determines how it treats H.323 voice data and call control flow (signaling that establishes and terminates VoIP connections).

---

**Note** VoiceMaster's ability to perform gatekeeper functionality depends on the system configuration purchased.

---

Here are the various VoiceMaster gatekeeper modes:

- **Static Mode**  
In Static Mode all call control signaling information and voice data pass directly between both ends (gateway to gateway or PC to gateway). Routes are preset and can not be dynamically updated. Using this mode reduces VoiceMaster tasks, relevant in heavy network traffic scenarios. However, the system gateways must be able to accept a rewrite number. Gatekeepers have no call control when set to Static Mode.
- **Routed Mode**  
In Routed Mode, the gatekeeper controls all RAS signaling exchanges while voice data is still gateway-to-gateway. It is responsible for setting up and breaking down calls. Routed mode is most effective when network traffic is manageable, but can slow call efficiency when traffic escalates (due to the VoiceMaster's work load).
- **Proxy Mode**  
In Proxy Mode, both signaling (call control) and voice traffic flow through the Gatekeeper. This places the entire call processing load on the VoiceMaster, resulting in decreased call efficiency. Proxy mode is relevant when your business model dictates that customers have PC-to-phone service to areas serviced by gateways which prevent access from any device but the gatekeeper.
- **Routed Mode without H.245**  
This mimics Routed Mode, with the difference that H.245 call signaling is handled by the participating gateways, not the gatekeeper.

## VoiceMaster Call Basics

In the following sections we describe the mechanics of setting up an operational VoIP system. This includes the basics of configuration, how VoiceMaster routes and processes calls, and a look at key billing functionality.

### Configuration Basics

To configure the system for operations, an Administrator performs the following basic tasks:

- Routing
  - Create Provider
  - Import Provider Rates
  - Add Gateway
  - Assign Prefixes (provider area codes) to Gateway
  - Create Route (Routing Table)
  - Assign gateway to Routing Table
- Billing
  - Create Billing Rate Table
  - Add Rates to Billing Rate Table (Add/Import/Copy rates from provider)
- Integrate Routing & Billing
  - Assign route to account
  - Assign billing rate to account

---

**Note** The Billing Rate Table is really a collection of routes.

---

### How VoiceMaster Processes Calls

The following numbered list (not a ‘procedure’/instructions), describes the actions that the VoiceMaster needs to process to make a call occur. This sequence assumes the necessary routing and billing settings exist, that the caller (subscriber) is registered within the system, and that gatekeepers, gateways and endpoints are up and functioning:

- Call/Customer Authentication
  - Find the customer (caller) account
    - Check the balance
      - If it is a prepaid account, confirm that an adequate balance exists. (If not, stop the call)
    - If the account is post-paid, let the call go through (no minimum needed)
    - Locate the billing rate table and routing table
- Authorization & Billing
  - Find Billing Rate (see Billing Rate Table diagram below)
  - Find route

---

**Note** How a route is found and discovered is a function of 1) longest match and 2) other settings that the user configures – end point priority, preferred route, least cost route, etc.

---

The specific technical sequence, a variation of VoIP Call Processing Flow earlier, is:

- Step 1** A subscriber calls into the local VoIP gateway (connected to the PSTN) via an access number (such as 1-800-xxx-xxxx).
- Step 2** The gateway negotiates the call establishment request with the RADIUS server.
- Step 3** The gateway retrieves a welcome message from the IVR server and plays it. The message prompts the subscriber for his PIN number.
- Step 4** The subscriber enters the PIN number.

---

**Note** VoiceMaster supports multiple simultaneous calls using a single PIN.

---

- Step 5** The gateway sends the PIN number to the RADIUS server for authentication.
- Step 6** The RADIUS server authenticates (or denies) the subscriber's account and returns the remaining account balance information to the gateway.
- Step 7** Again invoking the IVR, the gateway plays a credit balance message, then prompts the caller for a destination number.

---

**Note** All IVR messages are retrieved as audio data from the IVR server unless the files are already cached (present) on the gateway itself.

---

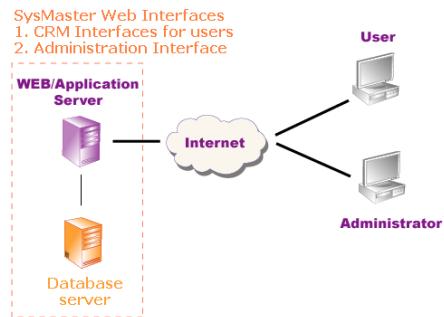
- Step 8** The caller enters the destination number.
- Step 9** The gateway sends the destination number to the RADIUS server for authorization.
- Step 10** The RADIUS server authorizes the destination number and passes to the gateway the permitted call length (based on account balance).
- Step 11** The gateway plays an IVR message specifying call time to the caller. By receiving the call duration information from RADIUS (previous step), the gateway knows when to disconnect the call.
- Step 12** The gatekeeper resolves the destination IP address (of the termination gateway) based on the destination phone number (endpoint), using defined Phone-to-IP address tables. Upon this resolution, the origination gateway establishes connection to the termination gateway.
- Step 13** The termination gateway establishes a connection to the destination endpoint side over PSTN (Public Switched Telephone Network).
- Step 14** The phone-to-phone connection is established. If either side disconnects, the local gateway informs the RADIUS server to stop call account processing. All call-relevant is written into the Database server, effectively updating VoiceMaster management billing status.

The subscriber can check at any moment status of his/her account including call history, user profile and also can recharge his/her account.

## Using The Administration Console

The VoiceMaster Administration Console is an advanced GUI (Graphical User Interface) used to administer the entire VoIP system. The Administration Console is a configuration and management tool for that business.

The different administrative functions are divided into folders and sub-folders that correspond to various management tasks.



The minimum system requirements for running the Administration console are:

- Microsoft Internet Explorer™ version 5.5 or 6.0 (recommended is version 6.0)
- Mozilla Firefox (Version \_\_)

The Administration Console is web-driven and browser-based. It interacts directly with the VoiceMaster administration web server to manage the system. This interaction is based on client-server architecture.

---

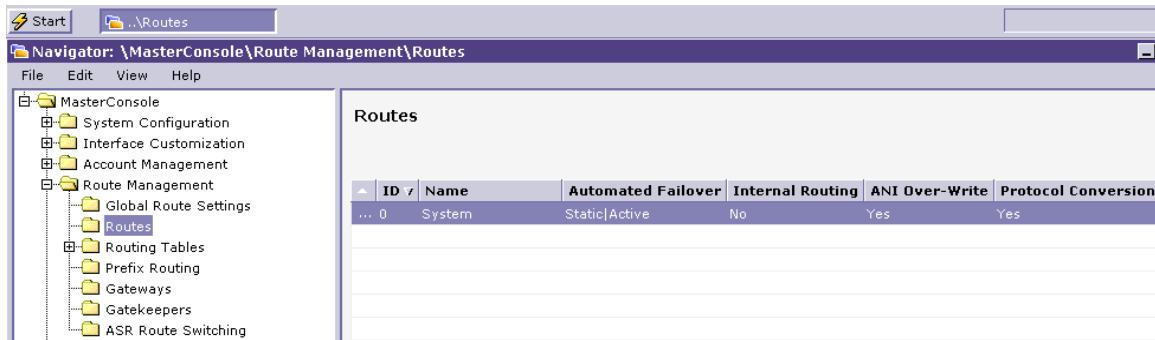
**Note** Some system commands can also be performed via a Command Line Interface. SysMaster generally recommends use of the Console for typical administrative activity.

---

The Console interface is organized according to a ‘tree’ or folder structure. Functions are organized in topic folders. Functions of similar importance or value are placed on the same level. Specific functions that belong to a larger category appear as sub-folders within the parent folder.

Folder organization reflects the natural relationship between functions and how a user (Administrator) is likely to work with them. So, for instance, Routing and Rates are ‘neighbor’ folders. When configuring client or user (subscriber) accounts, an Administrator is likely to open and close both these folders in a sequence of actions.

This illustration shows a sample view of the folder hierarchy. The user has opened the Navigator view and selected the Route Management and Routes folder:



**Figure 1-3 Route Management>Routes Folder Open**

An Administrator's working sequence typically breaks down this way:

- Step 1** Navigate to the desired function location.
- Step 2** Select the specific function or field entry (such as a route, user account, etc.).
- Step 3** Access the dialog box whose contents match the possible configuration parameters for the selected function. Define parameters, redefine existing parameters, enter field values and so on.
- Step 4** Apply the changes.
- Step 5** Navigate to another functional area and select another function/entry...

In the following sections, we detail Console components and how to use them. Read these sections carefully and refer to them as necessary during system administration.

---

**Note** One top-level folder is not used in standard VoiceMaster operation. This is the **PBX Management** folder - nestled between Batch Management and Custom Modules.

---

### Accessing the Administration Console

As mentioned, the Administration Console is web driven. You access it through a URL assigned to your VoiceMaster. This will be the public IP address assigned to the VoiceMaster during initial configuration (stored in the Network Configuration dialog box accessed from the System Configuration folder).

---

**Note** When starting the Console, a login prompt always appears. A valid username and password are required to open the console. (Usernames and passwords are case sensitive.)

---

To access the Console, follow these steps:

- Step 1** Open a Web browser.
- Step 2** Type in the URL for the VoiceMaster (this is the public IP address assigned during initial configuration) and press Enter to navigate to it.
- Step 3** A log in prompt appears, requesting:  
Username

Password

- (a) For the user name, enter **admin**
- (b) For the Password field, enter **admin** again.

---

**Note** We recommend that you change both *username* and *password* as soon as possible.  
To do so:

Select **Start>Navigator**

Select **System Configuration>System Users**

Select the Administrator from the System Users page (there will be one entry)

Select **Edit System User**

At the first field (Login Name), type in a new name (in the entry box)

At the next (Password) field, enter a new password

Confirm it in the next field entry box

Select **Apply** to save the new Login Name and Password.

**(If you have just changed the login/password,**

---

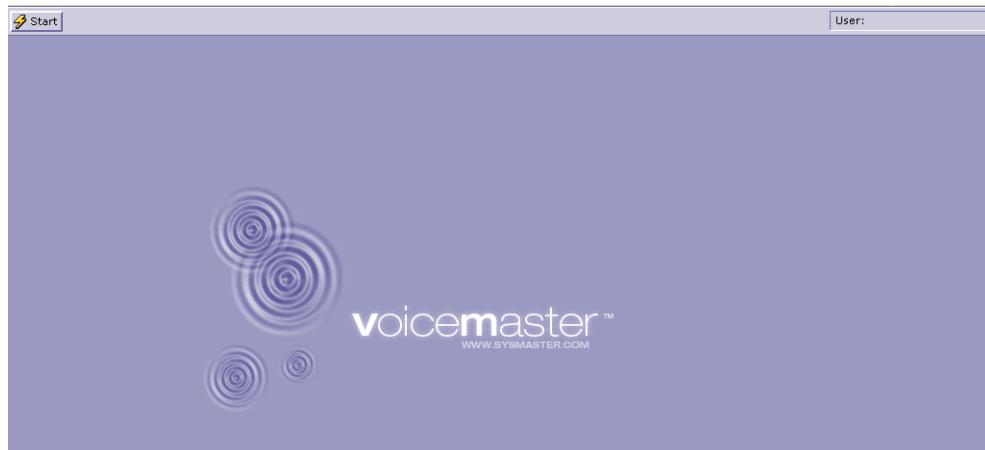
---

**Note** The system allows for only one user to login with a given system user account at a time. The user performs operations according to the privileges assigned by the top-level administrator.

---

**Step 4** Select the Login button or press Enter to log into the Console.

**Step 5** View the VoiceMaster logo and the Start menu bar:



**Figure 1-4 After Login**

**Step 6** Select **Start>Navigator** from the Start menu.



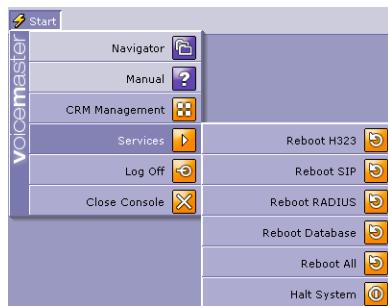
**Figure 1-5 Navigator Menu**

On selecting the Navigator option, the Navigator view is displayed:

At this point, you are ready and able to browse folders, select options and configure settings through the various dialog boxes. The Console components are discussed in detail in the next section.

### The Start Menu

Typically, you use the Start menu to open the Navigator. However, this menu has several options. All Start menu options are presented in the following illustration:



**Figure 1-6 Start Menu: All Options Visible**

Start menu options are as follows:

- Navigator opens a new Navigator window, or view (more than one can be opened at one time)
- Manual opens this Guide in .pdf format
- CRM Management
- Services, when selected, opens the displayed popup menu. This in turn offers several system reboot (and halt) options:
  - Reboot H323. Reboots H323 network protocol functions.
  - Reboot SIP. Reboots SIP protocol functions.
  - Reboot RADIUS. Reboots RADIUS AAA server.
  - Reboot Database. Reboots VoiceMaster database.
  - Reboot All
  - Halt System

**Note** Selecting any Reboot action erases previous configurations, including data. Perform these actions only if you are certain of their necessity.

---

## Administration Console Components

Basic Console elements include:

- **Start Button** – start point for running the Navigator window, show the Help window, Log out or close the console;
- **Task Bar** – hosts all buttons hooked to opened windows of the application;
- **Start Menu** – Contains basic commands for starting a new Navigator window, show the Help window, Log out and Close the console;
- **Status Bar** – Displays the currently logged user in the system;
- **Help Window** – Displays general help information or context information;
- **Navigator Window** – Serves as a browser of system objects for setup of the system;
- **Report Windows** – Separate windows containing report data.

All windows can be:

- **Moved** - drag them using the title bar;
- **Minimized** – use the minimize button on the window title bar;
- **Maximized** – use the maximize button on the window title bar;
- **Closed** – use the close button on the window title bar.

The Navigator Window menus contain the following commands:

- **File**
  - **New** – Opens a new Navigator Window;
  - **Print** – Prints the contents of the right pane of the Navigator window;
  - **Close** – Closes the window;

### View

- **Refresh** – Refreshes the right pane of the Navigator window;
- **Edit**. The Edit menu is dynamically changed, based on the selected object type from the tree. It always offers commands that are relevant to the currently selected object.
- **Add** – Adds a new object;
- **Modify** – Modifies an object selected in the right pane of the Navigator window;
- **Delete** – Deletes an object selected in the right pane of the Navigator window;
- **Manual** – Provides access to the VoiceMaster Platform manual. The manual is distributed in PDF format;
- **Help About** – Shows the current version of the product;

Report Window options vary and are discussed in their functional contexts throughout the Guide.

## Browsing and Managing Objects

The VoiceMaster Web Console features a Navigator window for browsing through the system objects and settings.

To open the Navigator window:

- Step 1** Use **Start Button > Navigator**;
- Step 2** Use the tree in the left pane of the Navigator window to browse through the objects and settings. With VoiceMaster every object can be listed in the right pane of the Navigator;
- Step 3** Click on a selected object from the tree;
- Step 4** On the right pane there will be listed all objects in the system relating to the object type selected in the tree;
- Step 5** Select an object to modify or delete;
- Step 6** Use the menu commands of the Navigator window. Alternatively, use the ellipsis button ... or double click on the selected object to edit its definition.

## CRM Web Interface/Web Server

The CRM (Customer Relationship Management) Interface is based on a modular and customizable Apache web server design. This web server features SSL functionality for safe customer information exchange. The server is the engine that runs the CRM interface, and allows a VoIP service provider's customer register for subscription and manage their own accounts.

The CRM interface allows for flexible user profile storage and account management. It provides facilities for detailed call history retrieval and account balance management. The web-based credit card interface facilitates online account funding, including balance re-charges.

---

**Note** The VoiceMaster Administrator can customize the CRM interface using the Administration Console. Different color schemes and interface layouts can be adapted to fit presentation needs. CRM website administration is discussed at length in Chapter Four of this Guide.

---



# Chapter 2: VoiceMaster Installation

---

## In This Chapter

This chapter addresses the installation requirements for the VoiceMaster and includes these sections:

- Safety Warnings
- VoiceMaster Hardware Installation
  - 2U Framework Enclosure Installation
  - 6U Framework Enclosure Installation
- VoiceMaster Initial Configuration

---

**Note** Initial configuration involves configuring public network settings for the VoiceMaster. The system ships with private IP settings.

---

We have designed the installation procedures to be as straightforward as possible. However, some procedures involve branching (multiple paths). The correct paths to follow for a given implementation are a function of 1) the Framework Enclosure purchased and 2) your network installation infrastructure and resources.

Some critical safety warnings are worth reviewing before beginning the installation procedures.

## General Safety Warnings

The warnings in this section relate to use of the hardware, including electrical components. Please review them thoroughly before unpacking your VoiceMaster.

**Warning**  This unit is intended for installation in restricted access areas accessed through the use of a special tool, lock and key, or other means. Only qualified personnel should install, replace or service this equipment.

**Warning**  Remove jewelry before working on equipment connected to power lines.

**Warning**  Always disconnect cables before you open an enclosure or touch or install internal components or an uninsulated connector. The system contains hazardous voltages.



**Warning** This equipment must be grounded. Never defeat the ground conductor or operate the equipment without a suitably installed ground conductor. Contact an electrician if suitable grounding is unavailable.



**Warning** Do not overload the AC supply branch circuit that provides power to the rack. Total rack load should not exceed 80% of the branch circuit rating.



**Warning** Blank faceplates and cover panels direct cooling airflow through the chassis and safeguard nearby equipment from the possible effects of hazardous voltages and currents originating within the chassis. All faceplates and cover ('filler') panels available should be used.



**Warning** Never attempt to lift or tilt the chassis using module handles. These may not support overall unit weight.

## **Hardware Installation**

The VoiceMaster comes in different system levels, referred to as Levels 1-5. The different levels reflect differences in processing and database CPU, as well as specific performance parameters such as call capacity.

---

**Note** Installation varies between Level 1 and Level 2 systems and higher. Level 1 systems can be installed in *either* Framework Enclosure: 2U or 6U. All Level 2 and higher systems will be housed in the 6U Framework Enclosure.

---

The two enclosures have different sizes, weights and appearances:

- The 2U Framework Enclosure is a compact, relatively light unit with a horizontal profile.
- The 6U Framework Enclosure is a heavier, larger unit with a vertical profile.

### **2U Framework Enclosure Installation**

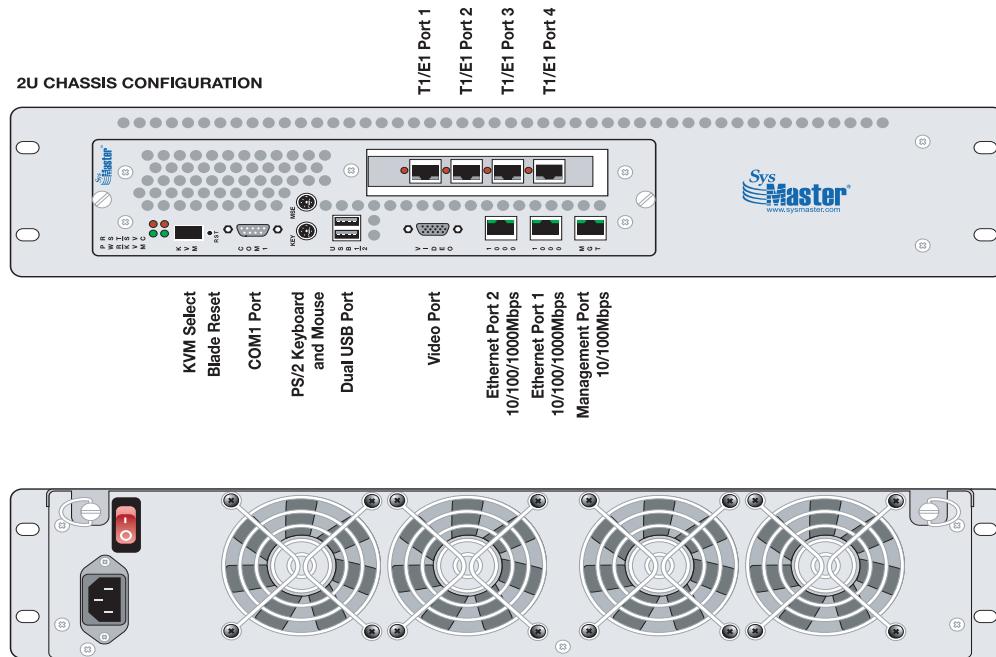
The VoiceMaster 2U Framework Enclosure is a simple, low-cost enclosure. It consists of a steel case, four fans, an AC power supply, and an On/Off switch. The 2U Framework Enclosure fits within a standard, 19-inch (482.6mm) rack mount cabinet. The installed weight of 42 pounds includes a server blade and hard disk drive.

(Specifications)

---

**Note** Please skip to the section called [6U Framework Enclosure Installation](#) if your VoiceMaster order is for the 6U Framework Enclosure.

---



**Figure 1-7      2U Framework Enclosure**

### Unpack/Install 2U Enclosure

To unpack and install the 2U enclosure, follow these steps:

- Step 1** Remove the enclosure from its packaging:
  - (a) Open the packaging, cutting any tape and seals.
  - (b) Remove the power cord and mounting brackets.
  - (c) Lift the enclosure from the package and set it on a stable surface
- Step 2** Attach the two rear mounting brackets to the rear panel slots.
- Step 3** Mount the enclosure in a network rack.
- Step 4** Insert the four pairs of mounting screws (sometimes called G-nuts) that secure the four Enclosure corners to the cabinet.
- Step 5** Connect the power cable.

---

**Note** Do not apply power to the enclosure yet. Only apply power when you configure the VoiceMaster's IP network settings (described).

---

Skip to the section called [VoiceMaster Initial Configuration](#) to configure the public network settings needed to make the VoiceMaster an active Internet node.

## 6U Framework Enclosure Installation

The VoiceMaster also comes in a 6U Framework Enclosure. This chassis provides power and cooling to multiple SysMaster Blade Servers. It consists of a steel case, dual AC power supply units, a rear Input/Output (I/O) panel, and fans.

This 6U Framework Enclosure fits inside a standard, 19-inch rack mount cabinet. With redundant, hot-plug 220V (110V) AC power supplies (see Figure 2), this enclosure weighs 70 lbs (32 kg). It is 25.5 inches deep with external fans.

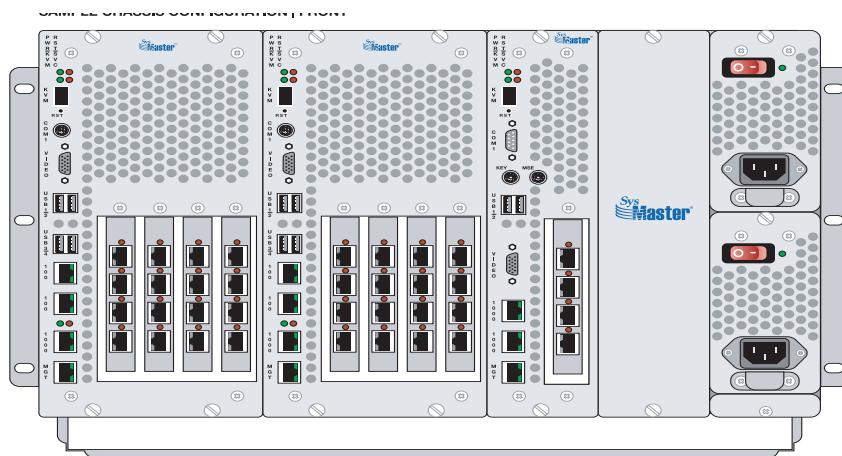
(Specifications)

---

**Note** SysMaster assumes that customers will install Framework Enclosures in a network rack. Possible options include 1) a plain rack with posts or 2) a rack enclosed within a full cabinet with front and rear doors. **In both cases, mounting instructions are identical.**

We do not describe mid-mounting or similar unconventional installation scenarios. Risks attached to any unconventional mounting configurations are borne by the customer.

---



**Figure 1-8 6U Framework Enclosure**

### Unpack and Rack Mount 6U Enclosure

Follow the instructions in this section to unpack and rack mount the 6U Framework Enclosure successfully.

The carton in which the 6U Enclosure ships includes:

- The Enclosure itself, containing the VoiceMaster server
- Dual AC power supplies in a single-unit two-winged packaged (sits atop the Framework Enclosure)
- Miscellaneous components, each in its carton or plastic wrapping:
  - A filler panel or panels (the number and size to fit your system specifications)
  - A keyboard
  - A cable tunnel

- Two rack mount brackets
- Screws
- Four power cords
- The *VoiceMaster QuickStart Guide*.

---

**Note** SysMaster supplies two sets of AC power supply cords to accommodate both 110 and 220 VAC installations. Use the 220 VAC cords if your infrastructure supports this standard. This facilitates power supply redundancy. Using 110V with multiple server blades may not provide Power Supply redundancy.

---

## 6U Framework Enclosure Unpacking

The VoiceMaster 6U Framework Enclosure has multiple components, all of which are packed into one large carton. Both because of the number of components and the weight of some, careful attention should be paid to the method and sequence of unpacking. Further, it is important to designate a pre-installation area where components can be ‘stored’ in preparation for installation (including rack mounting).

---

**Note** All components should be set on level surfaces to prevent component damage or injury to personnel. Do not unwrap individual components until you are ready to install them.

---

Follow these instructions to remove VoiceMaster 6U Framework Enclosure components:

- Step 1** Cut open the shipping carton at the top.
- Step 2** Remove the miscellaneous components: filler panel, keyboard, cable tunnel, rack mount brackets, power cords and manuals.

---

**Note** Review the Safety Warnings earlier in this chapter before proceeding.

---

- Step 3** Remove the power supply packaging (parallel wings connected by a bridge). Place it on a flat surface.
- Step 4** Remove the Framework Enclosure from the shipping box:
- Pull the Enclosure up by its front section while it is still in the shipping box.
  - Lift the Enclosure from the box and set it down on a stable surface.

---

**Note** The empty Framework Enclosure is a heavy object. Two or three people should participate in unpacking and installation.

---

- Step 5** Unwrap the Framework Enclosure by cutting the plastic secured by tape behind the rear panel and removing the wrapping.

- Step 6** Remove the VoiceMaster server blade(s) from the packaging.
- Whether you order one or more VoiceMaster server blades, each comes in its own packaging. Contents include: 1) a network cable 2) a crossover cable, and 3) an instruction sheet with serial number and default temporary IP address.
- (a) Remove the two packaging retainers.
  - (b) Lift the blade from the package and the plastic wrapping from the blade.
  - (c) Set the server blade in a safe place (blade installation follows enclosure rack mounting.)
  - (d) Repeat Steps a-c for any other blades you may have ordered.

---

**Note** Store all packaging for future use and avoid future logistical problems.

---

## 6U Installation and Mounting Instructions

Installing the VoiceMaster 6U Framework Enclosure is a two-part process:

- Framework Enclosure Preliminary Assembly
- Rack mounting

Cable tunnel mounting (optional) and AC power supply installation (mandatory) are explained in context.

---

**Note** Do not move large racks by yourself. Before working with a network rack, install stabilizing feet or join multiple racks together. The full rack weight must rest on the floor. Always load a rack from the bottom up for stability. When removing a component, do so slowly. Never remove multiple components at once.

---

### Framework Enclosure Preliminary Assembly

Preliminary assembly of the Framework Enclosure involves attaching the two rack mount brackets where the Enclosure sides and back meet. Each bracket is unique and intended for a particular side of the Enclosure. Trial and error will quickly reveal which bracket fits which side of the enclosure.

---

**Note** When attaching the brackets, make sure the shelves ('ears') are at the Enclosure rear, not the mid-point.

---

- Step 1** Locate the two rack mount brackets and the packaged screws. Unwrap the two brackets and remove six screws from their package.
- Step 2** Lift the first bracket and slide it against the side of the enclosure with the shelf at the back. The shelf should protrude from the corner of the unit just as the front shelf does.
- Step 3** Using a Phillips screwdriver, attach three screws through the holes to secure the rack mount bracket to the Enclosure.
- Step 4** Repeat Steps 1-3 for the rack mount bracket on the opposite side of the Framework Enclosure.

## Cable Tunnel Mounting (Optional)

If you intend to use the cable tunnel supplied with the system, you must mount it *before* mounting the Framework Enclosure itself. The tunnel is attached to the bottom of the enclosure.

To complete cable tunnel installation, these items are needed:

- A #2 Phillips screwdriver
- Six flathead screws (enclosed)

---

**Note** The tunnel has no true front or back, so no orientation is needed.

---

**Step 1** Turn the 6U Framework Enclosure on its side.

**Step 2** Position the cable tunnel so the screw holes are visible.

**Step 3** Fasten the cable tunnel to the bottom of 6U Framework Enclosure by attaching and tightening all six screws.

## Mounting the Framework Enclosure

The Framework Enclosure is now ready for mounting in a network cabinet rack. At least two people should participate in mounting the 6U Framework Enclosure because of its weight and the potential risks involved. **If three are involved, safety is increased for both the system and the installers.**

**Step 1** If your infrastructure includes a full cabinet, open both front and rear doors now.

**Step 2** Lift the Framework Enclosure and position it at the desired post level. Make sure that the holes in the forward shelves align with corresponding post holes.

**Step 3** Install (loosely) single screws in the **front** shelves center holes. (These shelves are at Enclosure left and right.)

**Step 4** Add the remaining screws to the front and rear shelves (12 screws secure the unit in total).

---

**Note** The exact order of screw-installation is manpower-dependant. The best way to do this is to secure first one side, then the other. If only two people are available, you will have to improvise. Always keep the safety of the unit and the personnel in mind.

---

**Step 5** Tighten all screws.

**Step 6** Mount the AC power supplies within the enclosure. See the [AC Power Supply Installation](#) section for details on installing or replacing a redundant hot-plug AC power supply. Do not plug in the power cords yet.

**Step 7** Mount your VoiceMaster Blade Server in the Framework Enclosure. To do so, fit the blade between the top and bottom rails (white in color) and slide it forward until seated.

---

**Note** Pushing a blade that is not positioned properly between rails will stress it and may cause either blade deformation or permanent structural damage.

---

**Step 8** If you have ordered multiple servers, install them now.

**Step 9** Connect KVM, USB peripherals and network cables.

- Step 10** Mount any filler panels in the Framework Enclosure midplane. These panels assure proper airflow across the Blade Servers.

**Note** The size and quantity of filler panels will fit your system configuration. If all slots are filled with blades, no panels are supplied.

---

- Step 11** Check the fan power cables at the rear of the unit. Both cables should be securely connected before applying power to the enclosure.
- Step 12** Apply power to the Framework Enclosure once the power supplies are installed. See [AC Power Supply Installation](#).
- Step 13** Once the power supplies are installed and all cables connected, close the front and back cabinet doors.

### AC Power Supply Installation

To install an AC power supply:

- Step 1** If you have not removed the AC power supplies from its packaging, do so now:
- Cut the tape that covers the protective foam around the first power supply.
  - Remove the foam and the first power supply.
  - Repeat (b) and (c) for the second AC power supply.
- Step 2** Support the power supply with one hand while you guide it into the power supply bay with the other.
- Step 3** Push the power supply all the way in until it settles at the rear. You will feel resistance. Do not force the power supply once you feel resistance or damage to the unit may result.
- Step 4** Repeat Steps 2 and 3 for the second supply.
- Step 5** Hand-tighten the screws at the top and bottom of both power supplies.
- Step 6** Plug in power cords (110 or 220, depending on your installation). Do not apply power unless both fan power cables are securely connected to the rear I/O panel.
- Step 7** Switch on the power supplies.

**Note** Do not simultaneously mount power supplies and blades in the 6U Framework Enclosure.

---

### Power Supply Removal

To remove an AC Power Supply (when hot swapping or otherwise replacing a supply):

- Step 1** Switch off the power supply (if hot swapping, power stays on).
- Step 2** Hand-loosen the screws at the top and bottom of both power supplies.
- Step 3** Grasp the front handle of the power supply bay and tug the power supply toward you.
- Step 4** Support the supply with your other hand as you pull it from the enclosure.

**Warning**  Do not leave the system without a power supply for any length of time, including a supply designated for replacement. This can affect system ventilation.

---

**Note** The installation of a redundant UPS power supply assures continuous operation in the event of system failure or a power outage. A VoiceMaster without UPS may suffer hard disk corruption during a failure.

---

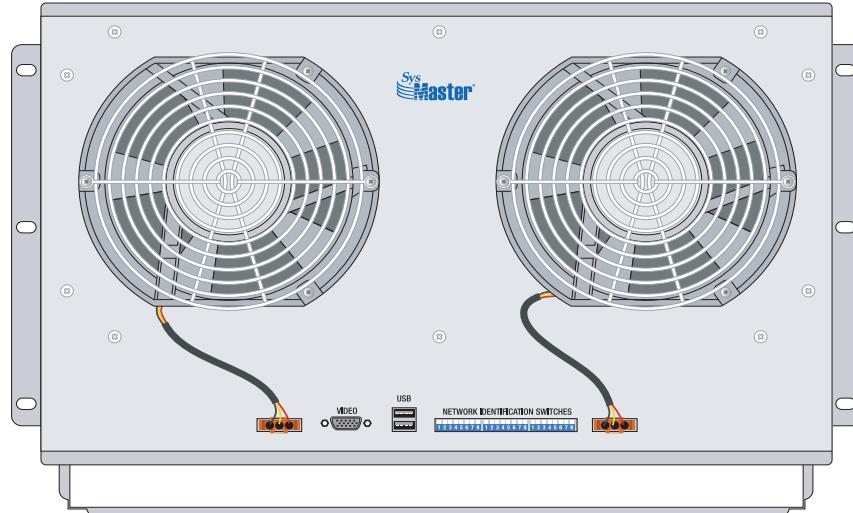
## System Fans

The 6U Framework Enclosure features two redundant 300 cubic feet per minute (cfm) system fans that circulate air from front to back (for a total of 600 cfm). Behind each fan is a set of baffles that closes in the event of fan failure. This guarantees that airflow travels only through a working fan.

---

**Note** These fans are hot swappable for replacement during system operation.

---



**Figure 1-9 Fans (Rear View)**

To hot swap (remove and replace a system fan during system operation):

- Step 1** Disconnect the fan's two-pronged power connector.
- Step 2** Remove the mounting screws that secure the fan to the enclosure at the fan's outside edges.
- Step 3** Remove the fan.
- Step 4** Install the new fan.
- Step 5** Secure the four mounting screws that hold the fan to the enclosure.
- Step 6** Connect the fan's power supply. If the system has power, it will start immediately.

## Rear Input / Output (I/O) Panel

Use the Framework Enclosure rear I/O panel to connect the fan power and KVM switch. The rear I/O panel contains outlets for the chassis fans. The panel also has three banks of switches to identify the location of the site, rack and Framework Enclosure.

### KVM Switches

Each Framework Enclosure has a built-in KVM switch that supports a single keyboard, video and mouse per enclosure. Connect multiple Framework Enclosures to a single KVM switch using the video port and USB ports for keyboard and mouse. If the KVM switch supports KVM-over-IP, you can connect it for this purpose as well.

### GSM Modem Connectivity (optional)

A GSM modem can also be attached, as shown in Figure 4.

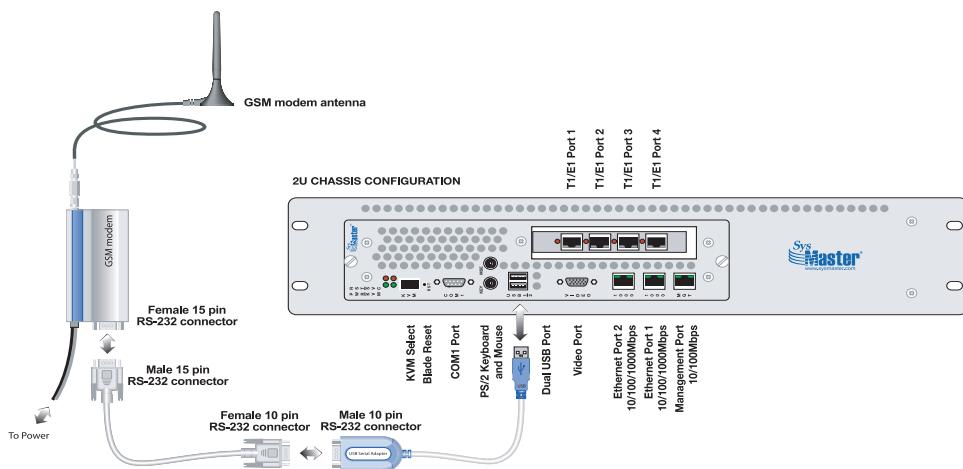


Figure 1-10 GSM Modem Connection

### Network Adapter Port Locations

One Ethernet port per enclosure is associated with the VoiceMaster's private IP address. Ethernet network adapter port location depends on the hardware enclosure ordered. *Connecting to any other port will not enable initial VoiceMaster configuration.*

The 2U enclosure (VoiceMaster Level 1) is horizontal in orientation, as shown:

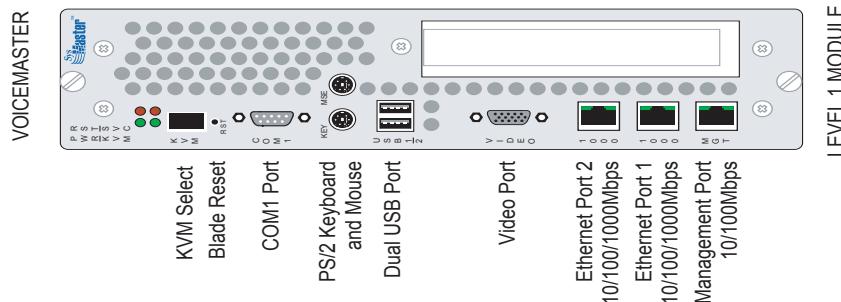
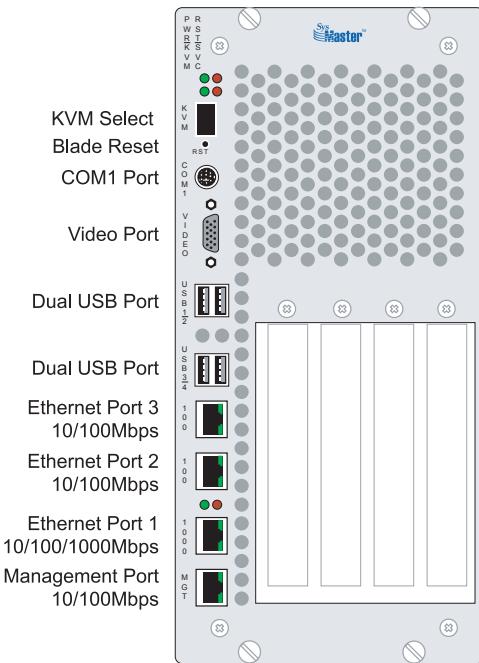


Figure 1-11 2U Framework Enclosure Port Locations

Note the three network adapter ports located at the bottom right portion of the faceplate. **Ethernet Port 1 10/100/1000 Mbps**, the middle of these three ports, receives the network cable.

Customers with the 6U hardware enclosure (VoiceMaster Level 2 and up) will see the following faceplate:



**Figure 1-12 Network Ports in (6U) Framework Enclosure**

The cable fits into Ethernet Port 1 that sits just above the Management Port.

## VoiceMaster Initial Configuration

Each unit is shipped with a private IP address. Before the VoiceMaster can operate as a recognized Internet device, or node, this private address must be changed to a public one.

In order to accomplish this, the Administrator must connect to the VoiceMaster through its private address, then replace that with public IP address settings (three in all). You do this by connecting to the VoiceMaster and using the Administration Console to change the default network settings.

A preliminary step is required before your system can ‘talk’ to the VoiceMaster, however. That is the temporary assignment of your (public) workstation/laptop IP address to a private IP within the VoiceMaster’s network and subnet.

Once the devices can communicate, you configure the required public IP settings for the VoiceMaster. The final step is to replace *your* system’s temporary network settings with its original, public settings.

This entire process is presented in the form of step-by-step procedures in the sections that follow.

---

**Note** Two connection methods exist for configuring the VoiceMaster via the network:

Peer-to-peer network connection between the PC/laptop and the VoiceMaster using a crossover cable.

Switch-based network connection, in which a network cable links the PC/laptop to a network switch and then to the VoiceMaster.

---

## Establish a Communications Link to the VoiceMaster

Before setting public VoiceMaster network configuration setting, you must establish network communications between your system and the VoiceMaster. This is done by changing your system network settings so they conform to the VoiceMaster private network:

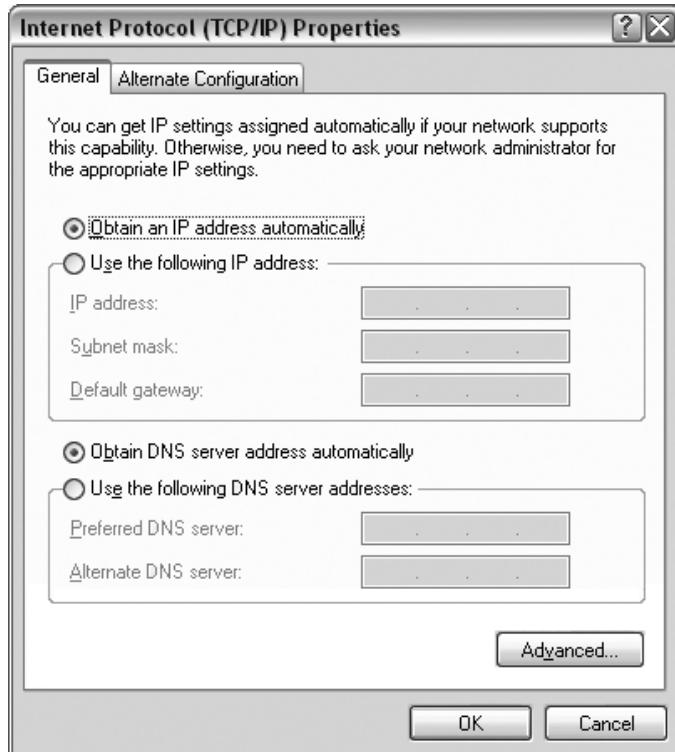
**Step 1** Refer to the printed documentation that shipped with the VoiceMaster to locate its temporary, private IP address (or addresses, if you ordered multiple servers).

**Step 2** Physically connect your system to the VoiceMaster:

- (a) For peer-to-peer connection, connect to the designated VoiceMaster Ethernet port using a *crossover cable*. Refer to Figures 2-5 and 2-6 to identify the correct Ethernet port for the appropriate Framework Enclosure.
- (b) If connecting to the VoiceMaster through a switch, connect the computer to the appropriate switch port using a network cable.

**Step 3** Assign the laptop or workstation a a **private IP address** that ‘sits’ on the same private network as the shipped VoiceMaster. To do this:

- (a) From the Windows Start menu, select Settings/Control panel.
- (b) Open the Network icon.
- (c) Select Local Area Connection and then right-click the Properties button.
- (d) Select TCP/IP Properties. Highlight Internet Protocol/TCP/IP and select Properties. This dialog is displayed:



**Figure 1-13 TCP/IP Properties Dialog**

**Step 4** Change your computer's IP address to add it temporarily to the VoiceMaster's private network:

If the VoiceMaster's private IP address is: 192.168.0.201, assign an IP where the first three strings match and the final portion is between 1-254 (in the same subnet mask as the VoiceMaster). For instance:

**192.168.0.207** (or any other unique IP address)

**Note** Be sure *not* to assign your computer an IP address *identical* to that of the VoiceMaster.

**Step 5** Assign a subnet mask (the same subnet mask to which the VoiceMaster belongs).

**Step 6** Select **OK** to confirm and enforce changes.

**Step 7** Execute Start/Run/CMD to open an Editing shell and confirm the changes in your computer's IP address and subnet mask.

Type **ipconfig /all**.

View the result, then close the 'shell' program.

## Configure VoiceMaster Public Network Settings

To configure the VoiceMaster public network settings:

- Step 1** Open a Browser.
- Step 2** In the URL Edit box, type in the private IP address for the VoiceMaster (available on the printed sheet included with your system).
- Step 3** Confirm any network security alert prompts and access the **Administration Console**.
- Step 4** Type in **Admin** and **Admin** again at the user name and password prompts.
- Step 5** Select **Start>Navigator**.
- Step 6** Select **System Configuration>Network Configuration**.
- Step 7** Now select the first folder in Network Configuration. It is **Server Configuration**:

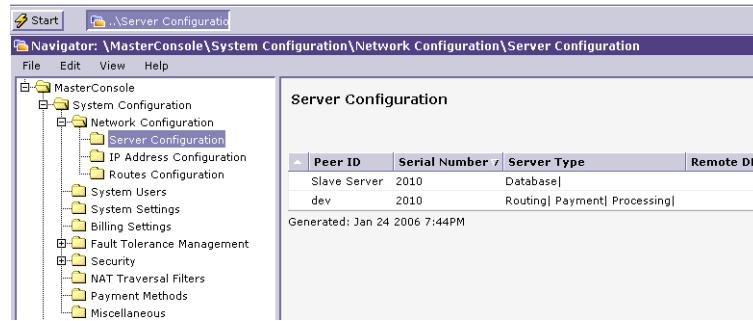


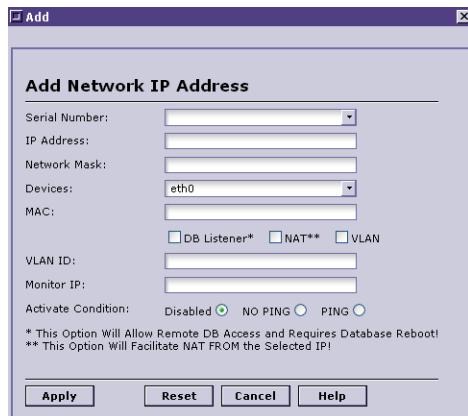
Figure 1-14 Server Configuration Window

- Step 8** Select **Edit>Add Server Configuration**. View the dialog:



**Figure 1-15 Configuring Public Network Settings**

- Step 9** Set the Gateway IP address at the Gateway field (no other parameters need be defined at this point).
- Step 10** Select **Apply**. The dialog box will close.
- Step 11** Select the **IP Address Configuration** folder.
- Step 12** Select **Edit>Add Server IP Configuration**. The following dialog appears:

**Figure 1-16 Completing VoiceMaster Public Network Configuration**

- Step 13** Set the Serial Number. Open the pull-down menu and select the correct serial number.

---

**Note** if your system has one server, one choice will be available. If you have multiple servers, refer to the information sheet included with your system and verify the correct serial number (the number will also appear on a label on the front of the system).

---

- Step 14** Set the IP Address in the next field.
- Step 15** Assign the Network Mask.
- Step 16** Click **Apply**. The VoiceMaster public network settings are now complete. Additional network settings may be configured later.

---

**Note** The preceding instruction set applies if you have a Level 1 or 2 system with one server handling all processing functions. Customers who have purchases Level 3 (and up) systems with multiple servers, will repeat Steps 11-16 to configure multiple server IP settings.

---

## Restore Your System's Public Network Settings

Now that the VoiceMaster is publicly configured, your own system must also be reset to its original settings. (The temporary, private IP settings configured to contact the VoiceMaster must be replaced.)

Refer to the section called [Establish a Communications Link with the VoiceMaster](#). Repeat Steps 3-6 in that section, replacing the temporary private settings with the original IP address and subnet mask parameters.

## Network Connectivity

We nearly forgot. One step remains to make the VoiceMaster an accessible public node. Using a straight-through network cable, connect the VoiceMaster to the network switch or hub (see the relevant device documentation for correct port locations).

## Changing Default Password

Use the VoiceMaster Administration Console to change the default system password. This is essential to preserve system security.

Perform these actions to replace the default password with a unique and secure password:

- Step 1** Open the VoiceMaster Administration Console on your network management workstation.
- Step 2** Select **Start>Navigator**.
- Step 3** Once the Navigator window appears, select the **System Configuration** folder.
- Step 4** Select **Global VoIP Settings>System Configuration**.
- Step 5** Select **Edit Settings** from the Edit menu.
- Step 6** The System Configuration dialog box appears. Click on the second text entry box next for **System Password for ‘manager’**.
- Step 7** Type in a new password. Write the password down and store for reference.
- Step 8** Select **Apply** to save the password change and close the dialog box.
- Step 9** Close the Administration Console.

## Synchronizing the Uniswitch with Voicemaster Billing Platform and Streamer and/or Concentrator with Content Management Server

In order for the Uniswitch to operate in conjunction with the Voicemaster Billing platform, the Uniswitch needs to be configured to use the database of the Voicemaster. The same applies for the configuration of an IPTV system when the Streamer and Concentrator have to be configured to use the database of the Content Management Server. The Voicemaster and the Content Management Server serve as a remote database for the Uniswitch and Streamer/Concentrator servers, respectively. Therefore, the following explanation will be referring only to Uniswitch and Voicemaster Billing platform.

Each of the servers to be included in the setup must be defined under the Network Configuration/Server Configuration menu of the Voicemaster Billing Platform. In order to synchronize the servers, it is necessary to enter the serial numbers and an IP address of each corresponding server. Each server is pre-configured with a server entry that includes the serial number and a private IP address.

All servers that will use the database of the Voicemaster Billing platform must be listed in the Server and Network Configuration lists of the Voicemaster Billing platform. The network settings for each server must be correct because once the Uniswitch is synchronized with the remote database of the Voicemaster, it will use the network information from the Voicemaster database.

Perform the following steps to synchronize the Uniswitch with the remote database of the Voicemaster Billing platform. Note that these steps assume that all servers have been assigned IP addresses and the servers are accessible remotely:

**Server Definition in the Voicemaster Billing Server:**

- 1** Navigate to the Server Configuration folder.
- 2** In the IP Address Configuration of the Voicemaster Billing Server, the DB Listener check-box must be checked.
- 3** Create a server configuration entry for the Uniswitch with the Serial Number of the Uniswitch. The server type should be "Routing" and "Processing"
- 4** In the Remote DB IP field of the Uniswitch server entry, provide the IP address of the Voicemaster Billing platform (serving as remote database).
- 5** Create an IP Address Configuration entry with the serial number of the Uniswitch.
- 6** Activate the network configuration of the Voicemaster Billing platform from the Voicemaster Billing web administration console by highlighting the server entry, then right-click and select the "Activate Network Configuration" option.

**Server Definition in the Uniswitch**

- 1** Create a server configuration entry for the Voicemaster Billing platform with the VM Serial Number. The server type should be "Database Server" and "Payment Server".
- 2** Create an IP Address Configuration entry with the serial number of the Voicemaster Billing platform.
- 3** In the Remote DB IP field of the Uniswitch server entry, provide the IP address of the Voicemaster Billing platform (serving as remote database).
- 4** Activate the Uniswitch network configuration from the Uniswitch web administration console by highlighting the server entry, then right-click and select the "Activate Network Configuration" option.



# Chapter 3: VoIP Service Configuration

---

## In This Chapter

This chapter explains how to set up basic VoIP service using the VoiceMaster Administration Console. At this point, all elements are in place to create the infrastructure that makes the VoIP call network go.

We focus on the phases required to build this infrastructure and create basic VoIP service.

The Chapter sections divide the configuration procedure into stages, each with its own distinct purpose. They include:

- An **Overview** section describes how VoiceMaster is used to build VoIP service.
- Network Provider Configuration explains how to configure provider accounts and rates and set up provider-related routing elements.
- **Configure Routing Tables (Routes)** sets out the actual configuration of routing tables and the routes associated with them. Routing tables create a store of possible routes that the system uses to build a pathway for each authorized call.
- **Billing Configuration** explains how to configure a provider and the billing rate structures.
- Activating VoIP Service: Linking Routes, Rates & Subscribers describes how to tie customer accounts to this infrastructure and enable VoIP calls.

---

**Note** The order in which we present the basic procedural sections is a logical way to configure a service. VoiceMaster is modular by nature, and the exact order of these procedures can vary. For instance, customer accounts may be configured in the last phase (as described in this chapter) - or at the time a provider account is created. *Please use the order provided here until you have gained sufficient familiarity with the Administration Console and the system to vary the sequence.*

---

Perform dry-run configurations to gain confidence with the process if necessary. We recommend applying procedures to ‘dummy’ accounts to become familiar with the process. (Any mistakes in defining actual configuration parameters are easily edited at any time.)

## Overview

The components of a successful VoIP service are in place. The pre-sale process involved constructing a business model with the help of a SysMaster salesperson. The purchase has been made, the system received, installed and configured to function as a working IP node.

What remains to be done is building a configuration infrastructure that turns the potential power of your VoiceMaster into a functioning VoIP service business operating center. The procedures in this chapter accomplish just that. By the time you complete them, a basic service will be configured, creating a foundation on which to enlarge and customize your business.

Here is a condensed view of how components are assembled and linked to create this working service:

- **Configure Network Providers.** This is the basic information describing each network provider that the service will employ. This phase includes creating the actual provider accounts, and defining provider billing rates and termination devices associated with the providers. Assign area codes to provider gateways via Prefix Routing.
- **Configure Routing Tables & Routes.** Create routing tables. Define parameters that structure the individual routes that will be associated with these tables. Associate gateways with routing tables, and create the actual routes by linking rules, clients and area codes with termination devices.
- **Billing Configuration.** This is where you create a billing rate table, establishing billing policies for different subscribers. How you build these tables is a reflection of business model needs, including revenue/profit requirements and subscriber expectations.
- **Link to Subscribers.** Create subscriber accounts, then assign configured routes and rates to these accounts. This is where all components come together. This stage is like turning the key to ignite the VoIP service engine. When complete, VoIP calls are enabled using the entire infrastructure:
  - The customer/subscriber requests call initiation. The call is authorized by the gateway/gatekeeper using account data stored in the VoiceMaster. The subscriber's balance is noted and call time is defined. Call (billing) accounting begins.
  - The system selects a route based on rules to apply to subscribers and requested destinations.
  - The system route utilizes the network provider's supplied bandwidth, relevant at the point the authorized call is shuttled (compressed into digital form) from the voice/PBX network to the Internet (data) network. Termination devices (gateways) terminate the IP call portion and send it to the receiving endpoint (telephone).
  - The call concludes, either because the parties end it or because allotted time expires. Real-time billing is processed. The call is charged to the subscriber, the data entered into the system database.

Thus we can see how basic configuration components (configured according to the procedures in the following sections) form the foundation of a VoIP service. They come into play on each and every call. Their implementation facilitates a smooth and profitable VoIP business model. Network Provider Configuration

This section includes all procedures that complete network provider(s) configuration. These lay the groundwork for routing and billing configuration functions that follow.

## Create a Provider Account

The very first step is to create and configure provider(s) accounts. (The provider supplies bandwidth and termination gateways and *charges* the VoIP service 'use' rates that represent his billing expenses.)

To create a provider account, follow these instructions:

- Step 1** Log into the Administration Console using current username and password.
- Step 2** Select **Start>Navigator**.
- Step 3** When the Navigator opens, select **Account Management**. The Console view changes:

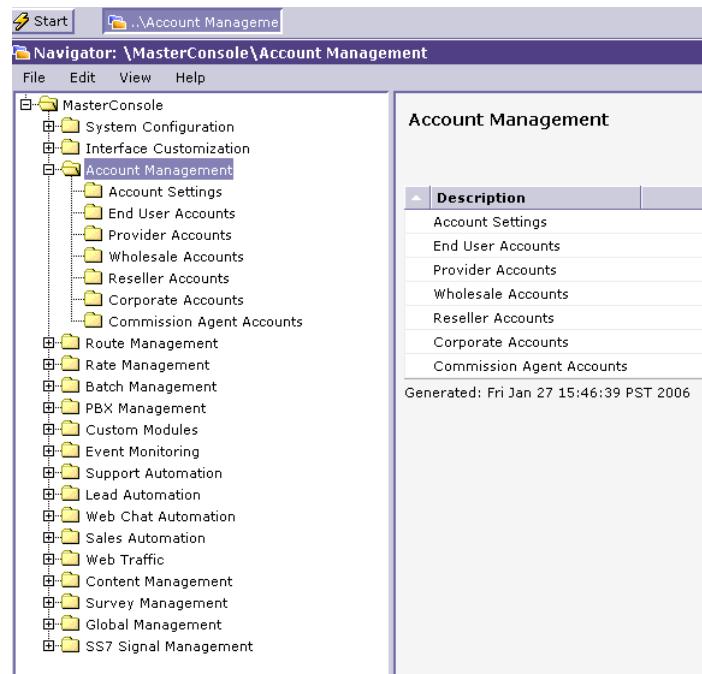


Figure 1-17 Account Management Functions

**Step 4** Select **Provider Accounts** and the view changes:

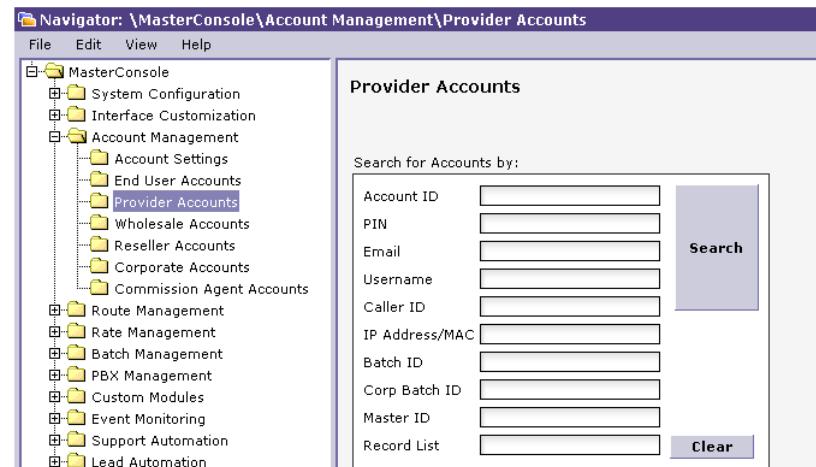
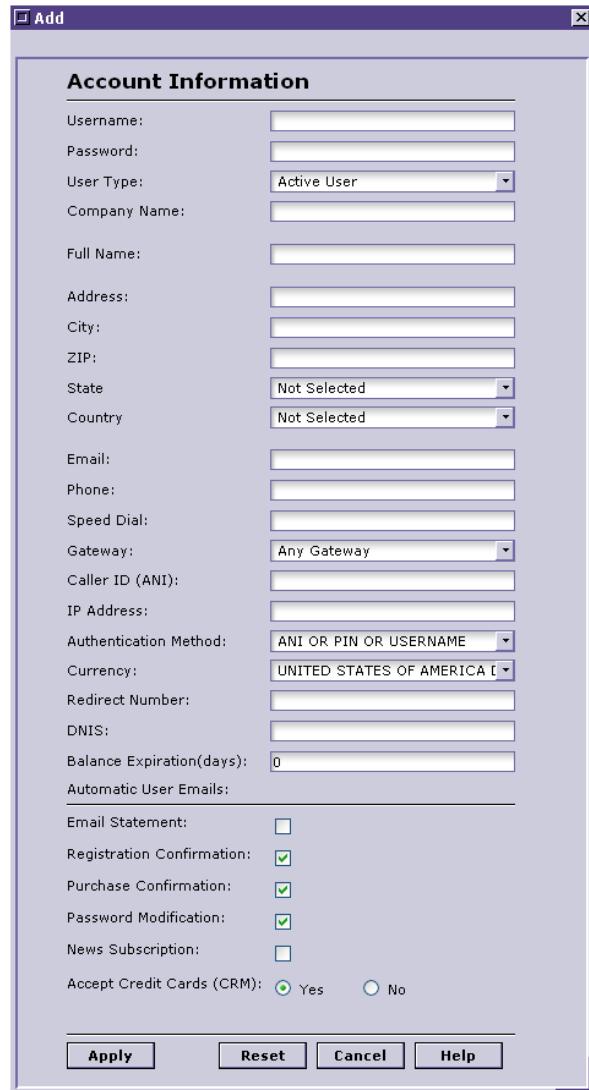


Figure 1-18 Provider Accounts View

**Step 5** From the Edit menu, select **Edit>Add Account**. The Account Information dialog opens:



**Figure 1-19 Add a Provider Account**

- Step 6** Create the new provider account by defining its parameters (either by typing information in text entry fields or by selecting options from pull-down menus; or select check boxes):
- Type a username in the first field;
  - Type a password;
  - Define the user type. Choose **Network Provider** from the pull-down options.

---

**Note** Once you select ‘Network Provider’ as the user type, the dialog box contents are abbreviated (as shown in the figure that follows).

---



Figure 1-20 Creating Provider Account: Dialog Change

- Step 7** Enter the provider company name.
- Step 8** Enter a full name. Most likely, this is the company owner.
- Step 9** In the remaining fields, enter the provider address and contact information.
- Step 10** Click **Apply**. The account is created and the dialog box disappears. The account is added below the Search box on the Provider Accounts window pane. **An Account ID is automatically generated and applied to the new account:**

Figure 1-21 New Provider Account Generated

Congratulations! The first step in configuring a working VoIP service is complete.

---

**Note** VoiceMaster will automatically create a new provider rate table for all new provider accounts. You can check this by selecting Rate Management>Provider Rate Tables. A new folder is visible. We recommend that you record the new provider account parameters for reference. Modify account definitions at any time through Account Management editing functions.

---

## Configure Provider Rates

The next phase in creating a VoIP infrastructure is configuring provider rates. Two approaches are available:

- **Import Provider Rates.** Importing provider rate spreadsheet data that you have received from the provider. When importing provider rates, the imported file *must be* in comma-delimited format with all parameter values supplied.)

---

**Note** Defining the various parameters is an essential aspect of configuring billing in VoiceMaster and enabling coherent billing administration practices.

---

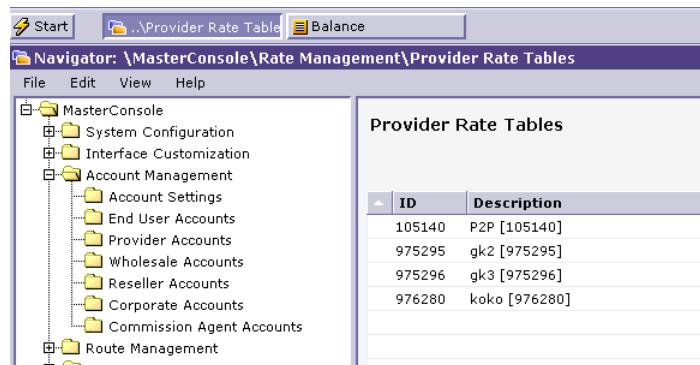
- **Add Provider Rates.** Manually add the provider rate data. This is used if the provider rates are not available in proper format or if only a few rates are to be configured.

### Importing Provider Rates

To import provider rates, perform these steps:

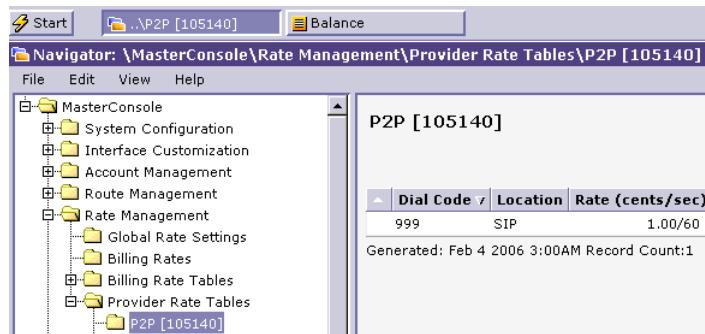
**Step 1** Locate the spreadsheet sent by the network provider whose account you have now created. Request it now if you have not done so. When you receive it, place it in a directory easily associated with the provider's file(s).

**Step 2** Select **Rate Management>Provider Rate Tables**. The Navigator view changes:



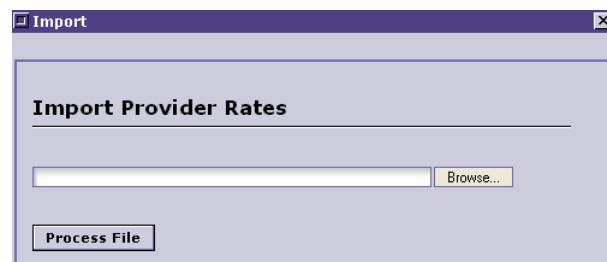
**Figure 1-22 Provider Rate Tables View**

**Step 3** Select the folder named for the new provider account. In this example, 'Vanoipe Enterprises' is the first provider account created for the new VoiceMaster. The table is displayed. (Since no rates have yet been imported, no rate entries appear.)



**Figure 1-23 New Provider Rate Table, Before Rates Import**

**Step 4** Select **Edit>Import Provider Rates**. The import dialog appears:



**Figure 1-24 Import Rates Dialog**

- Step 5** Type in or browse to the directory path and file name of the provider rate form. If you browse, use Windows “Choose File” dialog to locate the file (it will display on clicking the **Browse...** button).
- Step 6** Navigate to the correct folder and select the spreadsheet file. It will load into the ‘File name’ field.
- Step 7** Select **Open** to load the file into the Import Rates dialog (Figure 4-7).
- Step 8** Select **Process File** to import the first ‘Vanoipe’ rates into the Provider Rate table.

---

**Note** Provider rates are set *by area code*. If a provider services multiple area codes, then a set of rates for all area codes is imported. (VoiceMaster treats each entry individually as part of billing administration practices.)

---

### Add Provider Rates

The alternative to importing a provider’s rates is to add them to the system manually. This can be a quick way to add a single rate or when a provider does not provide your business his rates in an importable format.

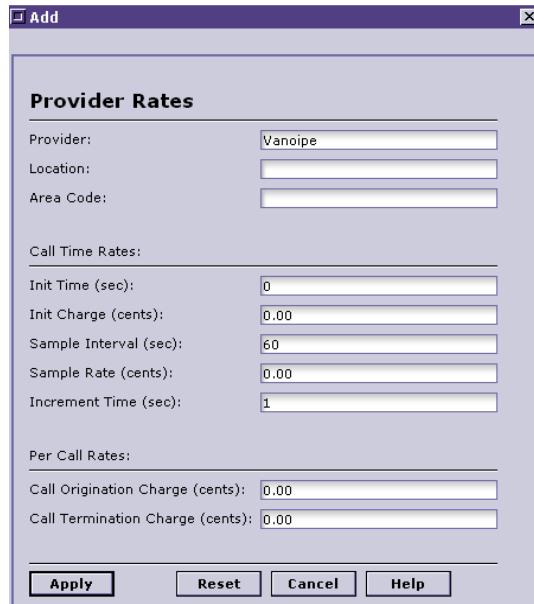
---

**Note** Even though you import the rates manually, you must still *know* them. Contact the provider if he has not supplied the parameters.

---

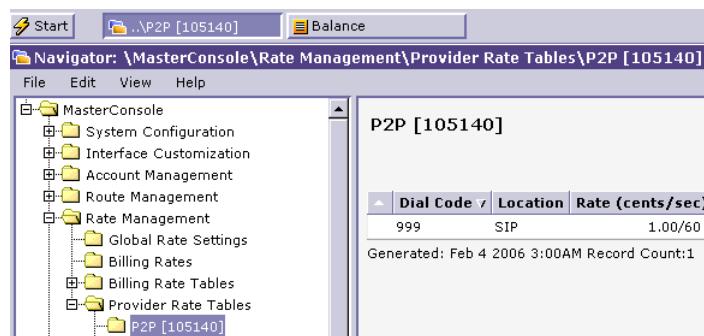
To add provider rates:

- Step 1** Select **Rate Management>Provider Rate Tables**.
- Step 2** Select the folder associated with the new provider.
- Step 3** Select **Edit>Add Provider Rate**. The dialog is displayed:



**Figure 1-25 Add Provider Rates**

- Step 4** Define provider location and area code. (Note that rates are associated with area codes; multiple rates are applicable when the provider ‘covers’ multiple termination area codes.)
- Step 5** Set Call Time Rate parameters (refer to the Rate Management chapter for expansion of each of these fields).
- Step 6** Assign Per Call Rates.
- Step 7** Select **Apply** to enforce changes.
- Step 8** The entry appears in the provider’s rate table:



**Figure 1-26 Provider Rate Entry**

Repeat the procedure for remaining provider rates to add manually.

## Add Provider Device

The third step in building the VoIP service routing foundation is to add the provider device. A network provider may use either a gateway or gatekeeper to terminate IP traffic and route the termination (PBX) leg of a VoIP call.

---

**Note** H.323 network providers will use either a gateway or a gatekeeper, while SIP providers employ gateways only.

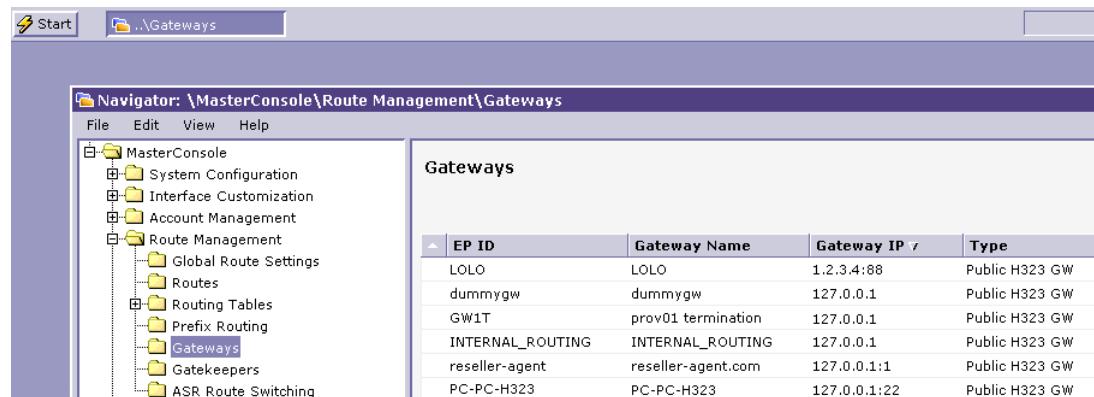
---

This section is divided into two procedural subsections, one for adding provider gateways and the second for provider gatekeepers.

### Add Provider Gateway

When the provider's device is a gateway, follow these instructions to add it to the system:

**Step 1** Select **Route Management>Gateways**. The Navigator view changes to reflect your selection:

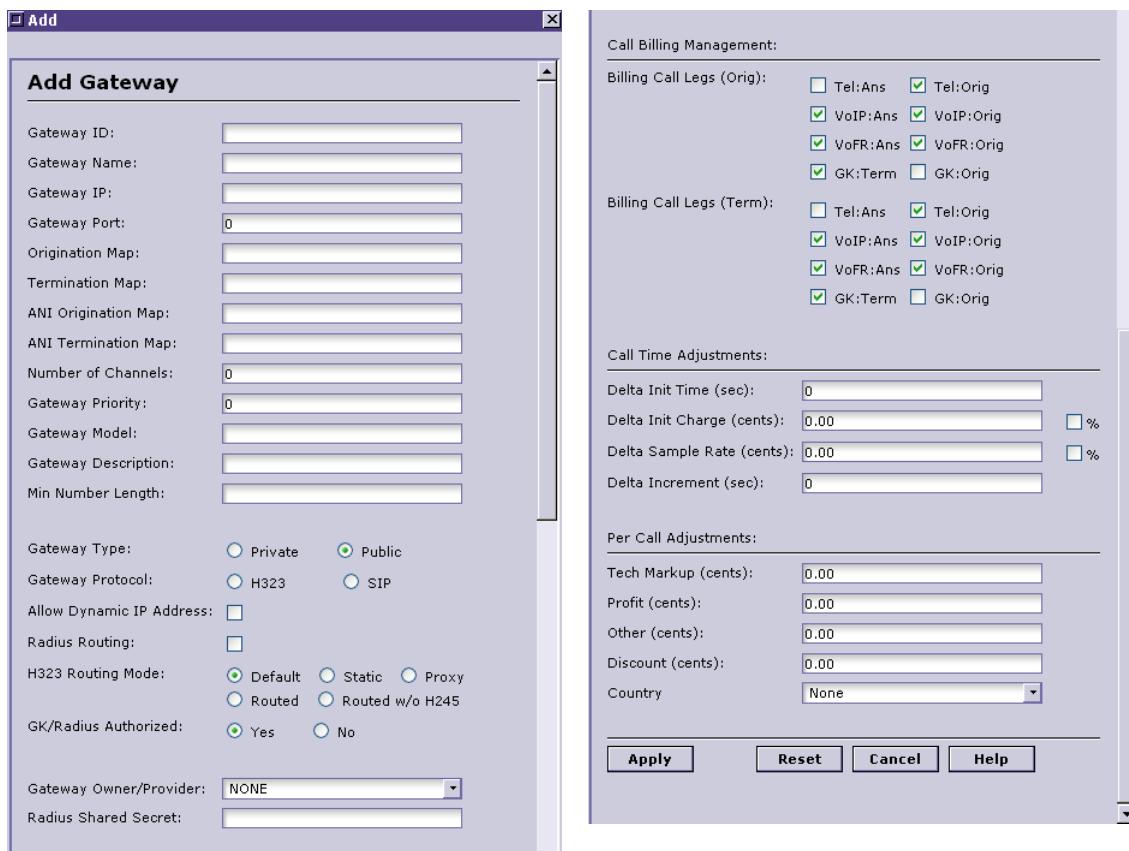


The screenshot shows the Cisco CallManager Navigator interface. The title bar reads "Navigator: \MasterConsole\Route Management\Gateways". The left pane displays a tree view of the configuration hierarchy under "MasterConsole", including "System Configuration", "Interface Customization", "Account Management", "Route Management" (which is expanded to show "Global Route Settings", "Routes", "Routing Tables", "Prefix Routing", "Gateways" - this item is selected and highlighted in blue, "Gatekeepers", and "ASR Route Switching"), and "File", "Edit", "View", "Help" menu options. The right pane is titled "Gateways" and contains a table with the following data:

EP ID	Gateway Name	Gateway IP /	Type
LOLO	LOLO	1.2.3.4:88	Public H323 GW
dummygw	dummygw	127.0.0.1	Public H323 GW
GW1T	prov01 termination	127.0.0.1	Public H323 GW
INTERNAL_ROUTING	INTERNAL_ROUTING	127.0.0.1	Public H323 GW
reseller-agent	reseller-agent.com	127.0.0.1:1	Public H323 GW
PC-PC-H323	PC-PC-H323	127.0.0.1:22	Public H323 GW

**Figure 1-27 Gateways List**

**Step 2** Select **Edit>Add Gateway**. The Add Gateway dialog appears:



**Figure 1-28 Add Gateway Dialog, All Fields Displayed**

---

**Note** Use the scroll bar to navigate to view all parameters.

---

**Step 3** Set the relevant parameters:

- Gateway ID, which must be unique
- Name
- Gateway IP address
- Port assignment. Here the default is ‘0’. If this is used, then by default the gateway will use Port 1720 for H.323 communication (traffic) and Port 5060 for SIP protocol traffic.
- Origination and Termination map definitions (if relevant)

---

**Note** Mapping is used to normalize call origination/termination information and create compatibility with international standards. The Custom Modules chapter and Custom Maps section contains information on this important function.

---

- Number of channels (if none, enter ‘0’) - total number of calls/ports that the gateway can accept.

- (g) Gateway priority. If set, establishes the endpoint (EP) priority in relation to additional endpoints for the same area code within the same routing table.
- (h) Gateway model and description
- (i) Minimum number length
- (j) Gateway type (private or public). “Public” is the right choice. Setting “private” excludes an endpoint from all routes.
- (k) Gateway protocol (H.323 or SIP)
- (l) Dynamic IP address (enable, if used)
- (m) Radius routing (only relevant if GK/Radius Authorized is set to ‘yes’ below)
- (n) H323 Routing mode: This the mode used by the VoiceMaster gatekeeper to route traffic from *this* gateway to the second termination device involved in a call.

If, for example, you select *Routed* mode as the active option, this means that this gateway and its ‘partner’ termination device will set up a communication channel between them to enable the call. Set *Proxy*, and all calls involving the gateway are routed through the VoiceMaster.

- (o) GK/Radius authorized (yes/no)
- (p) Gateway Owner/Provider (name)

---

**Note** You must name the gateway owner in order to continue setup at the Prefix Routing step which follows this one. **Failure to define the owner/provider prevents the system from adding the gateway to the Prefix Routing list.** (Configuring Prefix Routing is one of the core phases of setting up the routing infrastructure.)

---

- (q) Radius Shared Secret (password). Assigned if the gateway will employ Radius.

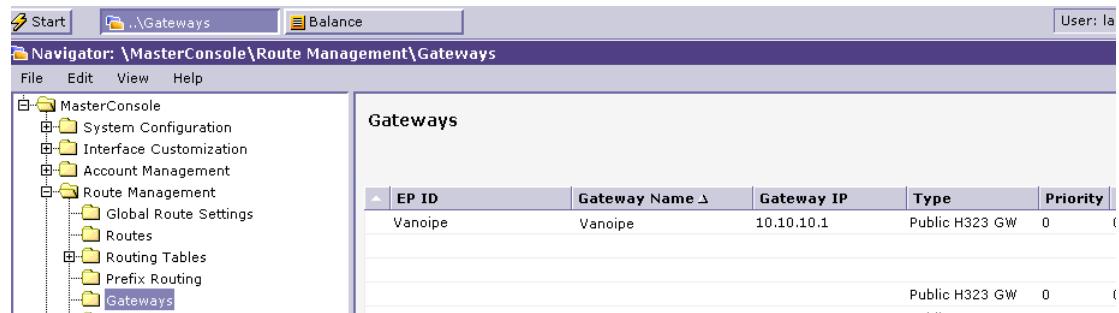
---

**Note** Radius Shared Secret must be set to 1) set up real-time billing for calls through the gateway, 2) activate Interactive Voice Response on the gateway (for prompting user call authentication). Without real-time billing administration, you must configure a CDR collection schedule to deliver billing records from gateways **not** configured for Radius.

---

- (r) Call Billing Management (Billing Call Legs). Call Billing settings determine which ‘legs’ of a call are billed. Select all billable legs.
- (s) Call Time and Per Call Adjustments. Define (optionally) additional charges on calls to the gateway.

**Step 4** Select **Apply** to save entries and add the provider gateway to the Gateways list.:

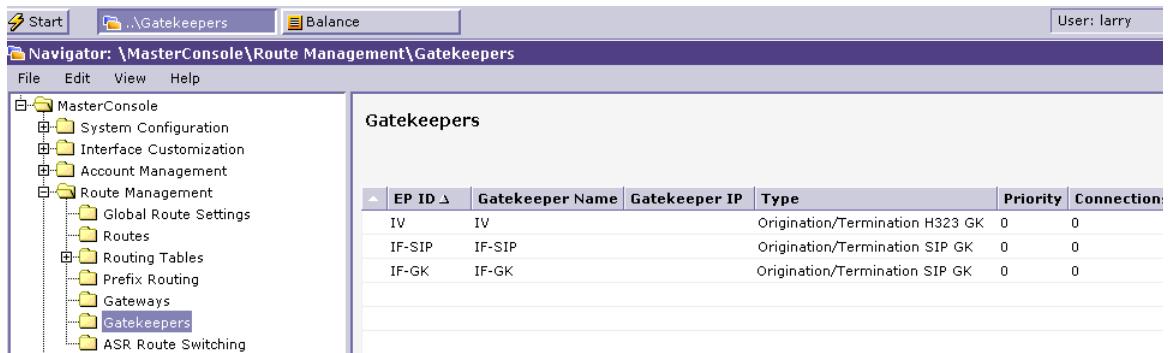


**Figure 1-29 Gateways List**

### Add Provider Gatekeeper

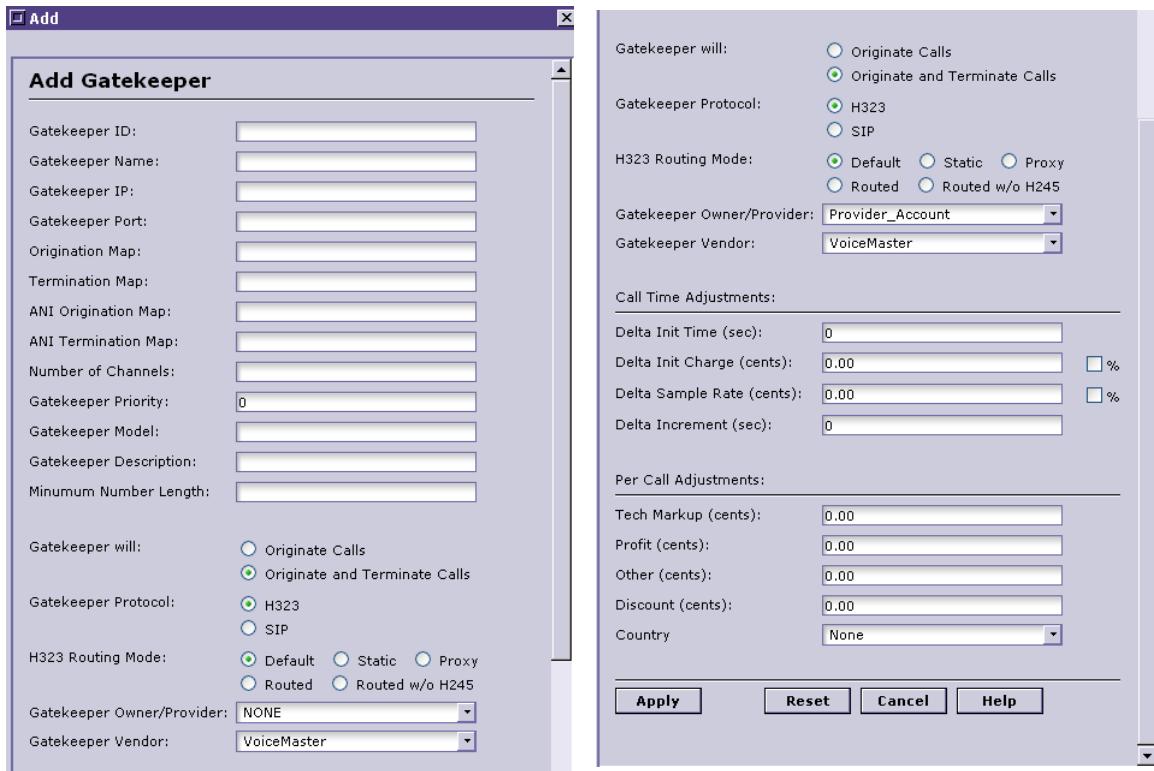
To add a *gatekeeper* as the provider device, follow this procedure:

- Step 1** Select **Route Management>Gatekeepers**. The Navigator reflects the selection:



**Figure 1-30 Route Management: Gatekeepers List**

- Step 2** Choose **Edit>Add Gatekeeper**. The associated dialog is displayed (it is one box, but two illustrations show all editable fields):



**Figure 1-31 Add Gatekeeper Dialog (Full View)**

- Step 3** Enter all relevant field data/parameter settings:
- Gatekeeper ID (must be a unique string)
  - Gatekeeper Name
  - Gatekeeper IP address
  - Port assignment. This is an optional setting, in that the default is set to '0', which sets up pre-assigned port usage for both H.323 (port 1729)
  - Origination map definitions, as appropriate (enter if mapping exists to translate call information for normalization purposes)
  - Number of channels ("0" is default) - number of calls that can be accepted by the gatekeeper.
  - Gatekeeper priority ("0"), model and description
  - Minimum number length
  - Gatekeeper role definition:
    - Originates calls; or
    - Originates and terminates calls
  - Gatekeeper protocol (H.323 or SIP)

(k) Gatekeeper owner/provider and vendor descriptions (**defining the owner is essential - failing to do so means that the device will not appear in the Prefix Routing list**).

(l) Call time adjustments (as desired)

(m) Per call adjustments (as desired)

**Step 4** Select **Apply** to save changes and add the provider gatekeeper to the Gatekeepers list.

## Prefix Routing

Prefix Routing is the VoiceMaster term for assigning area codes to provider termination endpoints. Endpoints associated with specific area codes are used in calls to the designated area codes.

The area codes available for assignment to an endpoint are drawn from a pool created when Provider Rates are configured. Each rate is associated with a specific area code, so importing a group of rates imports multiple area codes. Adding rates manually adds the available area codes (per provider) one at a time.

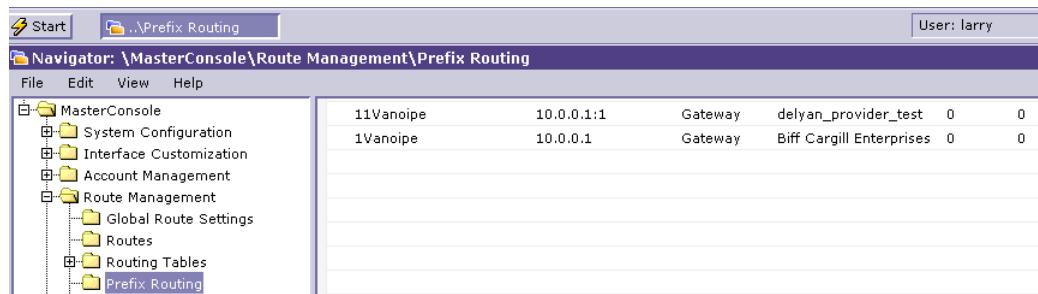
---

**Note** During Prefix Routing, you select specific codes to assign to a termination device. There is no requirement to assign **all** available area codes. Available area codes not assigned to a device may be assigned at any point chosen by the Administrator.

---

Follow these instructions to configure Prefix Routing:

**Step 1** Select **Route Management>Prefix Routing**. View the Prefix Routing list, which shows all provider termination devices added to the system:



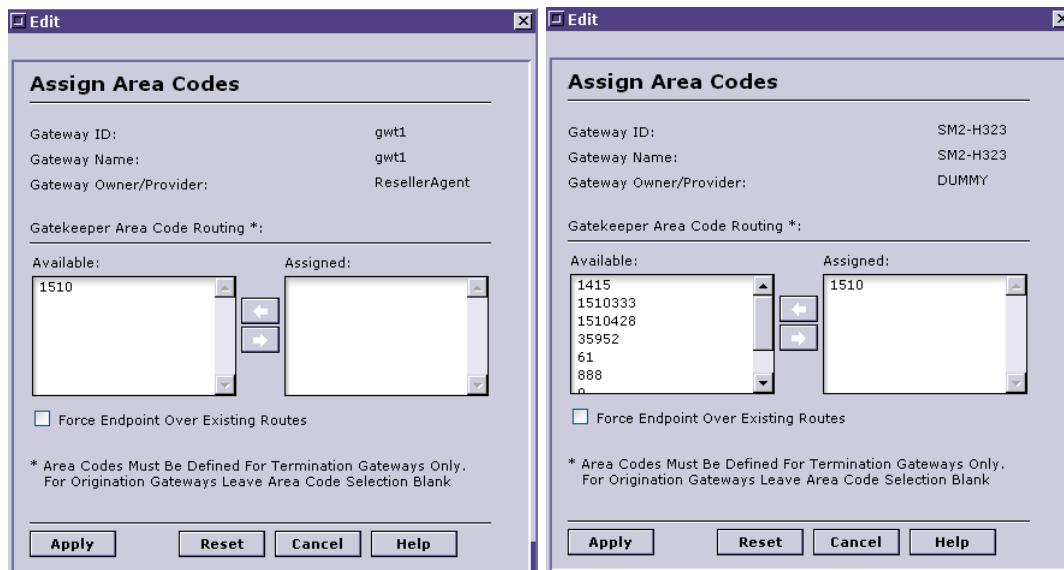
**Figure 1-32 Prefix Routing List**

**Step 2** Select the specific device to which you will assign available provider area codes.

---

**Note** If an expected entry does not appear, this may mean that you did not correctly identify the provider during the Add Provider Device procedure.

---

**Step 3** Select Edit>Assign Area Codes.**Figure 1-33 Assign Area Codes to Gateway**

- Step 4** Assign an area code: select the desired code, click the right arrow. Figure 3-17 shows the ‘before and after’ of code assignment to the designated gateway.
- Step 5** Assign any addition codes to the device.
- Step 6** Click **Apply**.

The foundation for route tables creation is laid.

## Configure Routing Tables (Routes)

The termination devices configured in previous sections form a reservoir of origination and termination endpoints. They enable the administrator to build a route, setting rules (priorities), and assigning customers and termination devices to the route.

---

**Note** A VoiceMaster *must* include the Custom Routes module in order for the Administrator to create routes. Otherwise, all calls are routed via the System Route.

---

On creation of a route, all information is stored in the Routing Tables, which include all custom routes *plus* the default system route.

To configure a routing table:

- Step 1** Open the Console (login) and the Navigator (if necessary).
- Step 2** Select **Route Management>Routes**. View the Routes List window. In Figure 3-18, just the default (system) route appears, as we assume this is the first custom route configured.

## Configure Routing Tables (Routes)

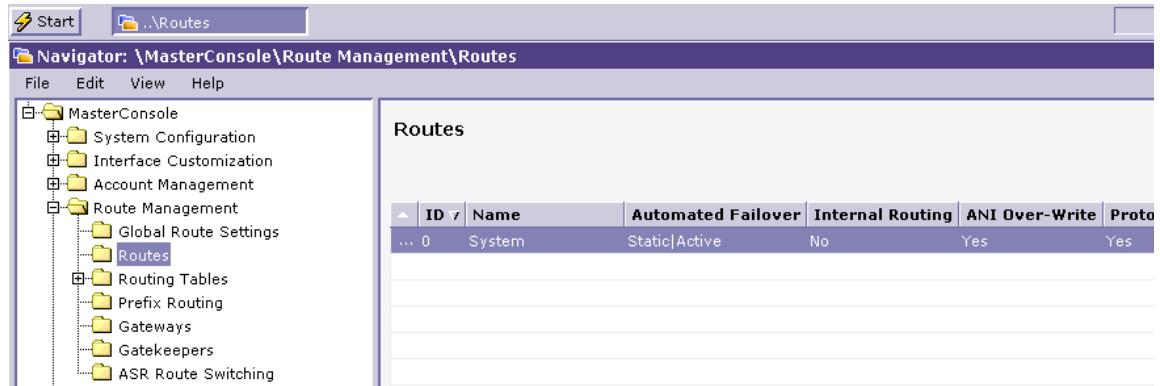


Figure 1-34 Routes List

**Step 3** Choose **Edit>Add Custom Route**. This dialog is displayed:

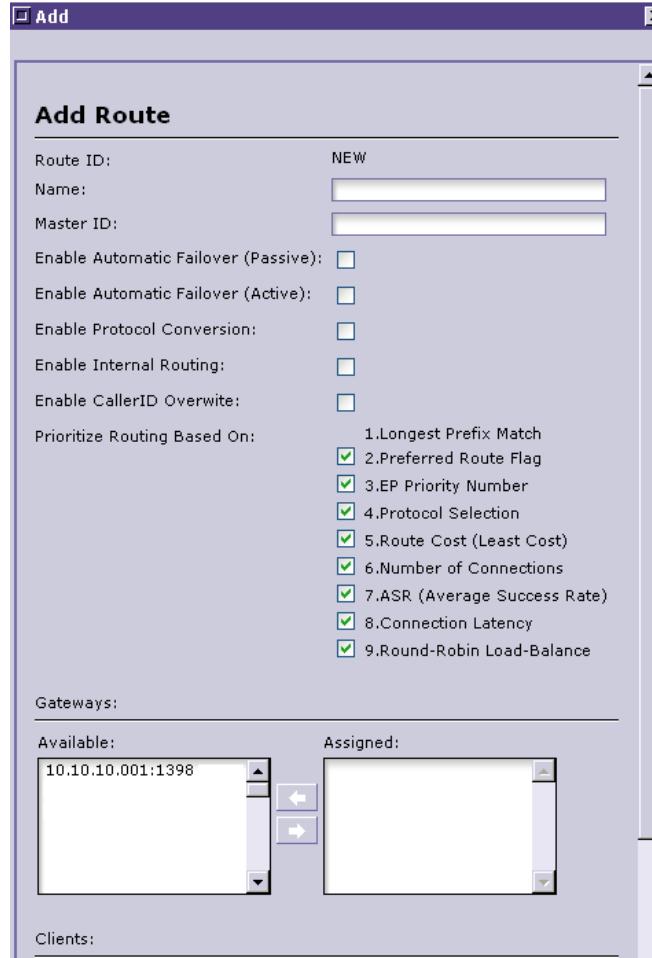


Figure 1-35 Add Route Dialog

**Step 4** Enter a name.

**Step 5** Assign a Master ID to the route. The Master ID defines the route *owner*. Failure to enter a Master ID produces a default of '0' and the system relates to the route as a system route.

---

**Note** For the Managed Services implementation, specific clients' Account IDs would be assigned in the Master ID field. The configured route will apply to the associated client group. [Chapter Ten: Special Implementations](#) covers the Managed Services scenario.

---

**Step 6** Enable any of the available routing policy parameters:

- **Automatic Failover.** Triggers failover (redundancy) to alternate routes in case the primary route fails, which happens when route devices (components) experience errors.

---

**Note** The global Route Failover settings must first be configured (System Configuration>System Settings>Route Failover Configuration). See the following chapter for more on configuring the general route failover settings and Chapter Seven for more on route management as a whole.

---

- **Internal Routing.** Set this parameter to enable the routing of calls to termination devices registered to the VoiceMaster (the VoiceMaster is the 'owner' of the terminating endpoint). See [Chapter Six: Route Administration](#), for additional information on Internal Routing functionality.
- **Caller ID Overwrite.** If enabled, this setting prevents a called party from viewing the caller ID on his receiver pad. (Requires Caller ID module to be implemented.)

**Step 7** Set Priority Routing. These are the settings that the system checks, one-by-one, when selecting the specific devices (and path) to use for route-defined calls. The system uses an algorithm which looks for a 'condition match', then shuttles the call accordingly. It examines each condition associated with every checked parameter:

- Longest Prefix Match (default-inclusion)
- Preferred Route Flag
- EP Priority Number
- Route Cost (Least Cost)
- Number of Connections
- ASR (Average Success Rate)
- Connection Latency
- Round-Robin Load Balance

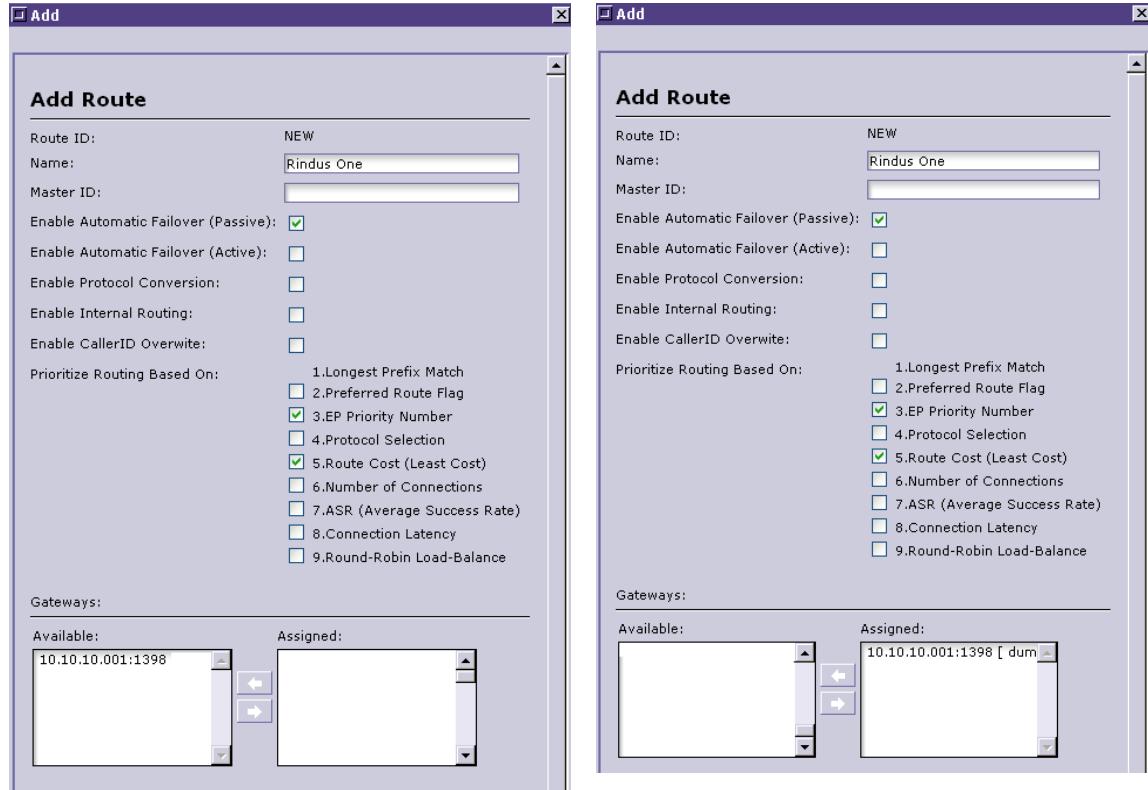
---

**Note** Each parameter and its routing function is discussed in greater detail in the Routing Administration chapter. Again, the selection algorithm works on the basis of 'first condition match found' and specific routing decisions are based on this.

---

**Step 8** Assign gateways to the route. Navigate to the Gateways Available/Assigned boxes in the lower part of the dialog box.

## Configure Routing Tables (Routes)



**Figure 1-36 Gateways Assignment**

- Step 9** Select gateways from the Available box and move them to the Assigned box. In Figure 3-20, two of five possible gateways are assigned to the new route.
- Step 10** Now assign one or more clients to the route by moving them from the *Clients* available list box to the Assigned box.
- Step 11** Select **Apply** to save the newly created route.

The route is added to the Routes list and a corresponding entry is created in Routing Tables.

ID	Name	Automated Failover	Internal Routing	Area Codes
46	Rindus One	Static	No	No
45	sip1c	Static Active	No	Yes
44	sip1b	Static Active	No	Yes

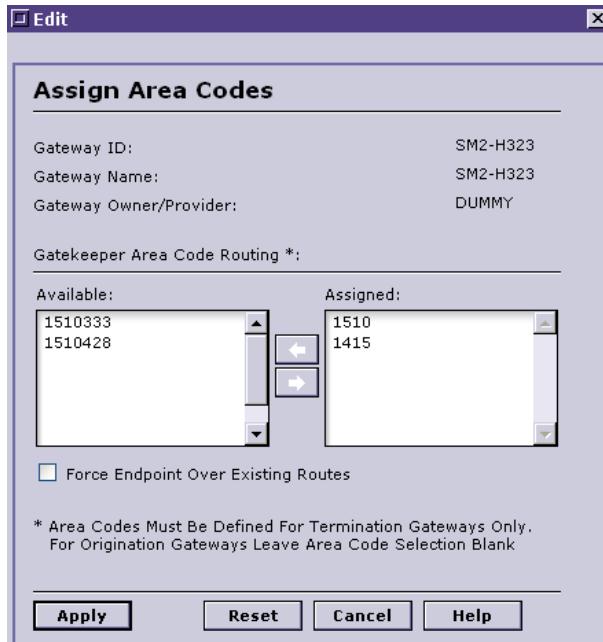
**Figure 1-37 'Rindus One' Added to Routes List**

### Assign Area Codes

At this stage the Administrator assigns all area codes associated with specific provider endpoints to the selected routing table.

To add these area codes:

- Step 1** Open the Navigator if it's not currently open.
- Step 2** Select **Route Management>Prefix Routing**.
- Step 3** Select the desired provider gateway from the Prefix Routing List. (These are gateways assigned to the route.)
- Step 4** Select **Assign Area Codes**. The relevant dialog is displayed:



**Figure 1-38 Assign Area Codes**

- Step 5** Select all available area codes and assign them.
- Step 6** Select **Apply** and the codes are assigned. gateways. *This ensures that these codes are associated with the endpoint and calls to these area codes go to the endpoint.*

## Billing Configuration

Configuring billing is the next phase of creating the VoIP service foundation. Billing configuration applies billing rates to designated clients - is a vital building block *and* an essential component of VoiceMaster.

---

**Note** As with other functional realms within VoiceMaster, the specific billing configuration/management capabilities will depend on the number of add-on modules integrated into the system. Certain functions are dependent on the inclusion of specific modules. Refer to the Modules Inventory (**System Configuration>Miscellaneous**) for a listing of system modules. Contact SysMaster for more information and additional module trials or purchases.

---

The basic billing configuration process necessitates two sets of actions:

- Billing Rate Table creation
- Billing Rate configuration.

There is a distinction between *billing* and *provider* rates. The latter reflect your network provider's charges, to be carried by any VoIP service that contracts to use the provider's bandwidth/devices. Billing rates are simply the universe of the various rates that you assign to different clients and subscribers.

The two are connected in that billing rates configuration should take into account the expenses that derive directly from the incorporation of provider rates into the system (.

---

**Note** In some cases, billing rates may be directly tied to (or based on) a provider's rates. In one application of VoiceMaster billing functionality, rates for targeted subscribed can be *bound* to provider rates, creating a one-to-one dependency.

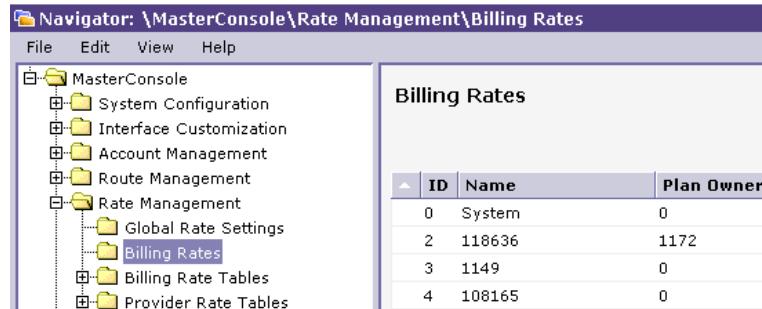
---

Keep in mind while configuring billing rates: this is the real source of profit and revenue for a VoIP service business such as yours. Rates set should integrate all infrastructure costs and allow for enough revenue to produce essential profit.

### Create Billing Rate Table

Complete this procedure to create a billing rate table:

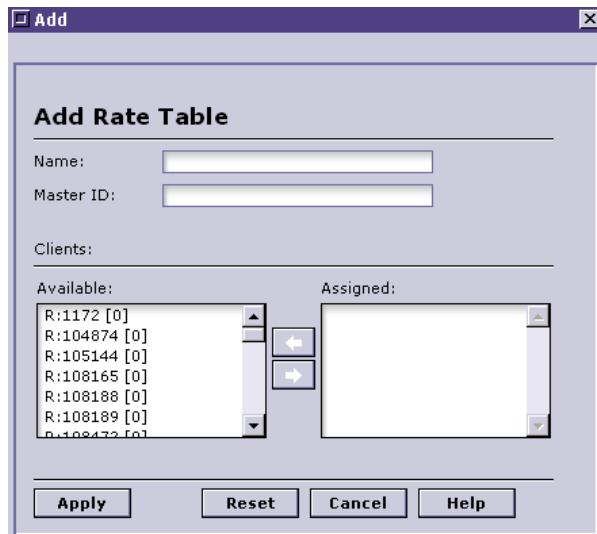
**Step 1** Select **Rate Management>Billing Rates**. The Billing Rates List is opened:



ID	Name	Plan Owner
0	System	0
2	118636	1172
3	1149	0
4	108165	0

**Figure 1-39 Billing Rates List**

**Step 2** Choose **Edit>Add Rate Table**. The necessary (and correct) dialog is presented:



- Step 3** Assign a Rate Table name, preferably one that is associated with rate characteristics and/or client assignments.
- Step 4** Provide a Master ID in the next field (optional).
- Step 5** Assign clients who will be billed according to rates set for the new rate table. (This will happen very soon, in the very next section.) Select each desired client from the Available box, and move the client to the Assigned box. Repeat for any additional target clients.
- Step 6** Select **Apply**. As the dialog closes, Voicemaster adds the new rate table to the Rates list and creates a Rates Table subfolder using the name you assigned.

## Configure Billing Rates

The second aspect of billing configuration is to configure the actual billing rates. Configuring the rates has its own branching, though, depending on how you set billing rates policy for a group of clients.

The standard method is to add a billing rate, defining area code, location and rate parameters.

It is also possible to copy rates from a provider and effectively bind a subscriber's rates to a provider. Calls to the provider's destination are then bound to provider-set rates as long as the binding remains. The Administrator can always 'unbind' such rates by replacing the provider rates with rates configured for the same destinations.

---

**Note** Unbinding is performed via a 'toggle' option in the Bind dialog box. If you select "Remove Binding" this is effected.

---

A variation of this second option is *global binding* to a particular provider. This path is followed in instances when an Administrator wishes to bind subscriber rates to *all* rates set by a particular subscriber to all destinations serviced by that subscriber.

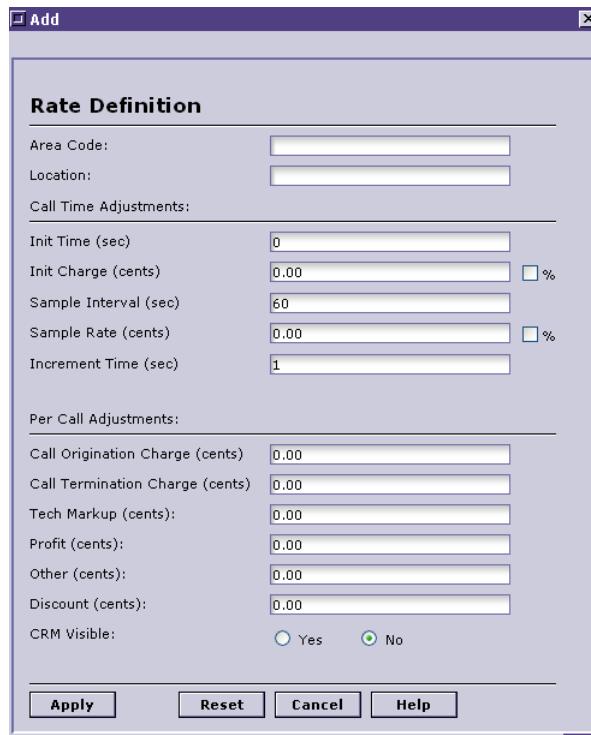
### Add Billing Rates

To add a billing rate:

- Step 1** Select **Rate Management>Rate Tables**.

**Step 2** Select the newly created Rate Table folder.

**Step 3** Select **Edit>Add Rate**. View the dialog:



**Figure 1-40 Rate Definition Dialog**

**Step 4** Set the destination area code.

**Step 5** Define the location called - usually a country.

**Step 6** Set call time adjustments to apply to the rate:

- Init Time - specifies the total interval for which to apply the different rates that define the call
- Init Charge - one time charge to apply to the call, activated when the Init Time entry specifies
- Sample Interval. Measure of how often sample rate is to be applied.
- Sample Rate. Cyclical rate to be charged each time the interval is reached.
- Increment Time. Measure of last portion of call, used to calculate final interval.

**Step 7** Set per call adjustments.

- Call origination charge. A special charge levied for call origination.
- Call termination charge. Another charge fixed to call end.
- Tech Markup, Profit, Discount and Other. Special charges to account for VoIP infrastructure costs

---

**Note** All charges are optional, to be set at the Administrator's discretion.

---

**Step 8** CRM Visible. Enable this option to make the billing rates visible on the subscriber (CRM) web site.

**Step 9** Click **Apply** to enforce the parameters assigned in the previous steps. The new rate is added to the Rates List for the selected rate table.

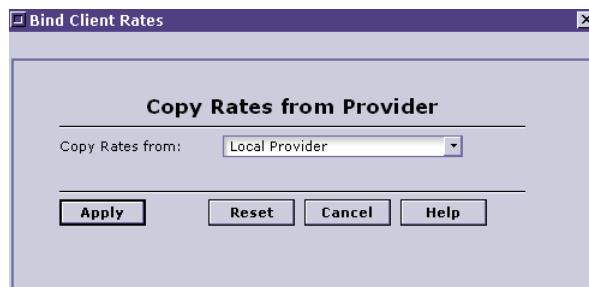
### Copy Rates from a Provider (Binding)

The alternative to adding a new rate is to copy rates from a provider. To do this, and bind subscriber calls to the relevant destination area codes to the provider rate, follow these instructions:

**Step 1** Select **Rate Management>Billing Rate Tables**.

**Step 2** Select the desired rate table folder from the Billing Rate Tables folder.

**Step 3** Now select **Edit>Copy Rates from Provider**. This interactive dialog is presented:



**Figure 1-41 Copy Provider Rates**

**Step 4** Select the pulldown menu and select the provider whose rates you intend to copy.

---

**Note** This will bind clients to all calls made to destinations serviced by the provider's termination gateway. (Calls to destinations serviced by the provider are billed according to provider rates.)

---

**Step 5** Select **Apply**. The provider rate is added to the Rates List for the selected table.

### Global Provider Rate Binding

A third billing rate configuration option exists, for binding *all* calls to a specific provider *for all area codes serviced by that provider*.

---

**Note** This configuration option is usually reserved for Managed Services scenarios, in which the administrator wants to apply a particular provider's rate structure to all subscriber calls over assigned routes (that use the provider's termination gateways).

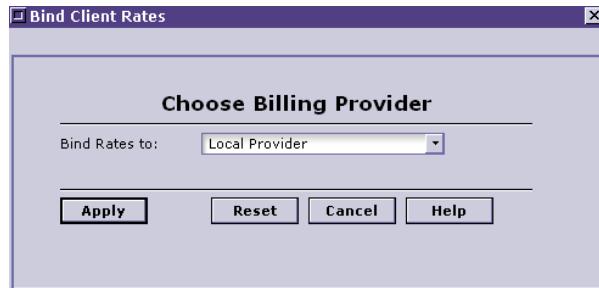
---

To enforce this:

**Step 1** Select **Rate Management>Billing Rate Tables**.

**Step 2** Select the desired rate table folder from the Billing Rate Tables folder.

**Step 3** Select **Edit>Bind to Provider Rates**. View the dialog:



**Figure 1-42 Bind Provider Selection**

**Step 4** Select the pulldown menu and select the desired provider.

**Step 5** Select **Apply**.

---

**Note** In this case, the rates for the billing provider appear simultaneously on the Rates List, replacing all previous rates. This is a global configuration option.

---

Congratulations! The full infrastructure for basic VoIP service is now in place. The last phase is linking configured routes and rates to active service subscribers.

## Activating VoIP Service: Linking Routes, Rates and Subscribers

We have reached the stage at which the VoIP infrastructure is linked to active service subscribers. We begin with configuration of subscriber accounts.

### Create Subscriber Account

The first step in this final phase is to create account(s) for subscribers to whom to apply the now-configured routes and rates:

**Step 1** Select **Account Management**.

**Step 2** Select the folder for the type of account that will describe the new subscriber(s):

- End User Accounts
- Wholesale Accounts
- Reseller Accounts
- Corporate Accounts
- Commission Agent Accounts

Your choice must be one of these folders. For a specific end user, select the first folder (End User Accounts). For a *group of subscribers* associated with a particular client group, pick that client group.

**Step 3** Select **Edit>Add Account** (the Edit menu option is the same no matter the account type chosen).

**Step 4** View the account creation dialog:

**Figure 1-43 Add New Client/Subscriber Account Dialog**

- Step 5** Assign username and password, to be entered by the user when accessing online account information (about his own account).
- Step 6** Select user type. Open the drop-down menu to select the type that accords with the desired client/subscriber account (this should be the same as the folder selected in Step 2).
- Step 7** Enter company name, if relevant (will not apply to ‘Active User’ type).
- Step 8** Enter the new client/subscriber contact information, starting with full name and continuing to E-mail and phone information.
- Step 9** Assign a gateway for the account. This is the specifically assigned gateway for all calls from the account. (This will prevent calls from the designated accounts from being routed over alternate gateways.)
- Step 10** Specifies Caller ID. This becomes the authentication number for calls made by the subscriber. (The number must match this entry for outgoing calls to be authenticated.)
- Step 11** Set an IP address for authentication. If this is set, the system will authenticate this address before permitting a call.
- Step 12** Set (overall) Authentication method. Use the pulldown menu to set an authentication method. That chosen decides the exact check (or combination of checks) required to authorize calls from the account.

**Note** The method selected should fit an administrative security approach. Whether you select a single or multiple authentication methods, choose that which best fits system security needs.

---

- Step 13** Select currency type (used by VoiceMaster to charge the new account).
- Step 14** Set Redirect and DNIS numbers. The numbers entered in these fields will be used to redirect calls authorized by DNIS authorization.
- Step 15** Set balance expiration: the number of days for which the account is active (and during which calls are permitted).
- Step 16** Set E-mail statement parameters. Choose any box that corresponds to subscriber-related action of which you wish to inform the subscriber. If such actions occur, he will be notified via E-mail address specified.
- Step 17** Enable or disable credit card payment by the subscriber.
- Step 18** Select **Apply**. The settings are saved and the new account is created. An entry for the account appears on the Account Management page (pane). *Record account information, an important step to retrieval of account records in the future (next section)!*

**Note** The specific type of client/subscriber account is indicated by the window heading. The account can now be modified (or deleted) at any point.

---

## Assign Route to Subscriber Account

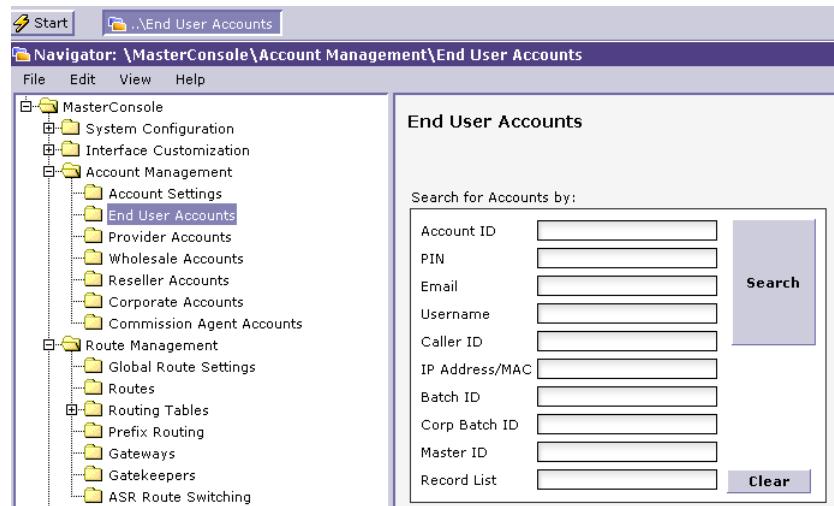
Routes have been created and added to the appropriate routing tables. Provider and billing rates have been established, and subscriber accounts now exist. It is time to assign a route to the configured subscriber account.

**Note** To simplify the following procedural explanation, we will assume that the subscriber account type created in the previous section was **End User**.

---

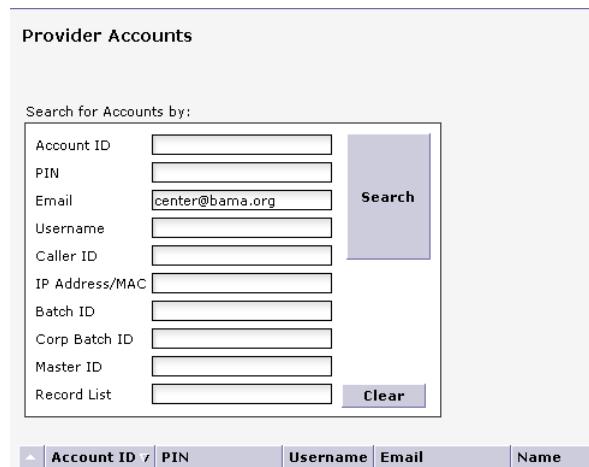
To do so:

- Step 1** Select **Account Management>End User Accounts**.
- Step 2** Locate the specific account using the entry fields on the End User account window. Refer to the account information and enter any search parameter to locate the (Type in a parameter and then select **Search** to retrieve it).



**Figure 1-44 End User Account: Search Options Displayed**

**Step 3** The account will be retrieved, as shown here:



**Figure 1-45 End User Account Retrieved**

**Step 4** Select the account record (it is visible beneath the Search dialog).

**Step 5** Select **Edit Account Info** (either from the Edit menu or from the options list which appears when you select the retrieved account):

## Activating VoIP Service: Linking Routes, Rates and Subscribers

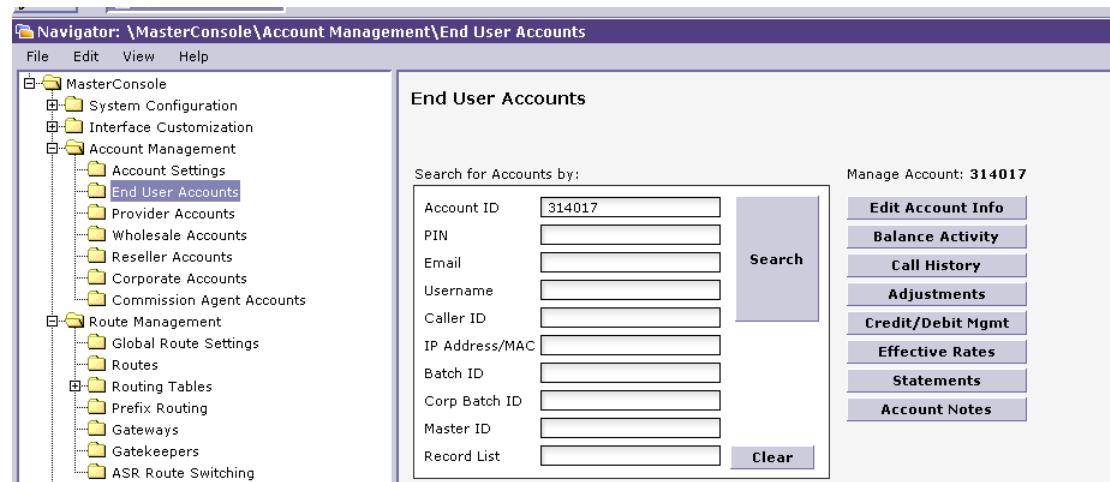


Figure 1-46 Account Retrieval: Account Selection Options

**Step 6** View the Edit dialog that appears, containing the configured account data:

The 'Edit' dialog box is titled 'Edit Account Information'. It contains a list of account configuration fields with their current values:

Field	Value
AccountID:	1857356
PIN:	1*87#
Username:	larry
Password:	larry
User Type:	Active User
Rate Plan:	1 [21]
Route Plan:	delyan [31]
ISP Rate Plan:	System [0]
Custom Service Plan:	postpaidtest [5]
Signup Plan:	NONE
Caller ID Distribution:	NONE
Content Plan:	NONE
Company:	
Full Name:	Larry Aych
Address:	123 Count Court
City:	Centerville
ZIP:	
State:	Alabama
Country:	United States of America
Email:	
Phone:	
Speed Dial:	
Gateway:	Car310
Caller ID (ANI):	
IP Address:	
Authentication Method:	IP ADDRESS ONLY
Currency:	UNITED STATES OF AMERICA

Figure 1-47 Retrieved End User Account - Edit Dialog

**Step 7** At the **Route** field, open the pulldown to select the route from the list of existing routes. View the available route and select one to apply to the subscriber.

---

**Note** Logically, you may select the route created earlier in this chapter. However, you can select any configured route to apply to the subscriber (assuming the presence of the Custom Route module).

---

- Step 8** Select **Apply**. The subscriber (end user) account is updated with the route assignment enforced as selected Step 7. *Alternately, do not apply changes if you are ready to set a billing rate for the subscriber. If so, read the Note in the next section to apply a rate now.*

## Assign Billing Rate to Subscriber Account

The final step in this implementation phase of VoIP service configuration is assigning a billing rate to the subscriber account (created, configured and with a route assigned).

Follow this procedure to complete billing rate assignment for the account:

---

**Note** The billing rate can also be applied immediately after selecting a route. If you have set a route and the Edit Account Info dialog is open, skip to **Step 4** in the following procedure and read Steps 4-7. Follow the instructions.

---

- Step 1** If you have navigated away from the **Accounts Management>End User Accounts** folder, select it again.
- Step 2** Locate and select the same end user account created earlier.
- Step 3** Select **Edit Account Info**.
- Step 4** When the dialog is displayed (Figure 4-29), open the pulldown menu for the Billing Rate Plan field.
- Step 5** Select the desired Billing Rate. This will likely be the one you have created during Billing Configuration, but can be any of the available rate plans the pulldown displays.
- Step 6** Optionally, add a Custom Service or Signup Plan if those options are relevant to this subscriber.
- Step 7** Select **Apply**. The settings are saved.

Assuming the subscriber has a prepaid, positive balance and the network is functioning smoothly, VoIP calls are now possible. Your VoIP service is in business!



# Chapter 4: VoiceMaster Administration

---

## In This Chapter

In this chapter, we describe the general administrative functions that make VoiceMaster configuration and management possible. We describe the purpose and roles of the various functions and the related administrative actions that apply these functions to an active VoIP service.

We assume that your VoiceMaster implementation contains essential gatekeeper, routing and billing functionality. If a particular explanation relates to functionality not part of your system, please skim it. (Console folders and functions are not present on the Administration Console if your system does not include them.)

---

**Note** We differentiate between add-on modules (e.g., Firewall Filters) and Custom Modules (CDR Collection Module, for instance). If you have Custom Modules, refer to Chapter 11 for description and procedures related to a given module.

---

The key chapter sections are as follows:

- Network Configuration. This section explains the three included network configuration functions and includes configuration procedures for each.
- *System Users Configuration*. This section describes the various VoiceMaster administrative roles and how to configure them.
- *System Settings* is a broad functional category that includes general configuration, gatekeeper configuration, PIN configuration, database backup, managed services, route failover and special VoIP protocol settings.
- *Billing Settings*. Another set of generic functions, this time pertaining to VoiceMaster billing configuration and management. Includes Call billing and IVR settings.
- *Payment Methods* presents the configuration of a range of customer-available payment methods for customer account activity.
- *Security*. A critical aspect of any network administration environment. We look at firewall filters, fraud detection, system alerts and additional measures.
- Fault Tolerance. This is a powerful set of administrative tools and functions that enforces fault tolerance (redundancy) at all system levels. Relies on the use of active and standby servers, essential to implementing both kinds of explicit redundant functions:
  - MD RAID Mirrors (both hardware and software), at the level of operating systems.

- System Redundancy. The replication and synchronization of all system data above the operating systems level.
- *Interface Customization.* How to customize both the Administration Console and the CRM web sites that subscribers access to establish and manage VoIP service subscription.
- *Miscellaneous functions.* Company information, module inventory, and configuring a network printer.

## Network Configuration

VoiceMaster is a system with one or more servers and (typically) multiple IP addresses. It is an Internet node - accessible to other nodes on the public Internet and ultimately able to perform its sophisticated VoIP functions because it is a configured network device (or set of devices).

In other words, all of the power of VoiceMaster and its gatekeeper, routing and billing capabilities must be utilized in the ‘real world’ of the Internet. Network configuration makes this possible.

---

**Note** We have discussed the basic network settings in the context of VoiceMaster initial configuration. These sections expand this discussion to include all network configuration functionality.

Note also that certain settings - IP address, gateway and network mask - may have been configured during the initial configuration process. This is true if you set up the VoiceMaster over the network.

---

Network configuration divides into three functional areas, each of which is represented on the Administration Console hierarchy as a sub-folder within **System Configuration>Network Configuration**.

- **Server Configuration:** Used to configure general network settings and server roles.
- **IP Address Configuration:** Besides IP address configuration, used to configure common network configuration strategies and connection options.
- **Routes Configuration:** Used to add static routes to a VoiceMaster residing on multiple IP networks.

We discuss each of these network configuration functional groups in turn, including the relevant procedures.

### Server Configuration

Server Configuration is the folder/function used to set the basic, generic network settings for the VoiceMaster server(s). These are the essential parameters that ‘ID’ the server, its domain and related gateway.

They include definitions of the server type - the role(s) it plays within the VoiceMaster system. For instance, a given server may be a routing, payment and processing server or a database server.

---

**Note** Depending on the hardware level that describes your VoiceMaster implementation, a single server may contain all essential system functions, including database. This is the case for Level 1 and 2 systems. For Level 3 systems and higher, multiple servers are included. Because of their inherently greater processing power, these Level 3+ servers divide system functions. Most specifically, the higher level systems include a single server that handles the CPU-intensive database tasks while a separate server is tasked to perform remaining functions.

---

The gamut of server configuration parameters includes:

- **Host Name.** The device name, default-defined as VoiceMaster.
- **Peer ID.** Identifies the system server. This will be used by other network devices (participants) that interact with the VoiceMaster.
- **Serial Number.** Specifies the serial number of the unit for administrative purposes.
- **Web Name.** Names the domain in which the CRM (subscriber) web site resides.
- **Domain Name.** Identifies the domain to which the VoiceMaster device belongs; could be something like ‘company.com’ where an actual company name is used. A domain describes a series of related devices in a geographic network area.
- **NTP Server.** Specifies the IP address or time server host name for time synchronization. Each hour the VoiceMaster and server time settings are synchronized using Network Time Protocol (NTP).
- **Time Zone.** Specifies the time zone of the device as a time offset from the Coordinated Universal Time (UTC). The time offset can be any integer from -12 to +12 to reflect the device’s time zone. -8 for PST, +1 for CET
- **Gateway.** Identifies the IP address of the gateway/router in the VoiceMaster network. The address should be specified in xxx.xxx.xxx.xxx notation, where xxx is a number from 0 to 255.
- **DNS Server.** Specifies the IP address of the Domain Name Server that will resolve domain name conflicts. The address should be specified in xxx.xxx.xxx.xxx notation, where xxx is a number from 0 to 255.
- **Server Type.** Enables the activation of different server types to perform specific, unique system functions. In most cases, each server belongs to a separate physical box denoted by its serial number. If a single physical box contains multiple servers, the same network configuration entries (IP, masks, etc.) will apply to all of them. Available server types are:
  - *Routing Server* - Routes H323/SIP calls, and/or act as a RADIUS server. (It is possible to have multiple routing servers connected to one Database Server).
  - *Database Server* - Acts as Database Server for Routing, Payment, and Processing Server. (Only 1 Server can act as a DB in a group of systems).
  - *Payment Server* - Handles CC payments and host a CRM website. (One server only can act as a Payment Server in a group of systems).
  - *Processing Server* - Runs maintenance tasks on the Database and functions as the master replication server if replication is enabled. (Only one server can be a Processing Server in a group of systems).
- **Server Status** (no Administrator configuration required)
- **Primary MAC** (address) (default-provided)

- **Remote DB IP.** This setting is applicable in cases when your system is based on Level 3/4 hardware, where the database resides on a single server and the routing, payment and processing functionality reside on a second server. The Remote DB IP is set on the routing (payment/processing) server and points to the DB server's IP address (links the two).

**Note** The VoiceMaster device utilizes the following TCP ports:

Gatekeeper: 1721, 1720, 1719, 1718,  
Web server: 80, 8080, 443  
Radius: 1812, 1813, 1814  
Database: 2000

### Add Server Configuration

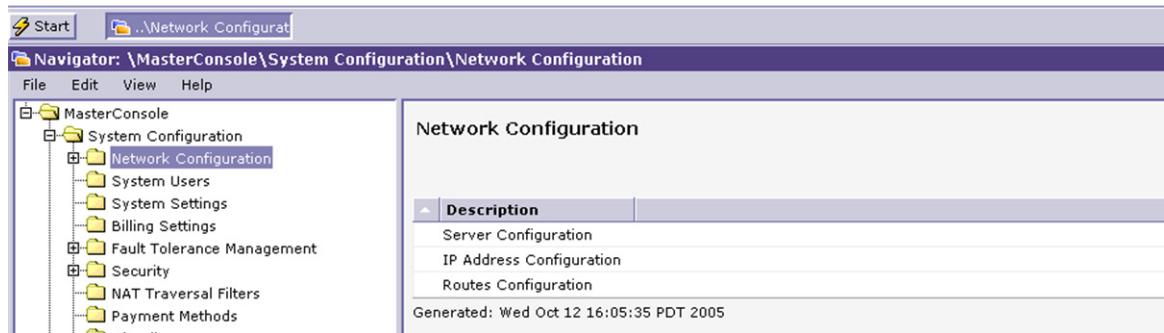
This section includes all steps needed to configure a VoiceMaster server.

**Note** Please refer to the single-page information sheet that came with your VoiceMaster for specific parameter information to be entered during this procedure.

Please keep in mind: VoiceMaster owners whose systems contain Level 1/2 hardware, will configure just one server, while Level 3/4 VoiceMaster owners will configure two (or more) servers. That means executing the procedure more than once.

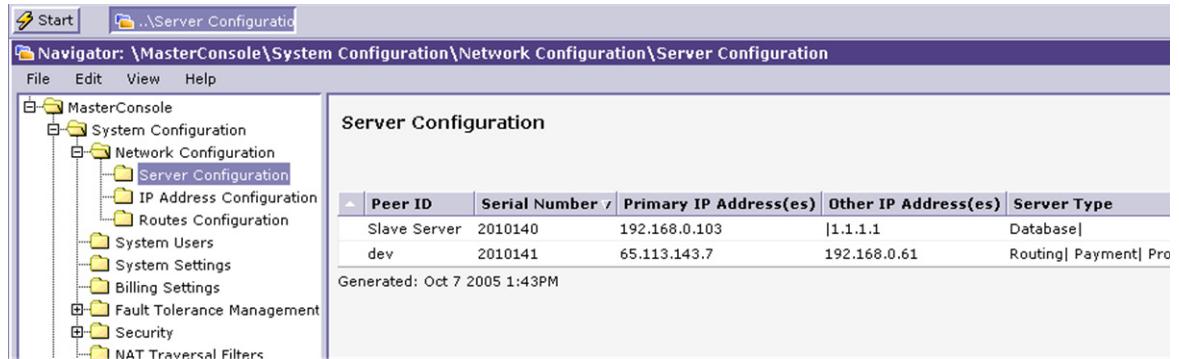
To add a server configuration:

- Step 1** Log in to the Administration Console with your username and password.
- Step 2** Select **Start>Navigator** to open the Navigator.
- Step 3** From the Navigator view, select **System Configuration>Network Configuration**. The Network Configuration window appears:



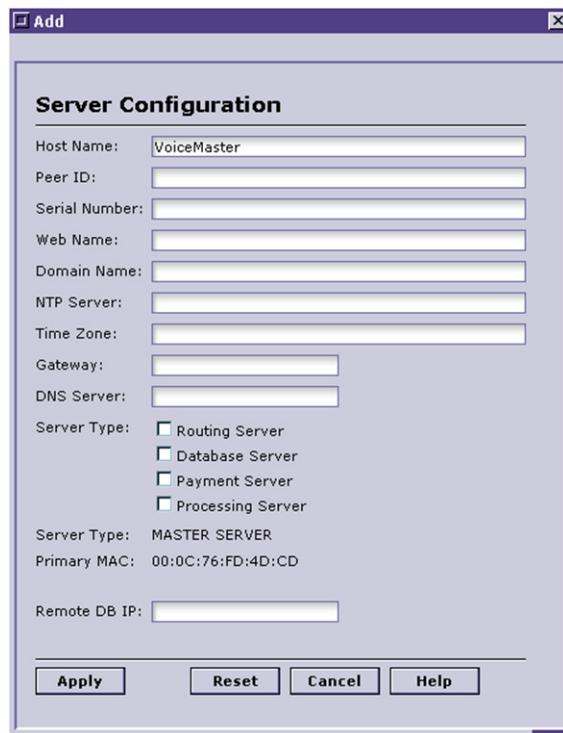
**Figure 1-48 Network Configuration Functions**

- Step 4** Select **Server Configuration** and then **Edit>Open Folder**, and the view changes accordingly:



**Figure 1-49 Server Configuration Underway**

**Step 5** Select **Edit>Add Server Configuration**. The Server Configuration dialog displays:



**Figure 1-50 Server Configuration Dialog**

**Step 6** Begin to define the configuration. Note that **Host Name** is preconfigured (VoiceMaster). Refer to the parameter definitions in the section overview, then define:

- Peer ID
- Serial Number
- Web Name
- Domain Name
- NTP Server
- Time Zone

- Gateway
- DNS Server
- Server Type

**Note** Server Type configuration is a bit tricky. Level 1 and Level 2 hardware owners will check all type boxes. Level 3 and 4 owners will choose Routing/Payment/Processing for one system server, and Database for the second.

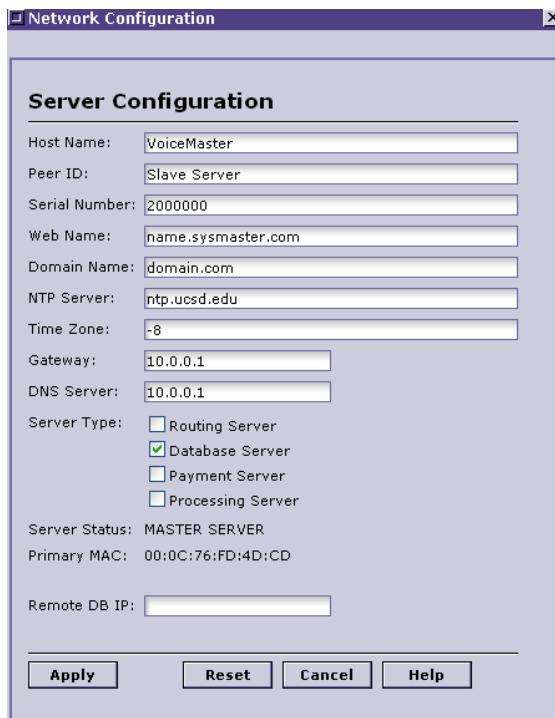
- Remote DB IP

**Step 7** Select **Apply** to save the configuration settings and add the configuration.

### Edit Server Configuration

To modify an existing network configuration, follow these instructions:

- Step 1** Log in to the Administration Console and open Navigator (skip this if Navigator is currently open).
- Step 2** From the Navigator view, select **System Configuration>Network Configuration**.
- Step 3** Select **Server Configuration** and then **Edit>Open Folder**:
- Step 4** Select the server configuration you wish to modify.
- Step 5** Choose **Edit>Edit Server Configuration**. The edit dialog comes into view:



**Figure 1-51 Editing a Server Configuration**

**Step 6** Change any of the fields or check boxes to reflect desired changes.

**Step 7** Select **Apply** to confirm. This saves the network configuration in its modified form.

### Delete Network Configuration

To delete an existing server configuration:

- Step 1** If not currently logged in, do so and open the Navigator.
- Step 2** From the Navigator view, select **System Configuration>Network Configuration**.
- Step 3** Select **Server Configuration** and then **Edit>Open Folder**:
- Step 4** Select the server configuration you wish to delete.
- Step 5** Confirm **OK** at the prompt to delete, or choose **Cancel** to abort the operation.

Once the deletion is confirmed, the configuration is removed.

## IP Address Configuration

IP Address Configuration facilitates configuring the server IP address and numerous related functions.

- **ID.** Default server identification.
- **Serial Number.** Defines which server in a group the public IP address will reside on. Enter the serial number that fits this server.
- **IP Address.** Sets a device IP address. The address should be specified in xxx.xxx.xxx.xxx notation, where xxx is a number from 0 to 255. This is typically the IP address of the ‘slave’ server. It checks the master server (Monitor IP) periodically by pinging it. As long as the master server is active, its address is what other nodes and users see. If the master is down, this IP address is activated.

---

**Note** The public network settings are established during the installation and initial configuration process described in detail in [Chapter Two: VoiceMaster Installation](#).

---

- **Network Mask.** Used to assign a network mask to primary IP Address. The network mask should fit network in which the VoiceMaster platform participates.
- **Devices.** Sets the physical device that the IP Address will reside on.
- **MAC.** Set the MAC address
- **DB Listener.** Tells VM to listen for Database Connections on this IP Address.
- **NAT Network Address Translation** enabled from this interface.
- **VLAN** Used in conjunction with the "VLAN ID" field. Allows the VoiceMaster to report a VLAN ID to switches that support VLANS. The VoiceMaster is then recognized as a VLAN network device.
- **VLAN ID.** The number that assigns the VoiceMaster to a particular VLAN. Only relevant if VLAN is checked.
- **Monitor IP.** The (master) IP Address that is used to monitor network reachability. The VoiceMaster periodically ‘pings’ this IP to affirm connectivity. If the Monitor IP is inaccessible, the VoiceMaster reverts to the IP address in the **IP Address** field above.
- **Activate Condition.** This parameter sets ping status. Options are disabled, no ping (unsuccessful ping) and ping (ping is set and working).

### Configure IP Address

To configure an IP Address, do the following:

- Step 1** If the Console is not currently active, log in and select **Start>Navigator**.
- Step 2** From the Navigator, select **Network Configuration>IP Address Configuration**. The window reflects your choice:

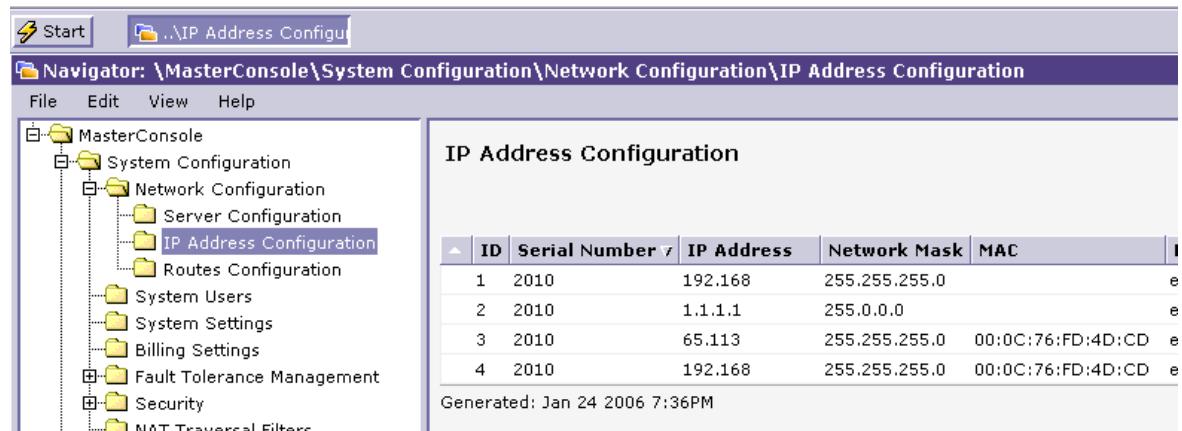


Figure 1-52 IP Address Configuration Begins

- Step 3** Select **Edit>Add Server IP Configuration**. The configuration dialog now displays:

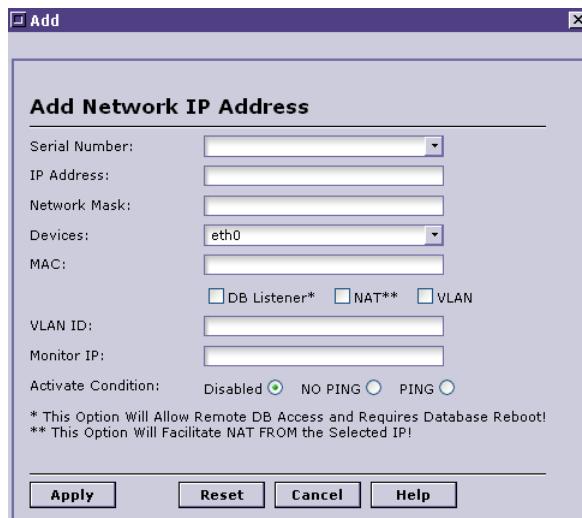


Figure 1-53 Defining Network IP Parameters

- Step 4** Refer to the description of each parameter above for reference as you configure:

- Serial Number
- IP Address
- Network Mask
- Devices
- MAC

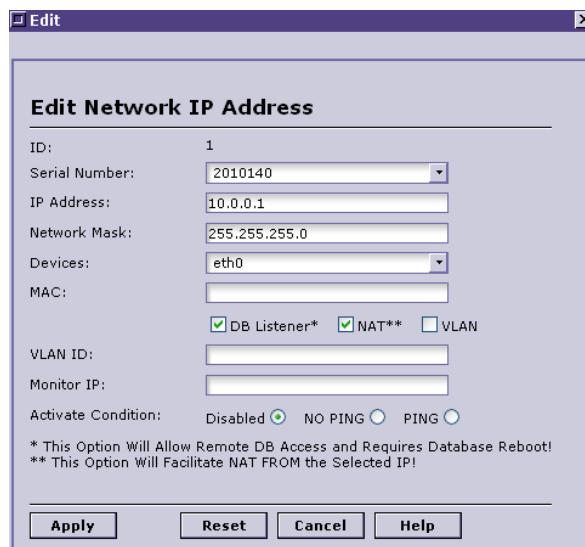
- IP Protocol/Status Variables:
  - DB Listener
  - VLAN
  - NAT
  - Dynamic
- VLAN ID
- Monitor IP

**Step 5** Select **Apply** to save the configuration and it is added to the IP Address Configuration window.

### Modify IP Address Configuration

To modify an existing IP address configuration:

- Step 1** If the Console is not currently active, log in and select **Start>Navigator**.
- Step 2** From the Navigator, select **Network Configuration>IP Address Configuration**.
- Step 3** Select the configuration from the IP Address Configuration window whose parameters you wish to modify.
- Step 4** Select **Edit>Edit Server IP Configuration**. The Edit Network IP Address dialog is displayed, with current configuration entries:



**Figure 1-54 Editing an Existing IP Address Configuration**

- Step 5** Change any of the existing definitions or settings.
- Step 6** When all modifications are complete, select **Apply**. The changes are effected.

### Delete IP Address Configuration

To delete a current configuration:

- Step 1** If the Console is not currently active, log in and select **Start>Navigator**.

- Step 2** From the Navigator, select **Network Configuration>IP Address Configuration**.
- Step 3** Select the configuration to delete (from those listed within the IP Address Configuration window).
- Step 4** Select **Edit>Delete Server IP Configuration**.
- Step 5** Confirm the deletion at the prompt (select **OK**) or cancel to abort. Confirmation deletes the IP address configuration and removes it from the list.

## Routes Configuration

Routes Configuration is the Network Configuration function that touches on the administration of actual network routes. Where the previous two functions identify and prepare the VoiceMaster for network function and operation, Routes Configuration configures actual data (packet) routing. Specifically, it is used to add static routes to a VoiceMaster residing on multiple IP networks.

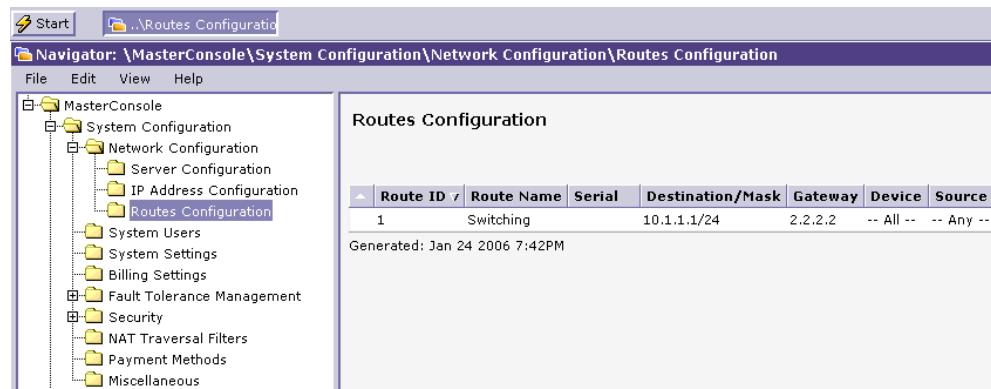
Routes Configuration parameters include:

- **Network Route Name:** Descriptive field for administrator reference.
- **Serial Number:** Assign the serial number for the server within the group on which the route will reside.
- **Destination/Mask:** Applies the route to packets with an IP destination within this range.
- **Gateway IP:** Routes the packets with the destination/mask to this IP Address.
- **Devices:** Applies the route specifically to the interface defined here.
- **Source:** Overwrites packet Source IP address to this address. If not selected, VoiceMaster identifies Source IP addresses automatically.
- **Status:** Enable or disable the route
- **Monitor IP:** Periodically ping this IP to check whether it is active. If inactive, VoiceMaster calls up replacement IP addresses to maintain function.
- **Activate Condition:** Configures ‘ping’ - must be set to ‘ping’ for VoiceMaster/Monitor IP checking to occur.

### Configuring a Route

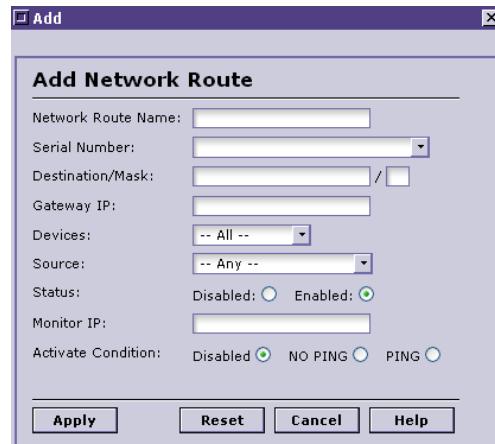
To configure a new network route:

- Step 1** Open the Console and Navigator as necessary.
- Step 2** Select **Network Configuration>Routes Configuration**. View the Routes Configuration window:



**Figure 1-55 Routes Configuration**

**Step 3** Choose **Edit>Add Network Route Configuration**. The configuration dialog appears:



**Figure 1-56 Configuring a New Route**

**Step 4** Refer to the parameters description in the section overview as you build the route, parameter by parameter:

- Define Network Route Name.
- Enter a serial number of the active server.
- Assign Destination/Mask to apply the route to packets that fall within the assigned range.
- Set the gateway IP - destination gateway for all packets assigned to the route.
- Set devices (the active interface for the route).
- Set Source IP (**still need clarification on what ‘overwriting’ does here**)
- Set route status, enabled or disabled.
- Assign Monitor IP for pinging and, in the last field, an activation status for pinging.

**Step 5** Select **Apply** to save the route and its individual parameters. It is added to the Routes Configuration list (window).

### Modify a Route

To modify an existing route:

- Step 1** Open the Console and Navigator as necessary.
- Step 2** Select **Network Configuration>Routes Configuration**.
- Step 3** Choose (select) the route to modify.
- Step 4** Select **Edit>Edit Network Route Configuration**. The dialog from Figure 5-9 is displayed, with existing parameters.
- Step 5** Modify any setting desired.
- Step 6** Select **Apply** to save changes. The route is saved and ‘returned’ to the list with modifications.

### Delete A Route

To delete a route:

- Step 1** Navigate to **Network Configuration>Routes Configuration**,
- Step 2** Select the route from the window to delete.
- Step 3** Select **Edit>Delete Network Route Configuration**.
- Step 4** At the confirmation prompt, confirm the deletion by clicking **OK** (or **Cancel** to abort).

Deleted routes are removed from the Routes Configuration window, and more importantly, from the system database.

## System Users Configuration

This section describes definitions of System Users and how to configure the different user roles vis-a-vis VoiceMaster administration. It also includes a detailed look at the privileges and limitations of the available System User roles in VoiceMaster.

In the context of the VoiceMaster Administration Console, a *user* is someone who has some level of access to the Console. This can be full managerial access, as expressed in the Administrator role, some limited role management of specific system aspects, or a ‘read-only’ role permitting viewing only. Users are usually system administrators or customer support representatives.

---

**Note** A *user* is not the same as a VoIP service *customer* or *subscriber*. These are the actual VoIP customers who initiate and receive calls through the network. A user, on the other hand, is a generic term for the range of roles (and associated individuals) that have access the Administration Console.

---

Multiple user role accounts exists, each with its own set of functions and privileges.

A user role is selected during the system user creation process. We will explain the field and parameter meanings in System Users Administration which follows shortly. The most common user roles and associated ‘rights’ are presented.

---

**Note** Obscure roles that pertain to unusual implementations are omitted. SysMaster sales and technical staff will describe the parameters of these roles to customers before purchase and installation.

---

The roles are:

- **Administrator**

Administrators have full privileges within VoiceMaster. They can configure users, routes, rates, custom module rules, etc. An administrator has both full privileges and the responsibility of managing the working VoiceMaster - including those user accounts that are subordinate to the Administrator role.

The **Administrator Account**, once created, is the gateway to creation of new accounts, route and rate configuration (provider and billing), batches, etc. This account is created just as any other account is (explained below). By default the system also supports a Super Administrator account that is always enabled to ensure constant system accessibility.

- **Conference Manager**

This user role describes the manager of conference calls. (A rare implementation.)

- **Customer Service**

This is a customer service administration role, responsible for managing ticket agent requests. (Not a typical application of VoiceMaster.) The next role described (Operator) is the also meant for customer service agents.

- **Gatekeeper Administrator**

Another specialized administrative role, contains all necessary function for managing the VoiceMaster as a gatekeeper (intelligent routing) device, without additional routing or billing functionality.

- **Guest**

Guests can only view all objects and parameters of the system. Guests have limited, ‘read-only’ privileges. The role is intended for demonstration purposes or for VoiceMaster customers whose system is administered for them.

- **ISP Administrator -MS (“ISP Admin”)**

This specialized Administrator role exists when VoiceMaster is used as an ISP Billing application. This is one of several Managed Services implementations.

**Note** To learn more about the purpose and implementation of Managed Services installations, refer to [Managed Services Scenarios](#) later in this chapter.

- **Lead Manager**

A role designated for an individual using VoiceMaster as a system for sales leads - organizes and distributes leads. *Rare implementation.*

- **Operator**

An operator is a limited administrative role directed towards the management of accounts and rates only. While an operator will have ‘read/write’ (viewing and modification) access to all aspects of the system, he will only be able to ‘write’ (administer) account and rate functions.

- **Reseller/Corporate Client -MS**

The reseller/corporate client manages his own set of subscribers, and, depending on ‘permissions’ assigned by the Administrator, can perform rate management functions. This role is functions within a Managed Services implementation. The VoiceMaster owner/Administrator retains overall system responsibility while the agent (reseller/corporate client) administers the network on a day-to-day basis.

- **Sales Agent and Sales Manager**  
A sales agent or manager uses the system to generate leads. *An unusual VoiceMaster implementation.*
- **Support Manager**
- **Support Operator**
- **Ticket Admin**  
The ticket administrator uses VoiceMaster to handle customer support complaints. (Again, an exceptional implementation.)
- **Wholesaler-MS**  
Similar to a reseller/corporate client role, except this person manages wholesale accounts. ‘Parent’ administrative services to be supplied by VoiceMaster owner.

## System Users Configuration

Administering system user accounts divides into three basic procedures:

- Creating a system user account
- Modifying an existing account
- Deleting an account.

We describe each procedure in turn, starting with account creation.

### Create a System User Account

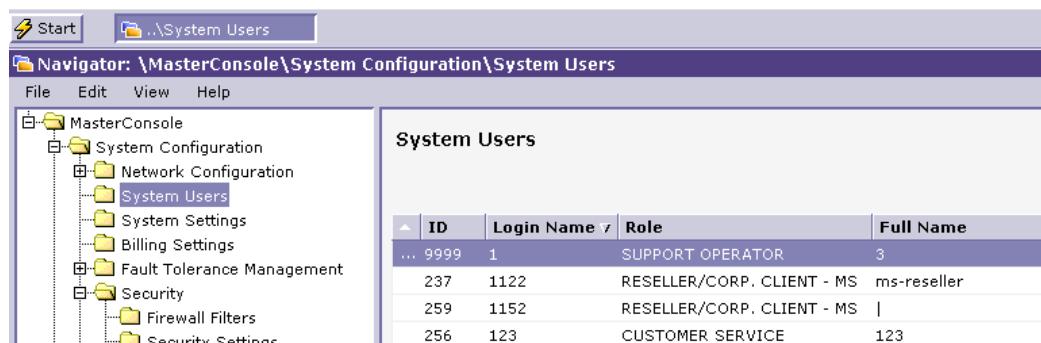
To create a System User account, follow these steps:

- Step 1** Log in to VoiceMaster as an Administrator.

**Note** Only an Administrator can create or modify system user accounts. Logging in as any other user type will block system user account administration actions.

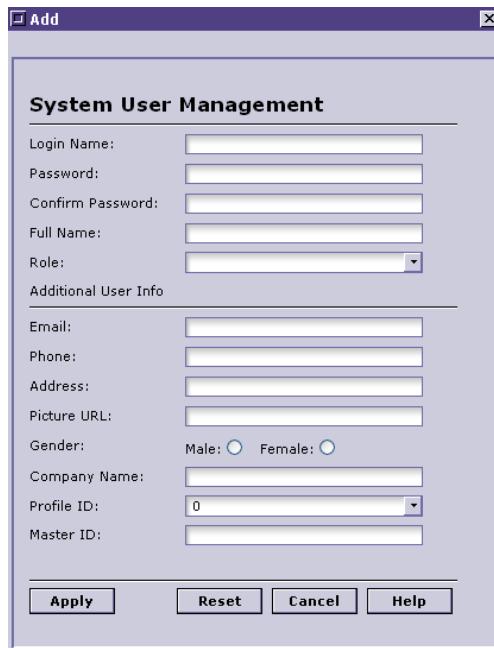
- Step 2** Select **Start>Navigator** to open the Navigator view.

- Step 3** Select **System Configuration>System Users** from the Administration Console folders at left. The System Users window will appear, as shown here:



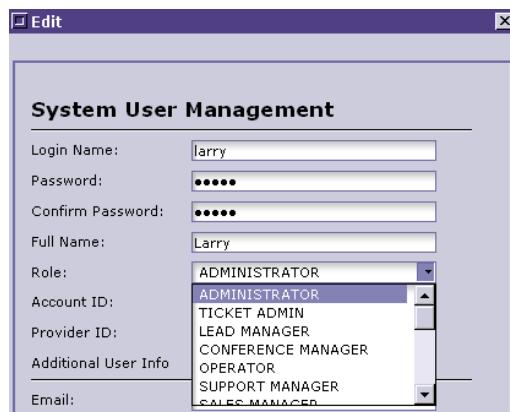
**Figure 1-57 System Users Selected**

- Step 4** Select **Edit>Add System User**, then wait for this dialog:



**Figure 1-58 Creating a System User Account**

- Step 5** Enter the new user Login Name.
- Step 6** Create a password in the next field, then confirm the entry in the following field (Confirm Password).
- Step 7** Type the user's full name.
- Step 8** Define the user role. *This is a critical step in the process; it accurately defines the new user and defines his VoiceMaster administrative privileges.* To do so:
  - (a) Select the pull-down menu to the right of the Role entry box.
  - (b) View the list of available roles:



**Figure 1-59 Selecting a User Role**

- (c) Scroll down the list (if necessary) using the scroll bar.

(d) Select the role that fits the new user.

**Step 9** Enter the additional user information to help identify the new system user. Four options are available: E-mail, phone, address and picture URL.

**Step 10** Define the user's gender.

**Step 11** Enter a company name, if applicable.

**Step 12** Assign a Profile and Master ID. The latter can be used when searching for the account, once created.

**Step 13** Select **Apply**. The new account is created and added to the System Users list (window).

### Modifying System User Accounts

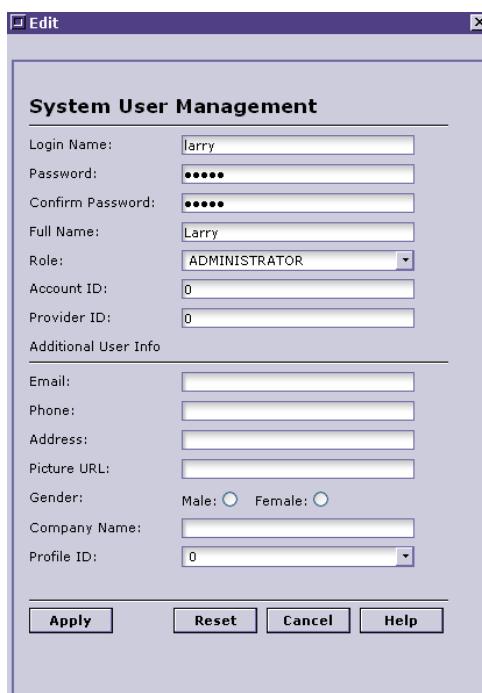
To edit an existing system user account, follow these steps:

**Step 1** Log in and select **Start>Navigator** (if the Console/Navigator are closed).

**Step 2** Select **System Configuration>System Users**.

**Step 3** From the System Users list, select the account to modify.

**Step 4** Select **Edit > Edit System User**. The Edit dialog for the selected user appears, with current parameters displayed:



**Figure 1-60 Modifying Current System User Account**

**Step 5** Change any parameters that you wish to modify. (If you intend to change user role, pull down the Role menu to select a new role.)

**Step 6** Select **Apply**. The dialog closes and the account is modified accordingly.

## Delete System User Account

To delete a system user account:

- Step 1** Log in and select **Start>Navigator** (if the Console/Navigator are closed).
- Step 2** Select **System Configuration>System Users**.
- Step 3** From the System Users list, select the account to delete
- Step 4** Select **Edit>Delete System User**.
- Step 5** At the Confirmation dialog, select **OK** to enforce the deletion, or **Cancel** to abort.
- Step 6** The deleted account is removed from the system (and from the System Users list).

# System Settings

A whole range of generic VoiceMaster configuration settings help create the foundation of later configuration and administrative actions. These settings, many of which are configured through the **System Administration** folder and its **Global VoIP Settings** subfolder, apply system-wide. They provide a functional base that catalyzes system operation and enables custom configuration of parameters for routes, rates and clients (subscriber groups).

System Settings together create a foundation of generic system behaviors. This foundation is constructed from several component functional categories:

- Caller ID Distribution Configuration. Enables the assignment of Caller ID prefixes to Softphone users (customers).
- **Database Backup Configuration.** Use this folder to set rules for database backup. The parameters let the Administrator set intervals for backups (by day/by hour).
- **Gatekeeper Configuration.** This function includes a set of parameters for configuring the system gateway. Includes working (routing) mode, enabling gatekeeper authentication and logs, called and calling prefix configuration/mapping, two-stage routing, endpoint registration and timeout settings.
- **General Configuration.** This function includes miscellaneous system configuration fields and parameters, including database/system password settings, payment methods and options, customer account recharge options, account billing initiation, session audit and timeout, and system currency and language settings.
- **Managed Services Configuration.** Managed services is a special VoiceMaster implementation in which an agent (wholesaler/reseller) ‘sits’ between VoiceMaster’s infrastructure and the actual calling customer. This intermediate layer changes both billing structure and VoiceMaster administration. In effect the latter is divided between the system’s owner and the agent. Managed Services is covered in detail in [Chapter 10: Special Implementations](#).
- **ISP Billing.** Another special implementation in which VoiceMaster is used to managed ISP billing for an Internet Service Provider. [Chapter 10: Special Implementations](#), includes the overview and procedural aspects of ISP Billing.
- **PIN Configuration.** Includes (gateway authentication) settings, PIN length definition, PIN generation and PIN batch configuration parameters, and related miscellaneous functions.
- **Route Failover Configuration.** The related functionality lets an Administrator set route failover policies, deciding which gateway and gatekeeper response codes (call error messages) will trigger failover to backup routes (if configured). Set failover policy by individual code, by setting code groups (per gateway/gatekeeper) or globally.

- **SIP Registrar-Proxy Configuration.** Used to set up VoIP call routing in SIP mode (SIP being the emerging alternative, or additional, protocol to the H.323 standard).
- **Special GK-Proxy Configuration.** The settings within Special GK-Proxy Configuration allow for the customization of message protocol function to fit network design and needs.

We now examine each of these System Settings and the procedures for configuring each function within this configuration category.

## Caller ID Distribution Configuration (Softphones)

Caller ID Distribution lets a VoiceMaster Administrator assign essential Caller ID prefixes to Softphone users. The key settings involved are:

- **Caller ID Prefix.** Designates the Caller ID prefix used upon softphone registration. Softphone users are registered to the system using the Caller ID prefix
- Caller ID Pointer. This setting defines the Caller ID prefix increment. The integer configured will increase each new caller ID assignment by its value. So, if the pointer is ‘2’ and a Caller ID of 35952123 is entered, newly generated prefixes are 359521230002, 359521230004, and so on.

---

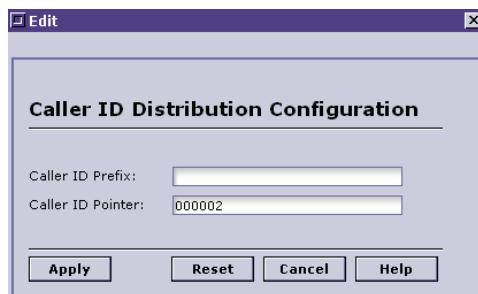
**Note** If the SoftPhone Profile Module is part of your VoiceMaster system, see the [Custom Modules](#) chapter for more on its functionality and configuration.

---

### Configuring Caller ID Distribution Settings

To configure the settings that configure Caller ID for the relevant subscribers, do the following:

- Step 1** Log in to the Administration Console and select **Start>Navigator** to open the Navigator.
- Step 2** Select **System Configuration>System Settings**.
- Step 3** Select **Caller ID Distribution Configuration** from the System Settings Window.
- Step 4** Choose **Edit>Edit Settings**. View the configuration dialog:



**Figure 1-61 Setting Caller ID Parameters**

- Step 5** Set the desired Caller ID prefix.
- Step 6** Define the Caller ID pointer (prefix increment).
- Step 7** Select **Apply** to save the settings.

## Database Backup Configuration

The Database Backup option serves to configure the process of backing up the VoiceMaster database. This is a vital activity, given the operational structure of the system.

All critical VoIP service-enabling components are stored in various database tables. The system calls on pieces of information (database entries) stored in specific tables when enabling calls. For instance, a route is chosen according to route configuration rules and the specific route designated for an authorized call. The selected route is stored in the system routing table and activated to complete the call. If the routing table data is compromised because it is inaccessible or corrupted, the VoIP service will be unreliable or even fail.

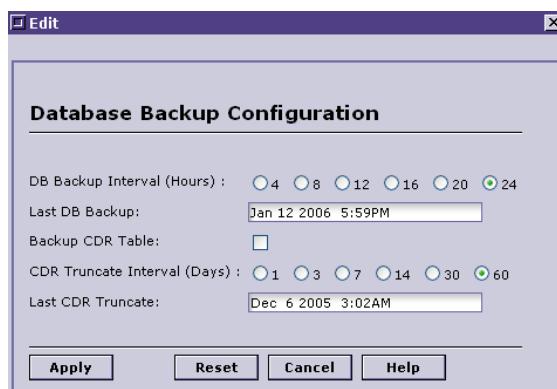
Therefore, preserving and duplicating the system database is key. Backup is critical, and is performed according to these parameters (configured by the Administrator):

- **DB Backup Interval.** Specifies how often the automatic backup will occur, in hours.
- **Last DB Backup.** Displays information about the latest database backup.
- **Backup CDR Table.** When selected, a CDR backup is periodically performed. All backup CDR files are stored in the /home/manager/cdr directory.
- **CDR Truncate Interval (Days).** Specifies the period between CDR truncations in days. *CDR truncation means expunging CDR records that are older than 180 days.* CDR Truncate Interval is calculated using Last CDR Truncate date as a start point.
- **Last CDR Truncate.** Specifies the time and date of the most recent CDR truncation.

### Configuring Database Backup

To set the database backup parameters (including the CDR aspects), take these steps:

- Step 1** Log in to the Administration Console and select **Start>Navigator** to open the Navigator.
- Step 2** Select **System Configuration>System Settings**.
- Step 3** Select **DB Backup Configuration**.
- Step 4** Choose **Edit>Edit Settings**. The Database Backup Settings dialog presents itself:



**Figure 1-62 Setting Database Backup Rules**

- Step 5** Set the DB Backup Interval. Frequency chosen should reflect overall system configuration realities. Systems that are processing large numbers of subscribers and their calls may require more frequent backup.

**Note** Both Last DB Backup and Last CDR Truncate entries are automatically filled in by the system, which monitors the last backup and confirms it.

---

**Step 6** Enable CDR table backup if desired.

**Step 7** Set the truncation interval parameter - the schedule for CDR truncation (record removal).

## Gatekeeper Configuration

Gatekeeper configuration settings permit the configuration of the various definitional components of the system gatekeeper. Together, the individual parameters comprise overall gatekeeper functionality.

The key gatekeeper configuration settings are described here and also displayed in Figure 5-7 (in the procedural section that follows):

- **GK Working Mode** Specifies the working mode of the Gatekeeper. It determines how the Gatekeeper treats the H.323 data flow (carrying voice data) and control flow (for establishing and terminating connections)
  - **Routed**  
In Routed Mode all system (RAS) information for call control is exchanged between the gateways by utilizing the gatekeeper, while the voice data flow travels directly from gateway to gateway. As a result, the Gatekeeper assumes part of the load, and that may slow down the connection in cases where heavy traffic exists. The Routed mode's advantage is that it works with all gateways and H.323 terminals in an H.323 zone.
  - **Proxy**  
In proxy mode, all traffic (voice data and call control) passes through the Gatekeeper. This places a significant load on the Gatekeeper and may slow down the whole system. The Proxy mode is relevant when the gatekeeper is the only device that can link to gateways that service PC-to-phone calls.
  - **Static**  
In Static Mode all system (RAS) information for call control, and voice data pass between both endpoints (gateway to gateway or PC to gateway). Static Mode reduces system load in cases of heavy traffic. It works only with Gateways capable of accepting a rewrite number, not with IP phone and other H.323 terminals.
- **H323 Gatekeeper Version**. Current version of H323 protocol implemented.
- **H323 Gatekeeper Log**. Enables/disables log that records gatekeeper activities.
- **SIP Registrar/Proxy Log**. When enabled, logs VoIP SIP Registrar events. (A SIP Gatekeeper is an H.323 gatekeeper provisioned to work in a SIP mode.)
- **GK Authentication**. When enabled, triggers authentication of all designated calls, usually PC-to-Internet, by the gatekeeper.
- **Called Station Prefix Pattern**. This parameter defines what portion of a number (prefix) should be stripped from incoming numbers. Users can specify multiple patterns. When any recognized pattern is discovered, the stripping mechanism is applied on a first-found basis. The following patterns are supported:

xx-y; -> finds prefix by the first 'xx' match and get y characters after the match.

**Example:** 10-4; will match 101234 from inbound number 1012345678901

-y; -> will match the first y characters of inbound number

**Example:** -2; will match the 10 from inbound number 1012345678901

.x; -> will match everything from beginning of the number to the x character

**Example:** .3; will match 10123 from inbound number 1012345678901

##; -> will disable the automatic '#' recognition of prefixes. The '#' is system built-in prefix recognition character. For example, if the inbound number 123#1012345678901 is received the system will automatically pick up 123# as a prefix. However, if '##' is specified the system will omit this prefix processing.

- **Calling Station Prefix Map.** This map is the pattern that is recognized and stripped according to mapping rules
- Internal Called Station Prefix. This prefix is used by all IP phones. When a calling number appears including such prefixes, VoiceMaster attempts to route the call using internal routing functionality.

---

**Note** Refer to the section on Internal Routing in [Chapter Seven: Route Management](#).

---

- **Two-Stage Route Management.** Enabling this option activates two-stage route management that optimizes system resources. (Single-stage management takes over if two-stage route management is disabled; this is a simpler, more resource-exploiting functionality). Two-stage route management is the default method unless disabled here. *Refer to Chapter Seven: Route Management* for more on two-stage routing.
- **Unknown EP Registration.** To deny the registration of unknown endpoints, enable this function. If it is disabled, such endpoints (gateways, etc.) can register with the system gatekeeper at will. This implies both general loss of system control and the creation of security risks.
- **GK Will Block CallerID/ANI.** If checked, the gatekeeper hide the calling party's caller ID/ANI.
- **Gatekeeper LRQ Timeout (2-10).** The value entered determines the number of seconds a VoIP Platform gatekeeper waits for a response to LRQ messages it sends to a receiving party. **Consult with a SysMaster support engineer before changing this value.**
- **Preserve Prefix** When checked, the prefix entered in the prefix pattern field above will be preserved. Available options are **International**, **System**, and **User**.

The Administrator can select none of these options, any specific option or all three. If Preserve Prefix is *not* enabled for any option, it is stripped during call establishment.

- **Failover Timeout (sec)** Specifies the amount of time that an alternative route is used after failover has occurred. When an alternate route has been used for 'X' seconds (determined by this parameter), the system will attempt to route calls over the primary route again.

---

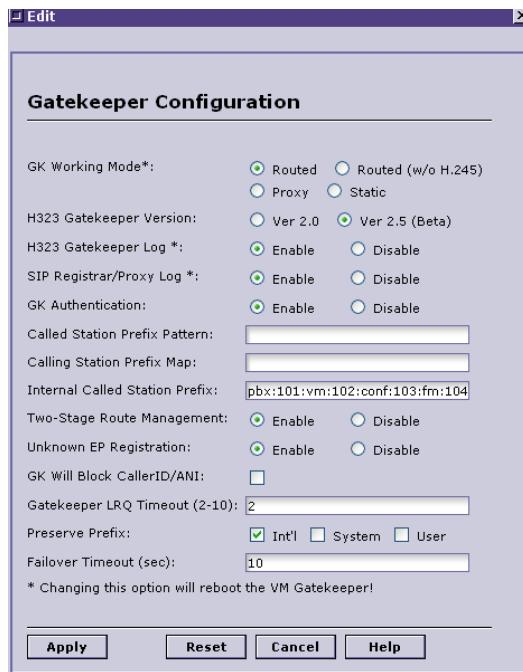
**Note** Route failover is designed so that if multiple routes are configured and a secondary route fails, the system uses the next alternate route. (Typically, multiple gateways are configured for a single destination area code.) No matter *which* alternate route is currently selected, the failover timeout triggers reactivation of the primary route.

---

### Gatekeeper Configuration

To configure gatekeeper settings:

- Step 1** Log in to the Administration Console and select **Start>Navigator**. (Skip this step if the Navigator is currently open.)
- Step 2** From the Navigator view, Select **System Configuration>System Settings**.
- Step 3** Select **Gatekeeper Configuration**.
- Step 4** Choose **Edit>Edit Settings**. Now view the Gatekeeper Settings dialog:



**Figure 1-63 Gatekeeper Configuration**

- Step 5** Configure each desired setting, choosing the desired radio button or check box, and entering data in text entry boxes where appropriate.

---

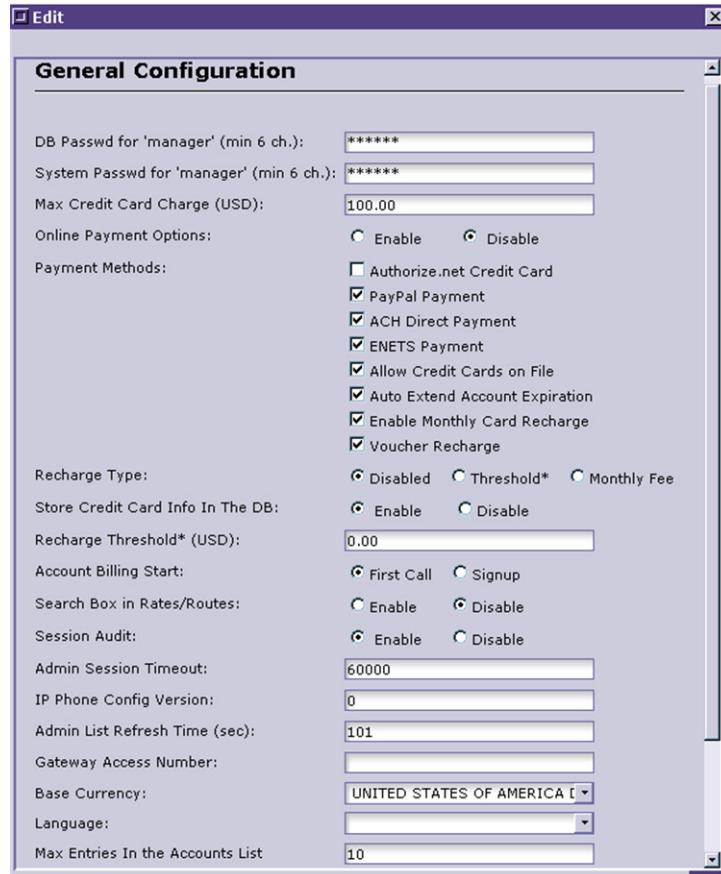
**Note** Refer to the parameter descriptions in the previous section to review the roles of individual parameters and the impact of the related configuration settings.

---

- Step 6** Select **Apply** to save settings and close the dialog box.

## General Configuration

General configuration settings let the Administrator set a whole group of critical system-wide parameters:



**Figure 1-64 General Configuration Settings**

General configuration settings include:

- **DB Password for "manager" (min 6 ch).** This password is required for a user ('manager') to access the system database. By entering the correct password, an authorized manager can establish a connection.

---

**Note** Default passwords may be changed at any time. We recommend that you do so at when first configuring the system. After that, changing database and system passwords is a good safety measure to protect against intrusions.

---

- **System Password for "manager" (min 6 ch).** Specifies the password used to set up a FTP and/or SSH session to the VoiceMaster interface. This password awards CLI command execution access to anyone using it.
- **Max Credit Card charge** –This sets a maximum amount that can be charged to a customer's credit card when buying calling time. Customers can charge up to the maximum, as can VoIP service administrators. Moreover, cards can be auto recharged if the *recharging options* explained below are configured.

- **Online Payment Options.** This option must be enabled before setting an individual payment method is possible. (*Both this option and a chosen payment method have to be selected before it's possible to actually configure that payment method [see [Payment Methods](#) later in this chapter]*). When a given payment method is configured, a user who has an account with the method vendor can charge calling time that way.)
- **Payment Methods.** These are the individual payment methods available to configure. Select any and all methods that your service supports; that is, with whose vendors you have previously contracted for the right to use the method. (Do not check any boxes for unsupported payment methods, as you will not be configuring them.)
- **Recharge Type.** Enabling this parameter is a prerequisite to activate the customer credit card recharge capability. Recharging a customer's card is both a useful convenience that allows auto-renewal of monthly plans and balance renewals as well. It is also an anti-fraud mechanism, when enabled and configured through a threshold balance. An Administrator can set a low threshold that protects in the case of credit card theft/subscriber account violation.

There are two paths for enabling Recharge Type:

- Enabling the Threshold option (two-part process). Check the radio button next to Threshold in the Recharge Type field, and the second is to establish a Recharge Threshold in that field (two fields below). Once an amount is set, the account is recharged according to the particular customer's configured account limit.
- Selecting Monthly Fee instructs the system to auto-renew the customer's monthly call amount using his credit card.

---

**Note** The customer's credit card information must be stored on the system database for this functionality to work. The **Store Credit Card Info...** option must be enabled for the recharge settings to take effect.

---

- **Store Credit Card Info in the Database.** Enable this parameter to store the customer's credit card information in the VoiceMaster database. This is required to perform renewal/recharge functions. However, note that a customer can still use his credit card to replenish his account. Credit card data *storage* is not required for such customer-initiated credit card purchases.
- **Account Billing Start.** The option decides when a subscriber's account billing cycle begins. **First Call** triggers billing accounting on the subscriber's first VoIP call made, while **Signup** begins the billing upon account subscription.
- **Search Box in Rates/Routes.** Enable this option to increase the speed of navigation throughout the Administration Console. By selecting Search Box display in all rate and route management folder windows, the time required to produce full rate and routes lists is saved. If disabled, all records for the relevant selection are recalled.
- **Session Audit.** When enabled, triggers the logging in the database of every system Administration action. This 'universe' of administrative actions includes 1) console session actions and 2) system messages.
- **Admin Session Timeout.** When the time entered in the field is reached, the Administrator is automatically logged out of the Console. This prevents unauthorized access and possible administrative mischief.
- **IP Phone Config Version.** Typically set to '0'. (For future configurations where different IP phone versions may be created; at which time setting a value other than 0 will have relevance.)

- **Admin List Refresh Time.** Sets a threshold for refreshing real-time statistics windows. The system counts the time down; when the threshold amount is reached, the data is updated and the window refreshed.
- **Gateway Access No.** For calling card subscribers. Designates the gateway number which the subscriber calls to request a VoIP connection.
- **Base Currency.** Assigns the currency to use for all transactions. Currencies are defined by country.
- **Language.** Specifies the language that the SysMaster gateway uses in playing Interactive Voice Response (IVR) messages to a subscriber requesting VoIP access. This option is relevant when SysMaster gateways are included. IVR messaging for other gateways is vendor-configured.
- **Max Entries in the Accounts List.** This sets a limit for wildcard search results, specifying the maximum number of results to return. The higher the result number, the longer any given search will take.
- **ISP Login File.**
- **Upgrade Server IP Address.**
- **Email Statements.** Two different methods of enabling email statements to the customer exist. They are:
  - Enable Link. When selected, will prompt subscriber with a message that directs him to a website where his statement may be accessed.
  - Enable Full. This option configures the sending of a full email statement as an attachment to the subscriber's registered Email address.

## General Configuration Procedures

To configure general system settings:

- Step 1** Log in to the Administration Console and select **Start>Navigator** as necessary.
- Step 2** From the Navigator view, Select **System Configuration>System Settings**.
- Step 3** Select **General Configuration** from the System Settings window.

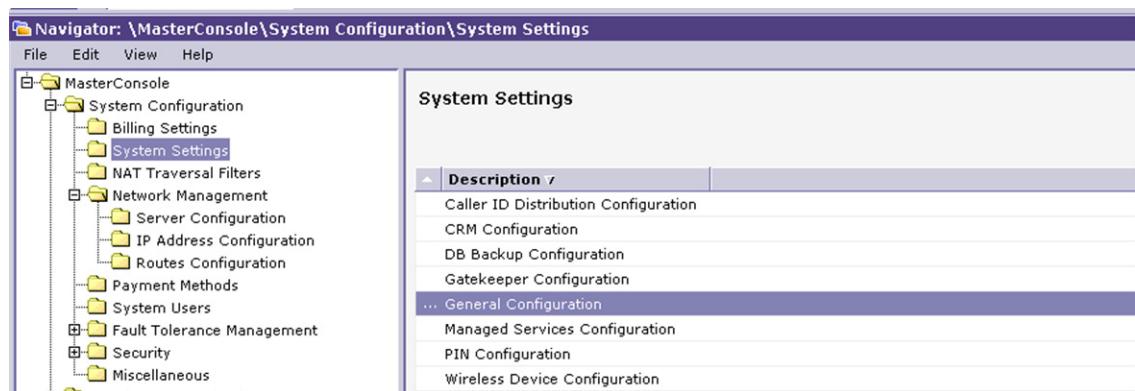
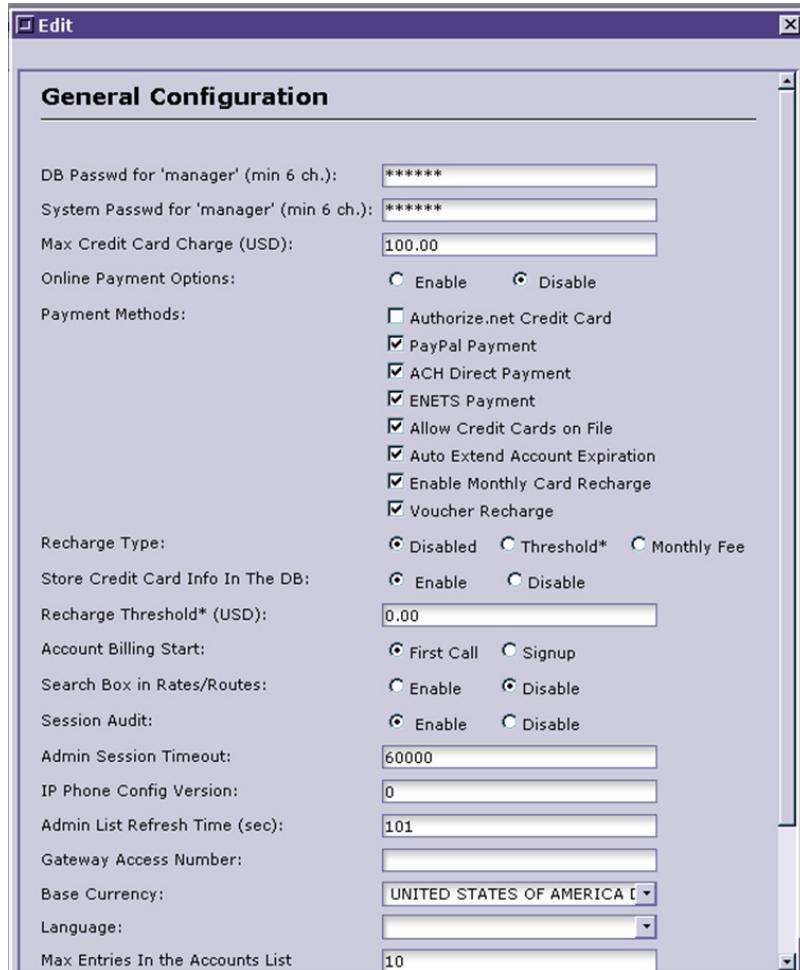


Figure 1-65 System Settings/General Configuration

- Step 4** Choose **Edit>Edit Settings** and view the General Configuration dialog:



**Figure 1-66 General Configuration**

- Step 5** Edit any parameter by selecting the text entry box, check box or radio button that enables the parameter in the desired way (for some, more than one enabling method is available).
- Step 6** When you have finished modifying the desired parameters, select **Apply**. The settings are saved and the dialog box closed.

## PIN Configuration

The purpose of PIN configuration is to set general parameters for PIN numbers and the generation (and activation) of batches of such numbers. This is an essential component of batch management (see [Chapter Nine: Batch Administration](#), for more on this aspect of VoiceMaster administration). An Administrator configures these general settings before creating and assigning batches to customers.

The available parameters are:

- **GW Authentication.** Enabling this triggers gateway authentication of PIN numbers and VoIP call attempts.
- **PIN Length (8-16).** Enter the number of digits that make up a PIN number. ‘8’ is the minimum, ‘16’ the maximum.

- **PIN Contains "\*" Separator.** Enable this to include the "\*" symbol within PIN numbers.
- **Enhanced PIN Generation.** Enables automatic batch generation (see the Batch Management chapter for more details).
- **PIN Prefix.** Assigns a prefix to all pin numbers based on this entry (if any).
- **Batch Bundle Activation Size.** Specifies the quantity of PINs that is activated during activation/generation of PIN batches (part of batch management).
- **Use Short State Name for CSR Generation.** When checked, displays state names in abbreviated form during CSR generation. (e.g CA, FL)
- **Disable Inter-Reseller Voucher Recharge.** If this parameter is *enabled*, it *disables* attempts by a reseller to recharge customer account vouchers.

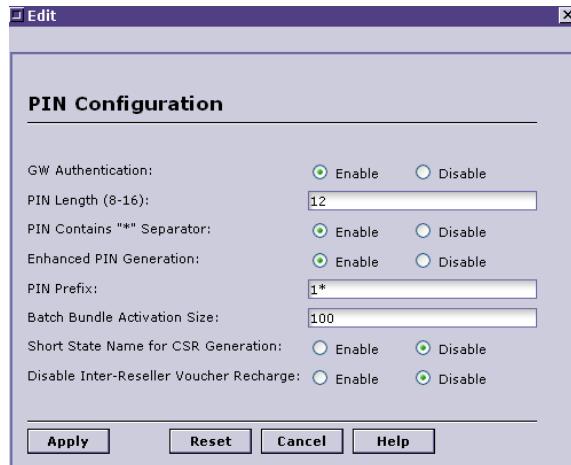
### PIN Configuration Procedure

To configure the PIN parameters:

**Step 1** At the Navigator, select **System Configuration>System Settings**.

**Step 2** Select **PIN Configuration**.

**Step 3** Select **Edit>Edit Settings**. The PIN Settings dialog is produced:



**Figure 1-67 Configuring PIN Parameters**

**Step 4** Set each option:

- GW Authentication. The default is ‘Enable’;
- PIN Length. Enter a value between 8 and 16.
- PIN Separator. Enable to add asterisk to separate between pins during batch creation.
- Enhanced PIN generation. Enable to configure.
- PIN Prefix. Add a prefix, if desired, and a \* to separate from main PIN number.
- Batch Bundle Activation Size. Set a maximum quantity to be activated during PIN batch generation.
- Short State Name...Enable to apply abbreviations during CSR generation.

- (h) Disable Inter-Reseller Voucher Recharge. Selecting ‘Enable’ disables this Reseller prerogative (the ‘Disable’ default permits such recharges).

**Step 5** Select **Apply** to save settings.

## Route Failover Configuration

The Route Failover functionality allows the gatekeeper to route a call to an alternate gateway should the currently selected gateway fail. A whole series of RADIUS response (error) codes is configurable.

The codes themselves reflect disconnect causes. Disconnect is what actually happens in the event of the error *when failover is not configured*.

When potential errors configured to trigger route failover occur, then the affected calls are routed to the alternate gateway.

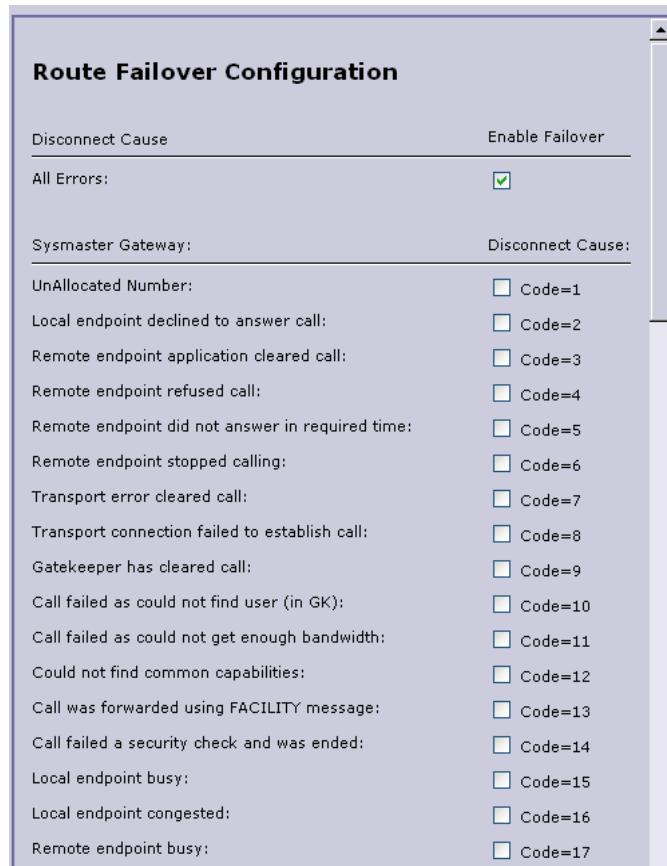
---

**Note** The full description of how route failover fits into routing configuration policies is found in [Chapter Seven, Route Management](#).

---

To configure Route Failover, do the following:

- Step 1** With the Navigator open, select **System Configuration>Global VoIP Settings**.
- Step 2** Select **Route Failover Configuration** from the Global VoIP Settings window.
- Step 3** Select **Edit>Edit Settings**. The Route Failover dialog is displayed (keep in mind that it is extremely long and you will need to scroll to view all error codes, divided into three categories):

**Figure 1-68 Route Failover Dialog**

**Step 4** Check the Disconnect Cause boxes associated with the error messages (triggering disconnect) that you want to trigger route failover (overriding disconnect).

---

**Note** Response codes exist for Sysmaster and non-Sysmaster gateways ('Cisco') as well as for gatekeepers. Configure settings for the gateway that fits your installation.

---

**Step 5** Alternately, enable **All Errors**, the first option, to cause failover for any and all listed errors that might occur.

**Step 6** Select **Apply** to save the configuration settings made and the dialog is closed.

## SIP Registrar-Proxy Configuration

SIP Registrar-Proxy Configuration is used to set up gatekeeper operation in SIP mode. (Recall that SIP is an alternative or complementary VoIP protocol to the H.323 protocol set standard.)

The SIP Registrar-Proxy settings include these key parameters:

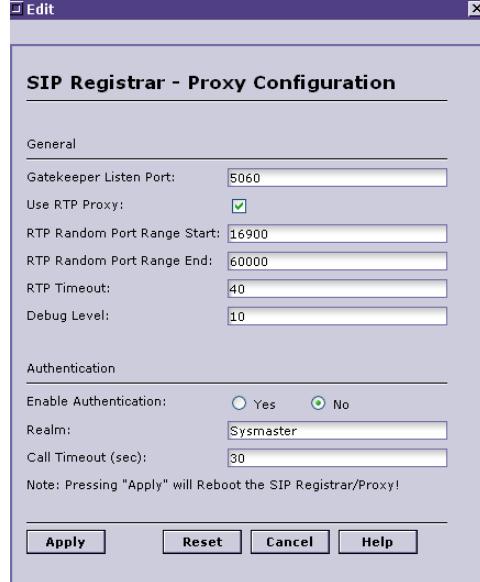
- **Gatekeeper Listen Port.** Specifies the port used to listen for SIP traffic
- **Use RTP Proxy.** Enables proxy mode for SIP RTP packets (voice payload packets). Gatekeeper recognizes and accepts such RTP traffic when the parameter is enabled.

- **RTP Random Port Range Start.** Specifies the starting port number for the group of gatekeeper UDP response ports assigned to SIP communication (including RTP packet transmission. RTP ‘receive’ packets always arrive at the listen port).
- **RTP Random Port Random Range End:** Specifies the last UDP response port in the series used for SIP communication and sending RTP packets. The gatekeeper *receives* RTP packets at the listen port.
- **RTP Timeout.** Specifies a timeout of inactivity for a SIP connection. Reaching the RTP timeout limit results in the connection being torn down.
- **Debug Level.** Specifies maximum number of debug messages the gatekeeper will output during operation. The values can be from 0 to 10. SysMaster recommends ‘0’ (the default setting) to achieve the highest performance level. Increasing message number may be advised when network problems exist.
- **Enable Authentication.** Allows or disallows gatekeeper authentication. Sub-settings include authentication realm and call timeout period (on sustained inactivity).

### Configure SIP Registrar-Proxy Operation

To configure SIP Registrar-Proxy mode operation, do the following:

- Step 1** Select **System Configuration>Global VoIP Settings**.
- Step 2** From the Global VoIP Settings window, select **SIP Registrar-Proxy Configuration**.
- Step 3** Select **Edit>Edit Settings**. View the edit dialog:



**Figure 1-69 Configuring SIP Registrar-Proxy Mode**

- Step 4** Set the Gatekeeper Listen Port. This is the port that will listen for voice (RTP) packets used for SIP operation.
- Step 5** Assign the **Use RTP Proxy** settings, in order
  - (a) RTP Random Port Range Start. First of ‘SIP’ ports within specified range)
  - (b) RTP Random Port Range End. Last of ports assigned to SIP operation.

- (c) RTP Timeout. Specifies period of inactivity at end of which SIP connection is torn down.
- (d) Debug Level. Assigns permitted number of debug messages to be delivered during a SIP session.

**Step 6** Set Authentication parameters:

- (a) Enable Authentication. Yes/No. Set to ‘Yes’ to authenticate SIP messages for the defined realm.
- (b) Realm. Define the realm in which SIP authentication is performed.
- (c) Call Timeout. Define period of inactivity before a call attempt is barred.

**Step 7** Select **Apply** to enforce SIP configuration settings.

---

**Note** Since SIP is a general VoIP protocol type governing a whole range of communication, applying configuration settings restarts (reboots) current SIP settings. Do not select Apply until you are sure that the settings are accurate.

---

## Special GK-Proxy Configuration

Special Gatekeeper-Proxy settings allow for more flexible processing of calls. Parameters can be set here for both H.323 and SIP operation mode.

Special GK-Proxy Configuration also allows the customization of messaging techniques within the VoIP network. Its parameters serve both to expand and custom-define messaging protocol functionality.

This list describes key functions parameters.

- Error Code Management. Error code translations (default-supplied).
- **Default Calling/Source Number:** Defines a specific source number that the gatekeeper inserts when H.323 calls do not specify a source number.
- **Call Signal Port:** Assigns a gatekeeper listen port for H.245 (call setup) signaling.
- **Listen on IP Address.** Listens for messages deriving from public IP addresses.
- **Enable GK H323 SoftSwitch Mode.** Triggers activation of softswitch mode for H23 proxying.
- **Strip Origination Tech-Prefix:** Strips all origination tech prefixes for active system users of the system who are not wholesalers. This applies to all incoming calls originating from H.323 terminals (part of call normalization process).
- **Strip Termination Tech-Prefix:** Strips all termination tech prefixes (again, a telephony normalization function).

---

**Note** The Custom Mapping module expands the VoiceMaster mapping functionality that helps apply E.164 conformity to all system calls.

---

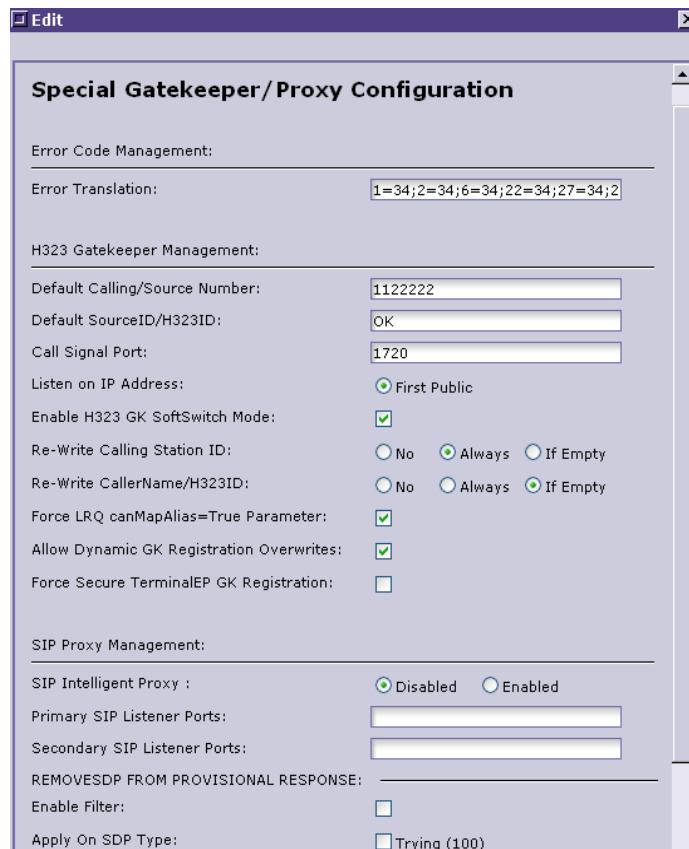
- **Force LRQ canMapAlias=True Parameter:** Forces the canMapAlias field of an LRQ request to True. When the gatekeeper initiates an LRQ request, phone number mapping is enabled.
- **Force Default H.323 ID (GK Routed/Proxy Mode):** Forces a default H.323 ID to all calls lacking one. Certain H.323 End Points require such an ID for correct authentication.

- **Enable Terminal End Points Active Call Pings:** Specifies that VoIP Platform will send pings to all endpoints registered within the gatekeeper zone; a monitoring function.
- **Display Registration Request in GK Terminal Console:** Displays all Requests for Registration, if set.
- **Force Secure Terminal End Point GK Registration:** Enforces secure registration of H.323 end points. Includes a database check for system users. If a user is not recognized, registration fails.
- **Allow Dynamic GK Registration Overwrites:** Allows for dynamic gateway registration associated with dynamic port assignments (available port assigned to registering gateways).

### Configure Special GK-Proxy Options

To configure Special GK-Proxy Configuration, follow this procedure:

- Step 1** From the Navigator view, select **System Configuration>Global VoIP Settings**.
- Step 2** Select **Special GK-Proxy Configuration**.
- Step 3** Open **Edit>Edit Settings**. View the dialog that appears:



**Figure 1-70 Special GK-Proxy Configuration Dialog**

- Step 4** Assign desired H.323 management parameters:
  - (a) Default Calling/Source Number. When defined, this number is inserted in cases where no source number is attached to a call.
  - (b) Default Source ID/H.323 ID. Enter “OK” to permit this replacement.

- (c) Call Signal Port. Define the listen port for all H.245 signaling (call setup attempts).
- (d) Listen on IP Address. Select “First Public” to have gatekeeper listen by IP address. It activates response when first public IP address is observed/heard.
- (e) Enable H.323 GK Softswitch Mode. Lets the gatekeeper work in conjunction with gateways that function as soft switches (proxying mode).
- (f) Re-write Calling Station ID. Applies policy for replacing calling station ID with mapped replacement number. Options are **No**, **Always** and **If Empty**. (In last case, existing station IDs are accepted, replacement provided only if the signalling message indicates that none has been provided.)
- (g) Rewrite CallerName/H323 ID. Identical options, as for previous parameter (No, Always, If Empty), except settings chosen will apply to Caller Name.
- (h) Force LRQ canMapAlias=True Parameter. *This is a Yes/No setting, as are the three that follow immediately.* Set to ‘Yes’ to enable mapping on initiation of LRQ request.
- (i) Ignore H.245 Address on Tunneling. Enables Tunneling mode (Virtual Private Network functionality) if set to Yes.
- (j) Allow Dynamic GK Registration Overwrites. Dynamic port registration enabled for gateway registration. When implemented, gateways connecting to systems are assigned current available port and so registered.
- (k) Force SecureTerminalEP GK Registration. When set to ‘Yes’, implements secure registration of ‘application’ endpoints (seeking registrations). Only those endpoints previously configured as legitimate system users are registered.

## (Wireless Device Configuration)

VoiceMaster customers who have this module should contact SysMaster Technical Support for configuration instructions.

## Billing Settings

Billing settings is a unique System Configuration folder with a set of four functions:

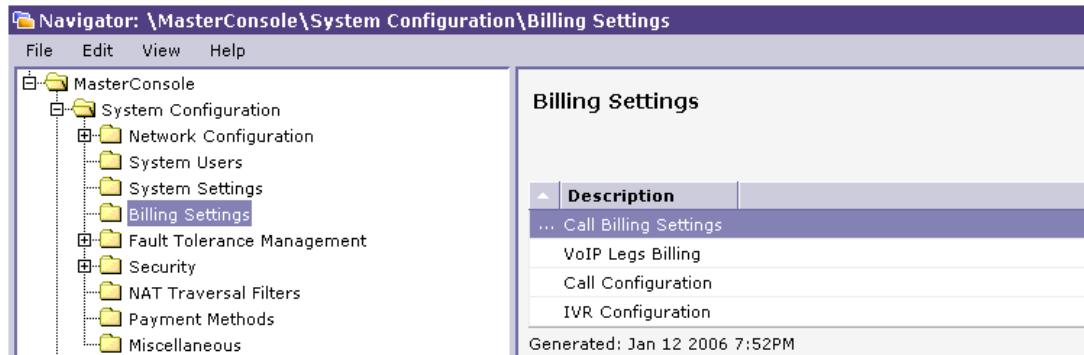
- **Call Billing Settings.** Includes a set of parameters such as call billing delay, exception billing and call merging.
- **Call Configuration.** Additional miscellaneous settings. Parameters such as maximum call time, grace period, post-paid balance and recharge limits are included.
- **IVR Configuration.** A range of Interactive Voice Response function settings that affect the contents messages played to the customer by system (origination) gateway IVR. For instance, one setting ‘tells’ the gateway IVR whether or not to specify number of seconds allotted to a call. Parameters are billing-related, directly or indirectly.
- **VoIP Legs Billing.** Facilitates configuration of different legs (segments) of VoIP calls. Include and exclude legs for billing purposes.

We now look at each of these Call Billing functions and how to configure their settings.

## Call Billing Settings

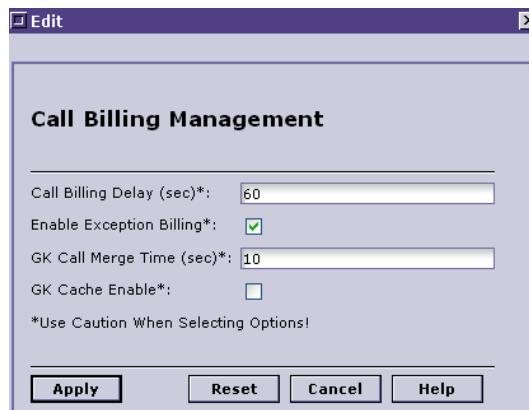
Call Billing settings are a small group of generic settings that, when configured, apply to all system calls. To configure these global billing parameters, follow these steps:

- Step 1** Log in and open the Navigator if you have not previously done so.
- Step 2** At the Navigator view, select **System Configuration>Billing Settings**:



**Figure 1-71 Global Billings Window**

- Step 3** Select **Call Billing Settings**
- Step 4** Select **Edit>Edit Settings**. The dialog is displayed:



**Figure 1-72 Configuring Call Billing Parameters**

- Step 5** Set a Call Billing Delay, if desired. Billing is delayed by the number of seconds entered.
- Step 6** Enable Exception Billing. If set, opens a range of billing customization options, including those available through the VoiceMaster Custom Modules (see the Custom Modules chapter for more information on any custom billing module included in your system).
- Step 7** GK Call Merge Time. Sets a time frame for merging multiple calls. If a second call is initiated within the time set in this field, the signals are merged. (See the Example at the close of this procedure.)
- Step 8** GK Cache Enable. Activates the gatekeeper's caching ability for enhanced processing.
- Step 9** Select **Apply** to save this group of global call billing settings.

## Call Merge Time Example

```

call merge time = 30 seconds
at 0:00 there is a call authentication request, including destination no.
at 0:15 another call authentication + destination no. is received.
Second call's signals are merged with the first call's signals.

```

## Call Configuration

Call Configuration, like Call Billing Settings, includes a miscellaneous set of global settings affecting system call billing. Because of their variety and range, it is simplest to describe each parameter rather than to attempt to categorize them.

The individual Call Settings parameters are:

- **Max Call Time (sec).** Specifies a duration for each call in the system. Calls exceeding this limit will be disconnected. Calls that exceed the configured threshold are identified as ‘hung’ (malfunctioning) calls by the VoiceMaster and terminated.
- **Bill Calls Over Max Call Time.** Sets a threshold, the breaching of which triggers billing for all call portions. This is relevant for older gateways that cannot disconnect calls that break a time threshold. *If your network includes only gateways that have ‘answer supervision’ functionality to disconnect such calls, this parameter need not be configured.*
- **Grace Period (sec).** This establishes a no-billing segment for a call, geared to events such as (billed) received busy signals, no receiver responses, etc. Calls are not billed for the number of seconds entered here unless the threshold is exceeded. In that case, the entire call duration is billed.
- **Bill Only Calls Above Time (sec).** Similar to the Grace Period, except that billing only begins at the threshold, even if it *is* exceed. These two parameters can be considered as one basic function broken into two; that is, each represents a different policy response to the same event.
- **Radius Log.** When checked, Radius Log generation will be enabled.
- **Failover CDR Collection.** CDR collection itself is the display of different aspects call history. This parameter shows all route failover instances in a combined format. If not enabled, such instances are displayed in longer, harder-to-view format.
- **Max Post-Paid Balance.** This is used to calculate call time in the absence of prepaid balances. If this parameter *and* the individual account’s post-paid balance are set to ‘0’, calls originating from such an account fail (are blocked).
- **Recharge Account to Balance.** Amount entered determines how much to charge a customer’s credit card when ‘0’ is reached in account balance. *This assumes a monthly call plan in place. Prepaid accounts always become inactive once ‘0’ is reached.* (Additional recharge options include the ability to recharge an account when a dollar threshold is reached. If that parameter is not set, this one performs the same function when the account balance is exhausted.)
- **Send ‘Billing-Model’ Parameter in Radius.** Activates this specific Radius parameter for gateways that support it. Relevant to Cisco gateways with Cisco IOS.
- **Min Credit To Make Calls (USD)** Specifies the minimum account credit necessary to make a call. If an account’s credit amount dips below this limit during a call, there is no impact, however.

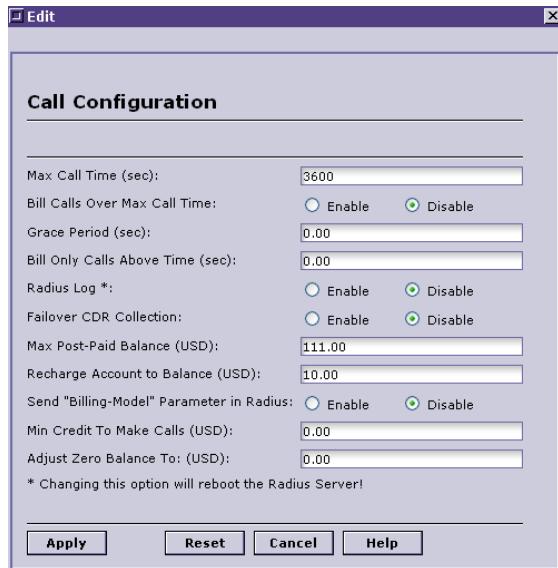
### Configure Call Settings

To configure Call Settings, follow these steps:

- Step 1** At the Navigator view, select **System Configuration>Billing Settings**.

**Step 2** Select Call Configuration from the window.

**Step 3** Select Edit>Edit Settings, and view the dialog:



**Figure 1-73 Call Settings Dialog**

**Step 4** Configure each desired parameter. Note that some settings are configured by entering text, others by moving currently selected radio buttons, and so on.

**Step 5** Select **Apply** to save settings and close the dialog.

## IVR Configuration

IVR Configuration options affect the contents of messages the origination gateway's Interactive Voice Response system delivers to the customer at designated prompts. (Recall that the customer is instructed to take specific actions like entering a PIN; on completion of each action the IVR sequence delivers the next instruction in the sequence.)

The gateway 'runs' the IVR system on its own. It is already programmed to guide the customer through the steps that authenticate his identity and allow the call. The entries here configure details of those announcements.

The settings are:

- **Fixed Charges and Taxes in IVR.** Enable this to include all fixed call charges and taxes in the IVR announcement.
- Custom Charges in IVR. Enable to have custom charges (if any) announced to customer.
- **Special Number Charges in IVR.** When enabled, announces charges that specifically apply to special numbers (contingent upon implementation of the Special Numbers module, described in the Custom Modules chapter later in this guide). //is this the case??
- **IVR Time Adjustment (sec).** The value entered here is added to the 'official' time reported to the user as available call time.
- **Play Seconds in IVR.** Will announce call time in seconds if enabled.

- **Convert Account Currency in IVR.** If checked, IVR will convert account currency from the base USD format to alternate currency (if one is configured). *An Administrator must have configured a different base currency for this option to apply.*
- **Enable Max Call Time in IVR.** If checked, IVR will announce the max call time per user account.

## Configuring IVR Settings

To configure any or all IVR settings and apply them, carry out the instructions in this section.

---

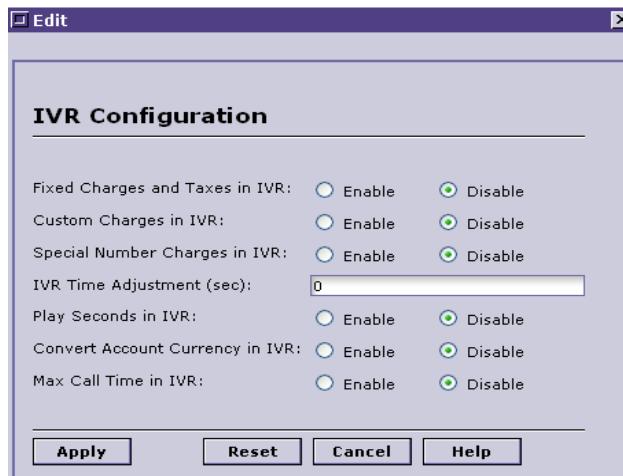
**Note** All IVR settings are default-disabled, which leaves the gateway IVR messages in a generic, basic mode. You must ‘manually’ enable each parameter to activate it.

---

**Step 1** At the Navigator view, select **System Configuration>Billing Settings**.

**Step 1** Select **IVR Configuration** from the window.

**Step 2** Choose **Edit>Edit Settings**. View the IVR Settings dialog:



**Figure 1-74 IVR Settings Configuration**

**Step 3** Enable any of the default-disabled options that you wish to apply to the IVR system.

**Step 4** Enter a value in the IVR Time Adjustment field to increase official announced time.

**Step 5** Select **Apply** to save settings. Origination gateway(s) announcements to the customer will change according to those parameters configured.

## VoIP Legs Billing

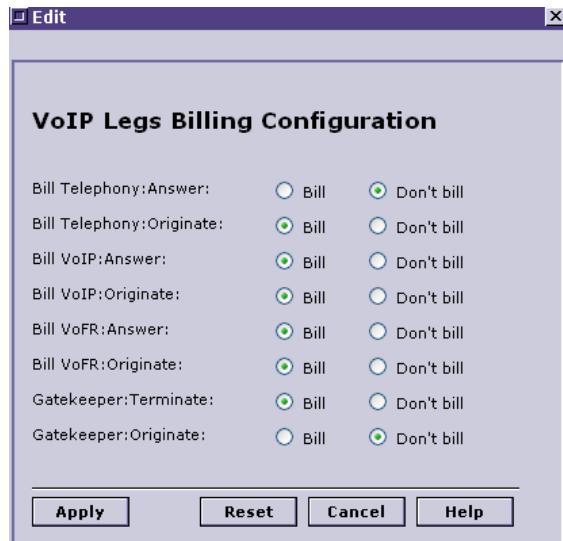
The VoIP Legs Billing option specifies which portions, or ‘legs’, VoiceMaster will bill.

To configure VoIP Legs Billing settings:

**Step 1** Select **System Configuration>Billing Settings**.

**Step 2** Select **VoIP Legs Billing** from the Billing Settings window.

**Step 3** Choose **Edit>Edit Settings** to produce the configuration dialog:



**Figure 1-75 Call Billing Configuration**

**Step 4** Select those Call Billing legs to bill ('Bill' or 'Don't Bill' each leg):

- (a) Bill Telephony:Answer. Bill the 'answer' leg/the PBX (voice) segment.
- (b) Bill Telephony:Originate. Bill the PBX origination leg (to the gateway).
- (c) Bill VoIP:Answer. VoIP (gateway) answering leg (IP data link portion).
- (d) Bill VoIP:Originate. VoIP (gateway) origination - IP leg data transmission.
- (e) Bill VoFR:Answer. FrameRelay data transmission (receive).
- (f) Bill VoFR:Originate. FrameRelay data transmission (send).
- (g) Gatekeeper:Terminate. For Gatekeeper terminated IP data traffic.
- (h) Gatekeeper:Originate. Gatekeeper-originated data link traffic.

**Step 5** Select **Apply** to enforce settings and close the dialog.

## Payment Methods

This function lets you configure various authorized payment methods available to a customer via the CRM web site.(An Administrator must have the specific parameter description information from each payment method vendor to configure any method). After a method's configuration is complete, a VoIP service subscriber can make account payments using any configured method.

---

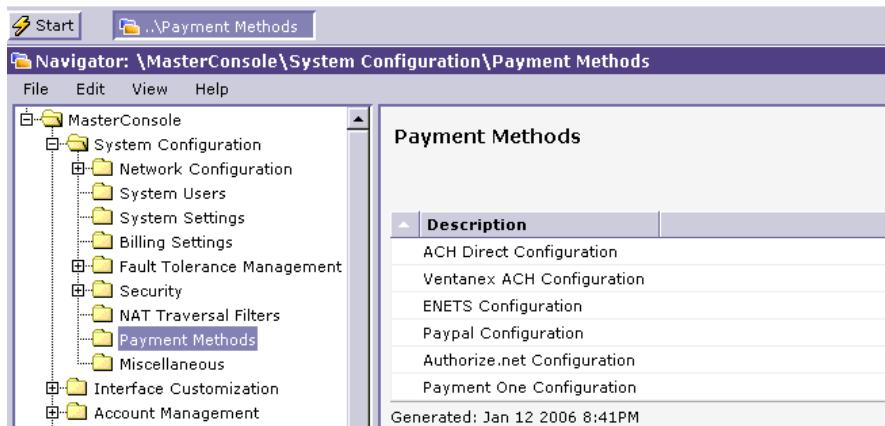
**Note** Configuration of Each payment method must be enabled first at **System Configuration>System Settings>General Configuration**.

---

We will use ACH Direct Configuration as a template for explaining payment method configuration. The basic steps are essentially the same. Specific fields and payment vendor parameters will vary according to the method selected for configuration.

To configure a payment method (in this case, ACH Direct), do the following:

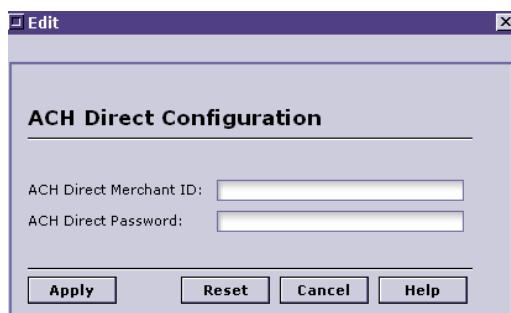
- Step 1** Select **System Configuration>Payment Methods** from the Navigator view. The Payment Methods window is displayed:



**Figure 1-76 Payment Methods Selected**

- Step 2** Select **ACH Direct Configuration**.

- Step 3** Open **Edit>Edit Settings**. The configuration dialog for ACH Direct appears:



**Figure 1-77 ACH Direct Configuration Dialog**

- Step 4** Enter the Merchant ID.

- Step 5** Enter the direct password.

- Step 6** Select **Apply** to confirm the entries.

ACH Direct payment method is configured and subscribers can pay account fees using this method (and all others you have configured).

---

**Note** A subscriber must first register with the individual payment method vendor before he can pay his VoIP bill or add amounts to his balance using the method.

---

# Security

Security is a critical aspect both of network performance and health, and is typically implemented as a suite of protective measures. Security functions help regulate access to administrative functions and to the network and specific devices on it. Security features usually define permissions and forestall intrusions. Fraud detection and blocking is an integral part of the latter function.

VoiceMaster is a system that relies on powerful functionality that revolves around a robust database, where routes, rates, provider and customer information, etc., are stored. The potential for unauthorized access is always present.

Protecting system integrity is accomplished different ways:

- User Roles Definitions. Defining roles for new users is also a form of security, with each role circumscribing related user functional permissions.
- **Password Control.** The system administrator can control access by strictly controlling distribution of passwords. Changing passwords is another anti-intrusion measure.
- **Port Restrictions.** The database is accessed through a single port. Access to this port can be controlled by firewall-based restrictions.

There is also the question of access to the call network itself. Common forms of VoIP network abuse include stealing legitimate subscriber identity to make unauthorized calls. This is counteracted by the use of AAA RADIUS, which explicitly checks a caller's identity and permissions (including account balance) before allowing a call to proceed. It looks for two parameters for each call:

- Caller identification. If this is illicit, the attempt is rejected.
- Account balance status. If insufficient, a caller is still blocked from using the system.

VoiceMaster also supplies special modules that actively detect and block fraud. The Fraud Detection module lets an Administrator 'blacklist' and 'graylist' unlawful calls. When used in conjunction with the custom module Exception Numbers, fraud detection measures block designated call sources.

VoiceMaster also uses System Alerts to configure alarm notifications when specified events occur.

---

**Note** CRM security is also offered via SSL encryption mechanisms. Site security is shown to the user, increasing customer confidence that credit card and personal information are protected. See the [Interface Customization](#) section for more on SSL CRM configuration.

---

## Database/Administrative Access

The first means of controlling access to the database is by defining user roles. One of the purposes of applying more role categories to a specific Console user is to wall off access to core functions, for instance, those that concern Route and Rate management. New user role definition is described in [System Users Configuration](#).

---

**Note** An 'Administrator' (the primary audience for this guide) has full rights to virtually all system functionality.

---

*Password control* is an even more direct way to control access to the database. Database and system passwords are set through the **General Configuration** options accessed through **System Configuration>System Settings**.

*Port restrictions* can also be enforced, limiting access to the database. An Administrator can block specified source and destination ports.

## Firewall Filters

VoiceMaster provides an integrated firewall capability that enables filtering of inbound and outbound traffic. Configuring firewall filters protects against unauthorized access - to the system database and to call activation.

---

**Note** Firewall filters, like fraud detection settings, are implemented as modules within VoiceMaster. Your ability to activate their functionality depends on their inclusion within *your* system.

---

The firewall filters perform full Ingress/Egress packet filtering to allow dynamic packet processing, accounting, and policy data collection and reporting. These filtering parameters are available for an Administrator to use as appropriate:

- **IP protocol**  
Supported protocols are: TCP, UDP and ICMP
- **Destination Network Address**  
Comprised of the destination IP address and the destination Network Mask
- **Destination TCP/UDP**  
Port or port range
- **Source Network Address**  
Consists of the source IP address and the source Network Mask
- **Source TCP/UDP**  
Port or port range

---

**Note** A firewall filter can be positive or negative, that is, a source port can be specified and then all packets from it *accepted*. Alternately, you can configure the rule to *drop* packets from a source. Thus, rules can be set to include and exclude traffic by specific nodes.

---

Firewall Ports associated with VoiceMaster include:

http	8080 / 80
ftp	21
ssh	22
ssl	443 / 8081
h323 1718,1719,1720,1721,16 000 - 50 000 (tcp/udp)	

In the next sections, we discuss how to add, edit and delete firewall filters.

### Add (Create) Firewall Filters

To configure new firewall filters, follow this procedure:

- Step 1** Log in and open the Navigator if it is not currently available.
- Step 2** Select **System Configuration>Security**.
- Step 3** Select **Firewall Filters**. The Console window changes accordingly:

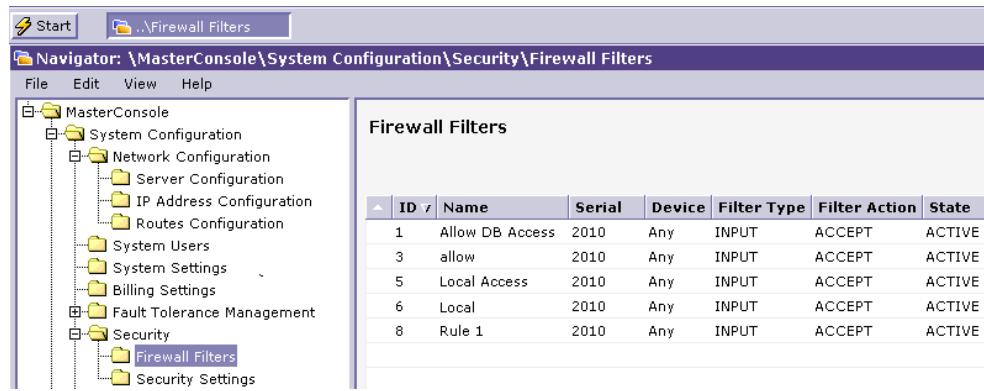


Figure 1-78 Firewall Filters Window

**Step 4** Select Edit>Add Firewall Filter. The appropriate dialog appears:



Figure 1-79 Adding a Firewall Filter

- Step 5** Assign a name to the rule. It can contain any number of characters and numeric values.
- Step 6** Assign serial number and device names. These describe the device and physical ports to be protected by the rule.
- Step 7** Set rule status (active or inactive). ‘Active’ implements the rule once you apply the settings, while ‘inactive’ saves the rule but does not apply it.
- Step 8** Set IP Filter action. Options are to accept or drop packets.

---

**Note** Rule status must be ‘active’ or accepting packets will have no practical meaning.

---

- Step 9** Filter traffic by protocol type. (The rule will act on traffic of the type specified here.)

- TCP
- UDP
- ICMP

TCP and UDP packets are matched by either IP based filtering or by port or port number range.

- IP-based filtering requires a destination and source network address.

A network address consists of an IP address and a network mask. In order to make a destination address configurable for outbound traffic, it should include Destination IP and Destination Network Mask values.

- Firewall filtering by port or port number range is achieved by specifying the TCP/UDP ports or the port range to be filtered. If a single port is to be filtered, its value should be entered against the respective Port field. For specifying a range of ports enter the least and biggest port encompassing that range (**e.g.** 1790:1792).

- Step 10** Set the Destination IP address.
- Step 11** Set the Destination Network Mask.
- Step 12** Identify the Destination Port. This is matched against the firewall rule (you can also set a specified range of ports).
- Step 13** Set Source IP (address).
- Step 14** Enter the Source Network Mask.
- Step 15** Specify the source port - a single port or a group of ports within the range indicated.
- Step 16** Set Rate Limit Packet/sec. Enter a value to define maximum number of packets per second for rule evaluation.
- Step 17** Set a Rate Profile ID (if rate limit is established).
- Step 18** Select **Apply** to save the rule settings and add it to the Firewall Filters list.

## Modifying Firewall Filters

To edit a Firewall Filter:

- Step 1** Log in and open the Navigator if it is not currently available.
- Step 2** Select **System Configuration>Security**.
- Step 3** Select **Firewall Filters**.
- Step 4** Now select a filter from the window (list) to modify.
- Step 5** Choose **Edit>Edit Firewall Filters**.
- Step 6** Change any of the parameters.
- Step 7** Click **Apply** when finished

## Delete Firewall Filter

To delete a Firewall Filter:

- Step 1** From the Navigator view, select **System Configuration>Security**.
- Step 2** Select **Firewall Filters** and click on the filter to delete.
- Step 3** Select **Edit>Delete Firewall Filter**.

- Step 4** Click **OK** at the prompt to delete the filter, or cancel to abort.
- Step 5** Confirming the deletion removes the filter from the Firewall Filter list (and from the system).

## Security Settings (Fraud Detection)

Fraud detection is perhaps the most specific form of security functionality available to the VoiceMaster Administrator. Configured fraud detection can:

- Detect possible fraud attempts
- Take active measures against such attempts such as blocking of the user's Caller ID.

---

**Note** Fraud detection, which includes blacklisting and graylisting of numbers associated with fraud attempts, is particularly useful for responses to calling card abuses. It is bundled with the Exception Numbers (custom) module that helps attack PIN fraud. See the Custom Module chapter for more on Exception Numbers.

---

The Fraud Detection features block fraudulent activity on the basis of two policy approaches/responses:

- **Blacklist.** The blacklist settings enforce a block/release policy on unauthorized call attempt sources. That is, if a specified user surpasses a configured thresholds for call attempt limits, that user/number is blocked for a specific period of time. Once this interval expires, the system automatically releases the policy and permits additional call attempts.  
Reports generated by a blacklist will display parameters such as:
  - Currently blocked customers
  - Number of wrong pin attempts
  - Blocking time
  - Unblocking time (when the system will automatically unblock).
- **Graylist.** The graylist option, actually more prohibitive in nature, both blocks a fraud-associated user *and* requires that the Administrator 'manually' release that user/number from the list of barred numbers. VoiceMaster will block the designated user for making (threshold-defined) 'X' number of wrong PIN attempts in a specified period of time. Reports on graylisted numbers are produced as part of the Fraud Detection Report functionality.

## Fraud Detection Administration

Administering fraud detection involves creating (adding), modifying and deletion of fraud detection rules. Each of these procedures follows, in order.

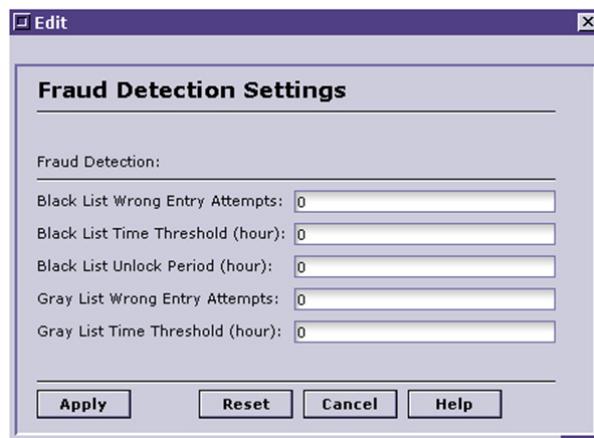
### Adding a Fraud Detection Rule

To set up a fraud detection rule:

- Step 1** Log in to the Console and open the Navigator, as necessary.
- Step 2** From the Navigator, select **System Configuration/Security**.
- Step 3** Select **Security Settings**.

**Step 4** Select **Fraud Detection Settings** from the Security Settings window.

**Step 5** Choose **Edit>Edit Settings** to display the Fraud Detection Settings dialog:



**Figure 1-80 Fraud Detection Settings**

**Step 6** Set Fraud Detection settings.

- (a) Enter values for each of the blacklist settings - wrong entry, time and unlock period. These are threshold settings, so (for instance) if ‘wrong entry attempt’ is set to ‘6’ the seventh attempt is blocked.
- (b) Set the Gray list parameters. *Remember, these are more prohibitive than the black list settings.*

**Step 7** Select **Apply** when done.

---

**Note** Setting Fraud Detection policies is a two-part procedure that involved setting Exception Number rules. Exception Number rules works to set an ‘action’ policy for certain numbers. If the action invoked is a fraud detection response, it is applied to the designated numbers.

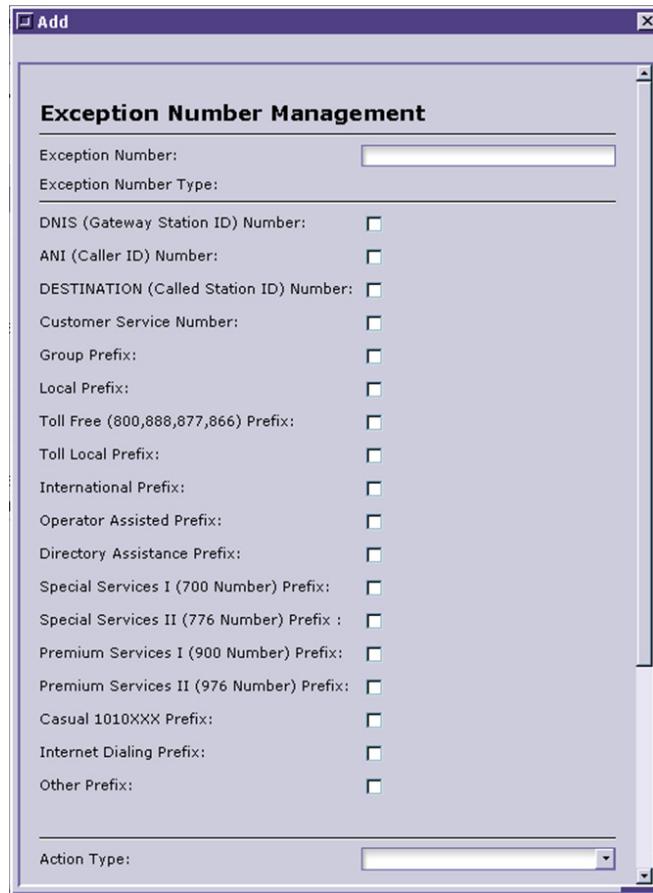
---

#### Exception Numbers & Fraud Detection Configuration

The second half of applying fraud detection policy assumes integration of the Exception Number modules, and goes like this:

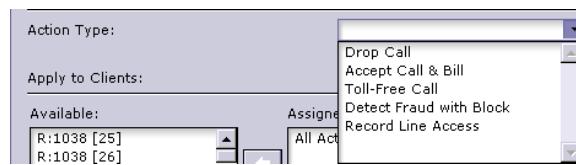
**Step 1** At the Navigator view, select **Custom Modules/Exception Numbers**.

**Step 2** Select **Edit>Add Exception Numbers** from the Edit menu. The dialog is displayed:



**Figure 1-81 Adding an Exception Number Rule**

- Step 3** Configure an exception number rule to work together with fraud detection as follows:
- Step 4** Enter an Exception Number - the Exception Number is the access number accepting calls for Calling Card IVR
- Step 5** Under Exception Number Type, check the DNIS (Gateway Station ID) Number box, only.
- Step 6** Select an action to assign from the six Action Type drop-down options:



**Figure 1-82 Exception Number Actions**

**Note** You **must** select “Detect Fraud with Block” to enforce fraud detection policies (previously configured) for the rule.

- Step 7** From the list of available clients, assign the client(s) to which the rule will apply.

- Step 8** Select **Apply** to set the policy. The database is updated, the dialog closed and the new number is added to the Exception Numbers list.

---

**Note** We will not describe here how to modify or delete an Exception Numbers rule. This is covered in the Custom Modules chapter, in the section on Exception Numbers.

---

## Create Fraud Detection Report

Once all rules have been created, you can configure a fraud detection report. This report facilitates the tracking of fraudulent activities and appropriate administrative responses to them.

To create a fraud detection report, perform these actions:

- Step 1** From the Administrative Console, select **Event Monitoring>Reports>System Reports>Fraud Detection**.
- Step 2** Select **Edit>New Report**. The Fraud Detection dialog is displayed:
- Step 3** Fill in the data fields specifying report parameters.
- Step 4** Click **Apply** when done.

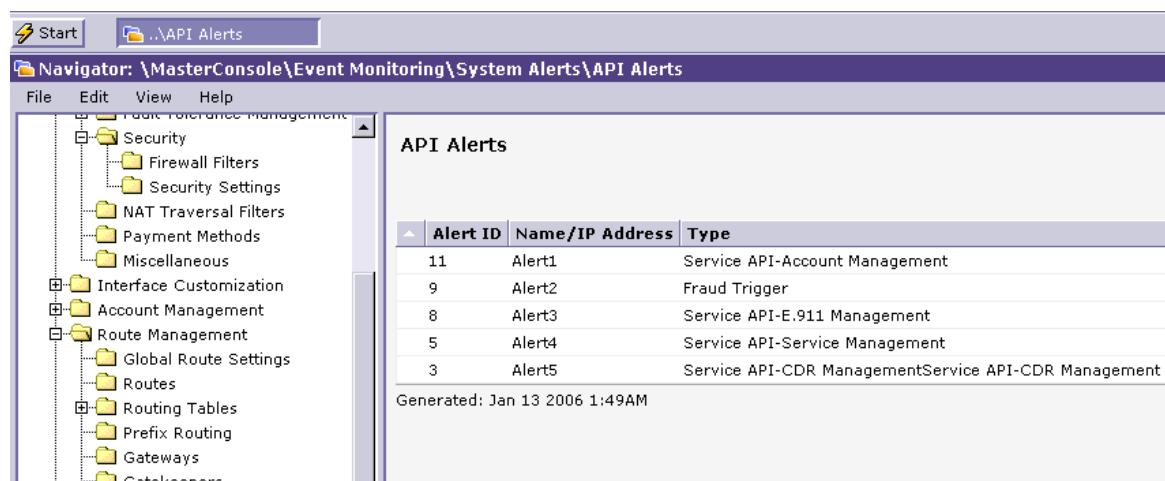
To generate a report:

- Step 1** From the Administrative Console, navigate to **Event Monitoring>Reports>System Reports>Fraud Detection**.
- Step 2** Select the report to generate.
- Step 3** Select **Edit>Generate Report**.
- Step 4** The report is generated to view, save, print, etc.

## Fraud Notification: System Alerts

VoiceMaster also permits administrator notification when fraud occurs. To alert an Administrator each time a fraud alert is triggered:

- Step 1** Configure the system fraud settings, as described in the preceding sections.
- Step 2** Select **Event Monitoring>System Alerts**.
- Step 3** Select **API Alerts**. The API Alerts window appears:



**Figure 1-83 Preparing to Trigger Fraud Detection Notification**

**Step 4** Select **Edit>Add System Alert**. The alert notification dialog pops into view:

**Figure 1-84 Adding a System Alert/Triggering Notification**

**Step 5** Name the alert.

**Step 6** Set the Alert Type. Choose Fraud Trigger in order to set automatic notification in motion when a fraud event occurs.

**Step 7** Set the administrator E-mail address.

**Step 8** Set a threshold value.

**Step 9** Select **Apply**. When a fraud event occurs, notification is sent to the configured E-mail address.

Full descriptions of the System Alerts functions are located in [System Alerts Configuration](#), which follows shortly.

### API System Alert Definitions

An API alert is used to trigger custom scripts/applications based on an event in the VM. When one of these events occurs on the VM, it will send a HTTP POST request and/or email to the URL/Address specified in the Alert configuration.

- Account Management API: Sends an alert when a account is created, modified, or deleted.
- CDR Management API: Sends an alert when a call is received by the system.
- Service Management API: When a user subscribes or unsubscribes from a Norfa/PBX service.

Each type of API sends different data as part of the HTTP POST request, these variables can be captured by the target script or application.

## NAT Traversal Filters

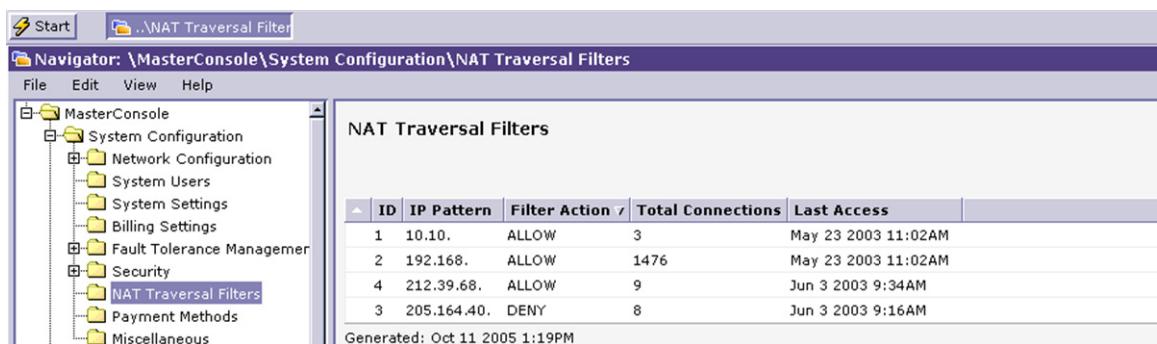
NAT Traversal Filters is also related to security. NAT translates private IP Addresses into public ones for broadcasting or routing. The nodes using such private addresses are shielded from the public network, while maintaining the ability to access it - for VoIP calls or any other network activity. NAT also counters the real limitations of public IP address distribution (companies do not have to acquire public addresses for all their working Internet nodes).

NAT parameters include:

- **ID.** Identifier that helps track changes associated with the selected NAT filter.
- **(Action) Allow.** Activates conversion of the selected private IP Address.
- **Action Deny.** Prevents this same conversion (of IP Address) from happening.
- **IP Pattern.** Displays available IP addresses for translation to public addresses.

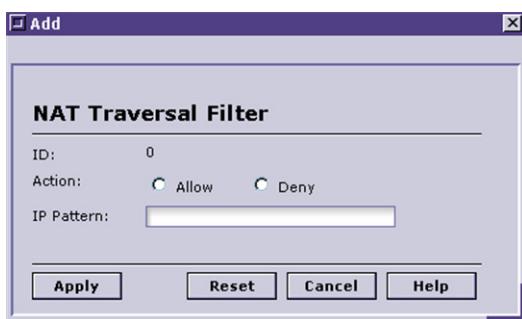
To implement NAT within VoiceMaster:

**Step 1** From the Navigator, select **System Configuration>NAT Traversal Filters**. View the NAT Traversal Filters window:



**Figure 1-85 Network Address Translation: Gateway to Configuration**

**Step 2** Select **Edit>Add NAT Traversal Filter**. The edit dialog appears:



**Figure 1-86 Configuring a NAT Filter**

**Step 3** Select Allow at the Action field to permit conversion of the assigned private IP address to a public address.

**Step 4** In the IP Pattern field, enter the private address to be translated.

---

**Note** If you set the action type to ‘Deny’, then any IP address defined will be blocked from accessing the public network.

---

**Step 5** Select **Apply**.

**Step 6** Repeat Steps 2-5 for as many IP addresses as you wish to configure for conversion.

## System Alerts Configuration

VoiceMaster includes a full set of system alert configuration options. These options relate to different, critical aspects of system functionality from performance to billing management to fraud notification.

The purpose of this section is to provide a quick overview of the nature and role of the three System Alerts functions in VoiceMaster. Configuration and use of each type of System Alert is presented in context; for instance, using alerts to trigger fraud notification (to the Administrator) was previously discussed in the Security section.

Here are the basic varieties of system alerts available to the Administrator:

- **Account Alerts.** The purpose of this billing alert mechanism is two-fold:
  - To simply inform the Administrator when a balance threshold has been breached (actions are up to the Admin, at that point)
  - To let the Admin know that the threshold has been crossed and the subscriber(s)’ accounts recharged according to settings configured in System Configuration>System Settings>General Configuration.

As is the case with nearly every configured rule in VoiceMaster, the alerts relate to a specific, administrator-defined group of clients and associated customers/subscribers.

- **Gateway Alerts.** Allows configuration of several basic (routing) network performance parameters, including thresholds to trigger alert notification.
- **API Alerts.** These alerts, when configured, run custom scripts that help monitor aspects of system performance. The Fraud Trigger setting is unique, and functions as a piece of fraud detection, as explained.

To access the system alerts:

**Step 1** Open the Navigator.

**Step 2** Select **System Alerts>API Alerts**.

**Step 3** Select the specific alert function to configure:

- Account Alerts
- Gateway Alerts
- API Alerts

**Step 4** Select **Edit>Add System Alert** to configure a new alert.

**Step 5** Select **Edit>Edit System Alert** to modify an existing alert.

**Step 6** Select **Edit>Delete System Alert** to delete an alert.

As you read the remaining chapters, system alerts will be discussed in the context of the relevant administrative subject (billing, routing, and so on).

# Fault Tolerance

Fault Tolerance, or system redundancy, is a key aspect of a robust network infrastructure. VoiceMaster is effectively a combined hardware/software solution. More specifically, it is a server-based *system* that includes physical disks, storage capacity, etc. All levels of this system are potentially vulnerable to data loss and corruption.

VoiceMaster's Fault Tolerance features safeguard all of the system levels - from the most basic to the level of stored software (module) configurations. To have confidence that all active configurations are safe, an Administrator must have the ability to perform system duplication on demand.

VoiceMaster provides this capability through the following mechanisms:

- **RAID Mirroring.** Mirroring is used to back up all disk partitions - boot, swap and root. Depending on your hardware configuration (VoiceMaster 'level'), this functionality is implemented either as 1) software RAID mirroring or 2) hardware mirroring. (Which flavor of mirroring is implemented for *your* system is explained in the following section).
- **System Replication (Synchronization).** System replication functionality covers all remaining system levels, including current configurations stored in the VoiceMaster database. During synchronization, its contents are copied from an active, 'master' server to a backup ('slave'). This enables server hot swapping from the master to the updated 'slave' should problems occur. More importantly, replication ensures that failure - even temporary - of the active server/database does not cripple VoIP service operations.

---

**Note** System replication is also useful for improving VoiceMaster performance by distributing active tasks between two servers and databases. This increases processing efficiency, facilitating a faster, more efficient call network. More details are provided below.

---

## RAID Mirroring

SysMaster provides two types of disk mirroring using RAID Mirroring 1:

- Software mirroring, the default for VoiceMaster customers who own Level 1 systems.
- Hardware mirroring, implemented on all (newer) VoiceMaster systems that are Level 2 and above.

If you have any doubts as to which hardware level describes your VoiceMaster, refer to the Installation chapter or contact SysMaster technical support staff. However, you will not need to configure the mirroring *type*. It is configured automatically to match your hardware.

The Administrator has Read-Only access to RAID Mirroring functionality. This is because mirroring is automatically configured and because any remedial actions in the case of mirroring malfunctions must be carried out by SysMaster. (Mirroring occurs at the most sensitive, critical levels of system functioning.)

---

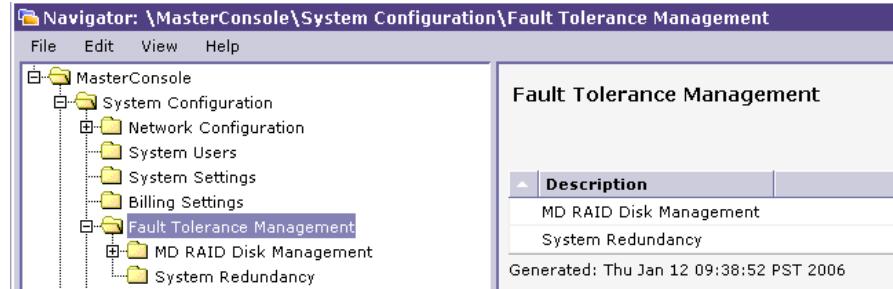
**Note** If, while observing RAID Mirroring status, you notice *Failed* status for any partition within either disk, **contact SysMaster Technical Support**. Such a status may indicate a failed disk (failures can be partial or total). In this circumstance, immediately synchronize (replicate) disk contents using the instructions in [System Replication \(Redundancy\)](#). **DO NOT attempt to operate the affected disk(s).**

---

An Administrator *can* and should monitor RAID status periodically. This confirms that the mirroring functionality is working properly. To do so:

**Step 1** Login and select **Start>Navigator** (if the Navigator is selected, ignore this step).

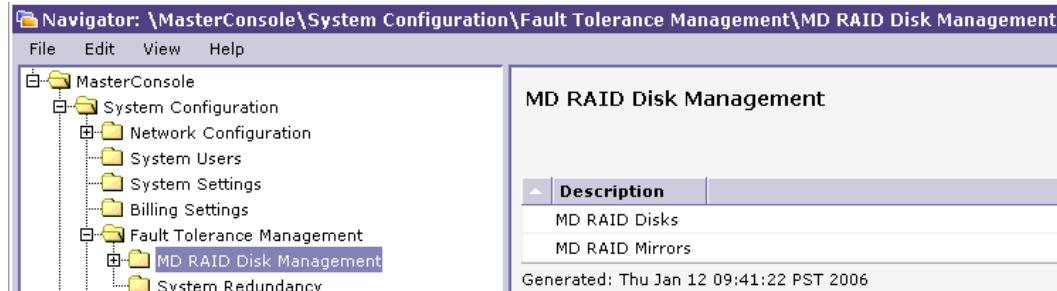
**Step 2** Open **System Configuration>Fault Tolerance Management**. The Fault Tolerance window is displayed:



**Figure 1-87 Fault Tolerance Management**

**Step 3** Select **MD RAID Disk Management**.

**Step 4** Select **Edit>Open Folder**. View the MD RAID Disk Management window:

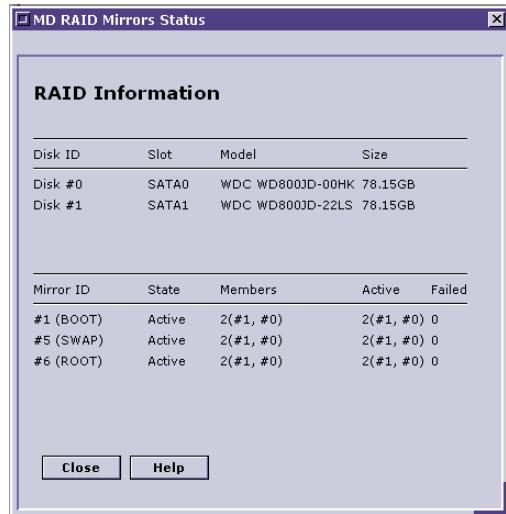


**Figure 1-88 MD Raid Disk Management Options**

**Step 5** To check disk status, select **MD RAID Disks**, then open the folder (**Edit>Open Folder**).

**Step 6** To monitor RAID mirroring status, select **MD RAID Mirrors**.

**Step 7** Select **Edit>MD RAID Mirrors Form**. An information is displayed, presenting boot, swap and root partition information for each mirrored disk:



**Figure 1-89 RAID Info Window**

**Step 8** Click **Close** when you are done.

## System Replication (Synchronization)

System Replication, or redundancy, is the second practical aspect of Fault Tolerance within VoiceMaster. System replication is a module that contains the necessary elements (algorithms, etc.) used to create, modify and synchronize database replicas. It is specifically designed for replication of the VoiceMaster database and no other.

System replication has two primary uses:

- Synchronizing primary and secondary databases to enhance the performance and availability of VoiceMaster applications. For example, an Administrator can dedicate the primary database to performing the billing and routing tasks while shifting report functionality to the secondary server. Since the production of reports is often a time-consuming process of answering user queries and producing data, shifting this task to a secondary server (database) distributes processing load and improves performance. In this scenario, the master system's *daemon* gathers report queries and passes them to the secondary system, which processes them.

---

**Note** The secondary system does not have this daemon functionality. During system replication/synchronization, interruptions may result in some report queries not being forwarded to the secondary machine.

---

- Maintaining the call network and its underlying application processes if the primary (master) server/database suffers a failure. The network continues to run, while the secondary database remains accessible, performing all tasks. The secondary device takes on all tasks it has not performed to this point. If it has been handling report functions, it now assumes routing and billing functions. If the primary server has handled *all* functions, these now shift to the (synchronized), fully activated backup.

The data replication mechanism is quite complex. First, there is synchronization. Afterwards, replication occurs.

First, all tables are unloaded from the primary database to the standby database serve, then loaded the data into the standby database. At this point, synchronization has been accomplished. Once a full ‘sync’ is performed, real-time replication can occur, which means that operations performed on the Primary Server now are executed as well on the Slave Server.

The first step in enabling replication is to create a Redundancy Configuration on the primary unit (master server). This creates an active-standby redundancy setup. The setup involves two servers: primary (master) and standby (slave) one. The two servers should be directly visible to each other on the network, and for optimal performance, should be connected to the same switch.

When this configuration is established, the slave server proactively monitors the master server. Data integrity is ensured by data replication running continuously in the background. The ‘slave’ is updated constantly with changes to the active, master server database. The slave checks the master’s ‘health’ every five minutes.

---

**Note** In order for these checks to run accurately, the two servers must have full access to each other. It is therefore recommended that no firewall sit between the two systems.

---

If an update query fails, the slave reads this as a signal that the master is down. It is configured to activate its services, effectively replacing the master. It does this by activating a 15-day license (this allows times for reconfiguration of the master server). Immediately, a full one-time replication of master to slave is enabled, including all database contents.

---

**Note** Keep in mind that system replication is enabling failover from the primary to the standby server. This means the standby must assume all routing and billing functionality, and *that* means that all gateways connected to the VoiceMaster must have assigned failover routes that include awareness of the replacement (standby) server.

---

An Administrator activates this replication using the procedures described below. All requests (from system endpoints, etc.) to the database are queued during replication. Then each query is executed individually to each machine – master and slave. Any future updates to the primary machine are now made as well to the backup, which has assumed an active role.

**Warning** Do not make changes to the slave using the WI or another method (CLI or DB management software). This enforces changes that will NOT be transferred to the master, and put the two systems in a non-synchronized state. **Do not** replicate changes from the Slave to the Master. If synchronization is interrupted by lack of network connectivity or another cause), this will overwrite all configuration changes stored on the Master. *However, once the master server is reactivated, a data migration must be performed.*

System replication is a two-part process, first making the master server replicable, then actually synchronizing the two databases. We describe each of these phases in the next sections.

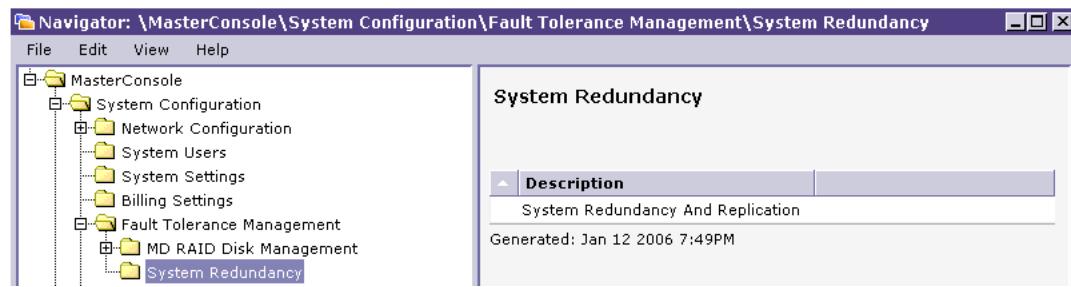
### Preparing System Replication

The first phase in the process is to configure the master server database for replication:

On the **Master** Server:

**Step 1** From the Navigator view, select **System Configuration>Fault Tolerance Management**.

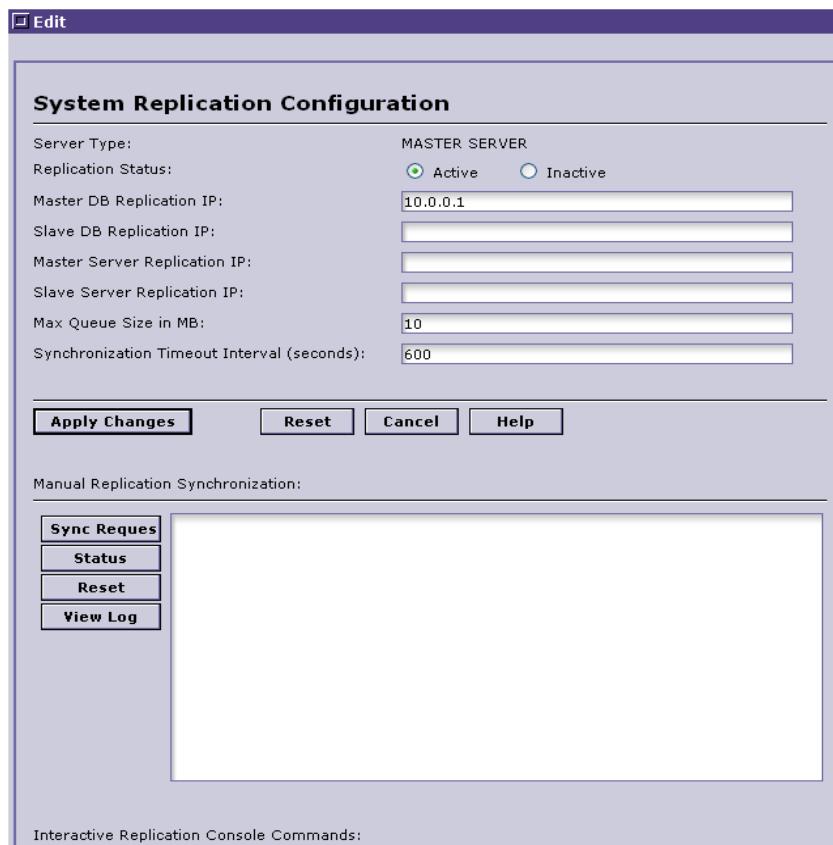
**Step 2** Select **System Redundancy**. The view changes to the following:



**Figure 1-90 System Redundancy Window**

**Step 3** Select System Redundancy and Replication.

**Step 4** Choose Edit>Edit Settings. This dialog is displayed:



**Figure 1-91 System Replication Configuration Dialog**

**Step 5** Fill in the fields at the top of the form:

- Replication Status: Set to Active.
- Master DB Replication IP: Enter the IP address for the master server database. (If this is a Level 1 or 2 system, this value is the same as that for Master server Replication ID (next field).

- (c) Slave DB Replication IP. Slave server database IP address; if it is a Level 1 or 2 system, the IP will be the same as for the server itself.
- (d) Master Server Replication IP.
- (e) Slave Server Replication IP.
- (f) Max Queue Size in MB. Maximum queue size for buffering before transfer from master to slave.
- (g) Synchronization Timeout Interval. Number of seconds master should wait before resuming ‘sync’ in case the slave fails. We recommend 600 seconds.

**Step 6** Click **Apply Changes** when done.

**Note** Do not navigate from your current Console location. Further synchronization actions will be performed shortly.

### Slave Server Replication Configuration

On the **Slave** Server, repeat the previous steps using the Administration Console. Navigate to System Redundancy and Replication. Fill out the fields, *using the same values as entered for the Master Server*. Apply the settings.

### Sample Configurations

Master Server: Level 1 or 2 Voicemaster

Slave Server: Level 1 or 2 Voicemaster

MASTER:

System Replication Configuration	
Server Type:	MASTER SERVER
Replication Status:	<input checked="" type="radio"/> Active <input type="radio"/> Inactive
Master DB Replication IP:	192.168.0.1
Slave DB Replication IP:	192.168.0.2
Master Server Replication IP:	192.168.0.1
Slave Server Replication IP:	192.168.0.2
Max Queue Size in MB:	10
Synchronization Timeout Interval (seconds):	600

**Figure 1-92 System Replication - Master**

SLAVE:

**System Replication Configuration**

Server Type:	SLAVE SERVER
Replication Status:	<input checked="" type="radio"/> Active <input type="radio"/> Inactive
Master DB Replication IP:	192.168.0.1
Slave DB Replication IP:	192.168.0.2
Master Server Replication IP:	192.168.0.1
Slave Server Replication IP:	192.168.0.2
Max Queue Size in MB:	10
Synchronization Timeout Interval (seconds):	600

**Figure 1-93 System Replication: Slave****Sample Configuration Two**

Master Server: Level 3 or higher Voicemaster

Slave Server: Level 3 or higher Voicemaster

MASTER:

**System Replication Configuration**

Server Type:	MASTER SERVER
Replication Status:	<input checked="" type="radio"/> Active <input type="radio"/> Inactive
Master DB Replication IP:	192.168.0.3
Slave DB Replication IP:	192.168.0.4
Master Server Replication IP:	192.168.0.1
Slave Server Replication IP:	192.168.0.2
Max Queue Size in MB:	10
Synchronization Timeout Interval (seconds):	600

**Figure 1-94 Level 3/4 Master Replication Settings**

SLAVE

**System Replication Configuration**

Server Type:	SLAVE SERVER
Replication Status:	<input checked="" type="radio"/> Active <input type="radio"/> Inactive
Master DB Replication IP:	192.168.0.3
Slave DB Replication IP:	192.168.0.4
Master Server Replication IP:	192.168.0.1
Slave Server Replication IP:	192.168.0.2
Max Queue Size in MB:	10
Synchronization Timeout Interval (seconds):	600

**Figure 1-95 Slave Settings - Level 3-4 Replication**

### Creating a Database Replica

Once both master and slave database servers are configured, it is time to actually replicate the contents of the master database to the slave. This is in itself a two-part procedure:

- Initiating an initial Manual Synchronization to send the entire master server DB to the slave
- Commencing Interactive Replication (real-time replication).

Manual Replication Synchronization ensures that both master and slave database servers will be synched. The process is automated and involves minimum Administrative actions.

Here is a quick look at the Manual Replication Synchronization options:

- **Sync Request.** Starts replication when selected.
- **Status.** Shows replication status.
- **Reset.** Resets manual replication synchronization from beginning, interrupting sync in progress.
- **View Log.** Shows log file of the synchronization process up to the point View Log is selected.

Initiate the process on the *master server* by following these steps:

- Step 1** Recheck replication settings for both servers configured in the previous section.

---

**Note** This procedure assumes that the System Redundancy window remains your navigation location within the Administration Console. If this is not the case, select Fault Tolerance Management and the System Redundancy folder.

---

- Step 2** Select **System Redundancy and Replication** from the System Redundancy window, then choose **Edit>Edit Settings**.

- Step 3** The System Replication Configuration dialog is displayed. Look at the **Manual Replication Synchronization** screen beneath the configuration settings.

- Step 4** Select the **Sync Request** button. Synchronization will begin within 1 minute. During this time, you can click the **Status** button to check the progress.

- Step 5** When the status window shows replication completed, the sync process is finished. Interactive Replication will automatically begin.

### Interactive Replication

You can also activate *interactive replication* from the Interactive Replication Console interface. The command to start replication is the **Start** button located on the left-hand side of the menu. The selection options for Interactive Replication are (including Start):

- **Status.** Displays interactive replication status.
- **Start.** Starts the replication process.
- **Stop.** Stops the replication.
- **Pause.** Pauses the process for later restart; queries are queued during pause time.
- **Sync.** Resumes queries transmission after a pause has been issued.
- **Reload Cfg.** Reloads the configuration file.
- **File Dump.** Retrieves ‘dump’ log file where replication transactions are stored.

# Interface Customization

One of the flexible tools that VoiceMaster places in the hands of system administrators is the ability to customize application interfaces. We say *interfaces* because these features facilitate the customization of:

- The Administration Console itself
- The CRM web site(s) created to allow potential and actual customers to view the VoIP service, register for subscription and manage their accounts.

VoiceMaster Interface Customization functionality divides into four categories:

- **Currency Settings.** This feature enables the definition of international currencies. A reservoir of currencies is formed, any of which may be applied for system billing purposes. Includes exchange rate definitions and additional descriptive currency components.
- **Custom Color Schemes.** Create and apply custom color schemes for the Administration Console itself. Save and store the schemes, and use as desired. For visual variety and comfort.
- **Location Definition.** Used to define all possible system locations that may participate in the call network. Definitions may be used for configuration of routes, billing and so on.
- **CRM Interface.** The aspect of Interface Customization devoted to configuring the elements of any given CRM Interface (web site). Includes these sub-functions:
  - CRM Settings. Lets you configure essential functional and display components of the CRM interface.
  - Custom Statements. Create custom statements to send to customers. Each can be designed to include or exclude visual aspects and statement summary information.
  - SSL Configuration. This function enables the configuration and implementation of SSL (security) attributes to apply to the CRM site.
  - Virtual Web Services. The gateway to configuring and managing the various CRM sites (the number to be created at the Administrator's discretion).
  - Web Templates. Configure and modify templates that create the actual visual display and interface for a particular CRM site.

## Currency Settings

Currency management lets you configure a pool of currencies to be used in conjunction with the VoiceMaster base currency (USD). By assigning various essential parameters, currencies are defined and available for use as the system billing currency (if desired). Of course, this includes an updated exchange rate (the Administrator must monitor such rates), so that charges can be accurately converted and calculated in the new currency.

Currency functionality in VoiceMaster includes the ability to generate call history reports and billing rates (at the CRM site) in a selected currency. Monthly statements may also be generated in any configured currency. All currency settings can be made on a per-account basis, so that one customer may receive statements and calculate bills in an entirely different currency than another.

---

**Note** All international currencies should be present on the system or can be downloaded from SysMaster.

---

Currency definition parameters include:

- **Currency Code.** Specifies an internal currency code - system assigns automatically.
- **Currency Name.** Specifies the currency name administrators use for reference.
- **Currency Name.** Short Name of the currency.
- **Abbreviation.** A symbol (set of symbols) of the currency used as a prefix next to quoted amounts.
- **Symbol.** Appropriate prefix next to quoted currency amounts.
- **Subdivision Name.** Specifies the name of a subdivision unit of the currency. E.g. for US dollars the 1 cent has the name 'cent'.
- **Subdivision Symbol.** Specifies the symbol of a subdivision unit of the currency. E.g. for US dollars the 1 cent has the symbol 'c'.
- **Subdivision Rates.** Exchange rate of 1 currency unit to 1 USD.

### Configure Currency Settings

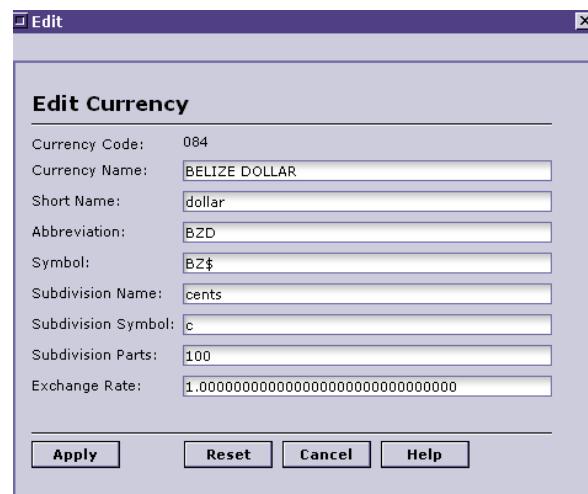
These steps, followed correctly, configure currency settings:

- Step 1** Open the Navigator, if not currently in view.
- Step 2** Select **Interface Customization>Currency Settings**.
- Step 3** The Currency Settings window is displayed:



**Figure 1-96 Currency Settings Selected**

- Step 4** Select the currency whose parameters you wish to edit and then **Edit>Edit Settings**. This dialog presents itself.



**Figure 1-97 Editing Algerian Currency Settings**

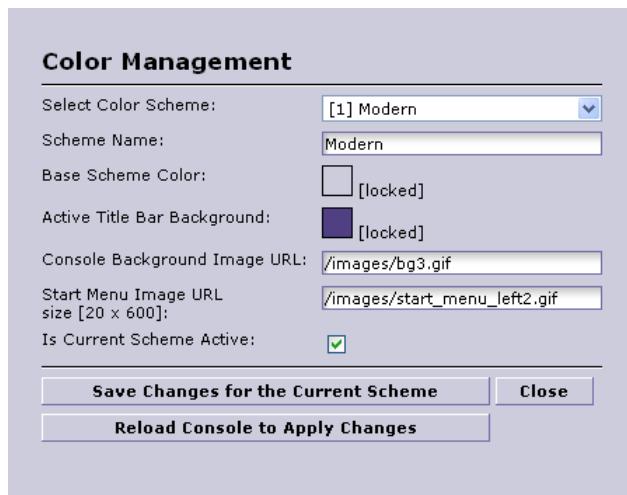
- Step 5** Modify any existing setting. (In most cases, the exchange rate will be of most interest as a field that frequently requires update.)
- Step 6** Select **Apply** to save changes.

## Custom Color Schemes

Configuring custom color schemes is a way to provide visual comfort while using the Administration Console. Some users may just enjoy a variety of ‘looks’ during long hours of system configuration and monitoring.

To configure custom color schemes for your Administration Console:

- Step 1** From the Navigator view, select **Interface Customization>Custom Color Schemes**. The Color Schemes window replaces the current view:

**Figure 1-98 Custom Color Schemes: No Small Window**

- Step 2** Choose a color scheme from the pull-down from the pool of available themes.
- Step 3** Name the scheme for reference.
- Step 4** Enter a URL for a console background image (assumes these are present on your system).
- Step 5** Set a directory path/file name for a Start Menu image.
- Step 6** Click the **Save Changes for the Current Scheme** button to save your work.
- Step 7** To immediately apply changes made, select **Reload Console to Apply Changes**. The Administration Console will reload.

## Location Definition

Location Definition permits the definition of states and countries within the call network. This informational data is then used as a parameter in additional configuration contexts.

To define new VoIP call locations, just follow these instructions:

- Step 1** Open the Console and Navigator, if not currently available.

- Step 2** Select **Interface Customization>Location Definition**. The Location Definition window appears:

The screenshot shows a software interface titled 'Navigator: \MasterConsole\Interface Customization\Location Definition'. On the left is a tree view of the 'MasterConsole' structure, including 'System Configuration', 'Interface Customization' (which is expanded to show 'Currency Settings', 'Custom Color Schemes', 'Location Definition', 'CRM Interface', 'Account Management', 'Route Management', 'Rate Management', 'Batch Management', 'PBX Management', 'Custom Modules', 'Event Monitoring', 'Support Automation', 'Lead Automation', 'Web Chat Automation', 'Sales Automation', 'Web Traffic', 'Content Management', 'Survey Management', 'Global Management', and 'SS7 Signal Management'). On the right is a table titled 'Location Definition' with the following data:

ID	Name	Abbreviation	Type
0	Non-US/Other	NONE	State
1	Alabama	AL	State
2	Alaska	AK	State
3	Arizona	AZ	State
4	Arkansas	AR	State
5	California	CA	State
6	Colorado	CO	State
7	Connecticut	CT	State
8	Washington D.C.	WD	State
9	Delaware	DE	State
10	Florida	FL	State
11	Georgia	GA	State
12	Hawaii	HI	State
13	Idaho	ID	State
14	Illinois	IL	State
15	Indiana	IN	State

**Figure 1-99 Location Definition**

- Step 3** Select **Edit>Add Location**:



**Figure 1-100 Adding a Location**

- Step 4** Name the location.  
**Step 5** Assign an abbreviation.  
**Step 6** Define location type (country or state).  
**Step 7** Select **Apply** to save it.

To modify an existing location definition:

- Step 1** Select **Interface Customization>Locations Management**.  
**Step 2** Select the state or country to modify.  
**Step 3** Select **Edit>Edit Location**.  
**Step 4** When the dialog is displayed, change any parameters and apply changes.

Deleting a given location is as simple as:

- Step 1** Select **Interface Customization>Locations Management**.
- Step 2** Select the state or country to delete.
- Step 3** Choose **Edit>Delete Location**.
- Step 4** Confirm the deletion to remove it from the list.

## CRM Interface

CRM Interface, the last Interface Customization function, is the most diverse. It is your avenue to control of CRM web sites and their contents. The four

- Configure all aspects of the CRM through a CRM Settings function dialog.
- Create custom statements for different users (VoIP call customers).
- Configure secure access to CRM sites by applying SSL (secure [socket] login to them).
- Configure Virtual web services for coherent management of the various CRM sites.
- Create a library of templates for use as the visual ‘face’ of these CRM sites.

Procedures for turning this functionality into reality follow.

## CRM Settings

The CRM Settings function, the first of the subfolders under **CRM Interface**, provides a set of general parameters whose definitions affect 1) CRM functionality and contents, and 2) CRM visual aspects.

**CRM Cache.** Enable cache on the CRM server.

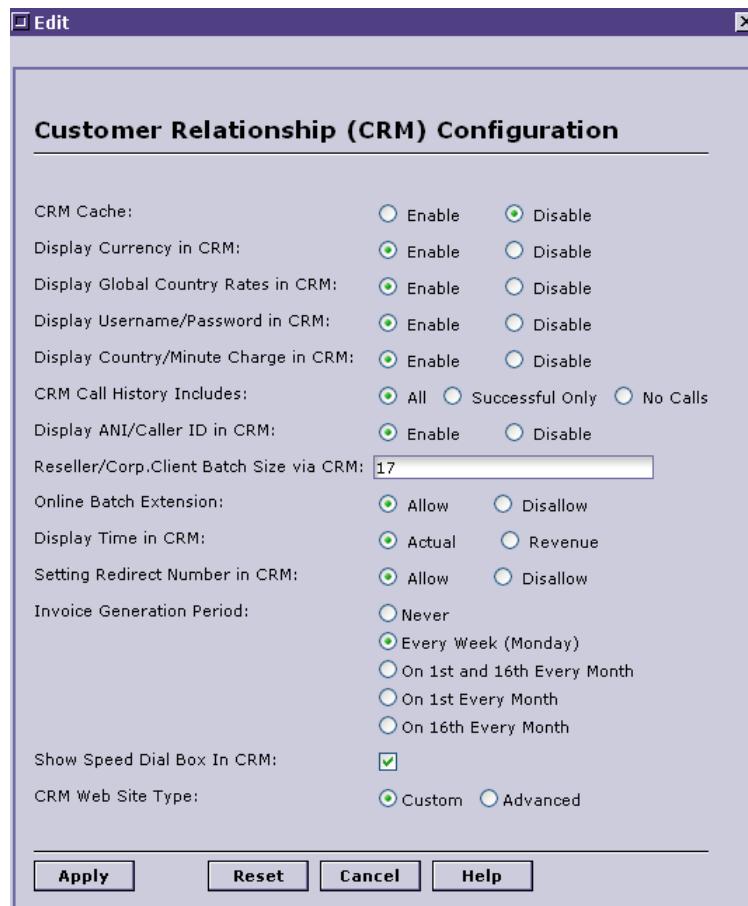
- **Disable Currency in CRM.** Select to block customers from viewing currency used in the balance/call history reports.
- **Disable Global Country Rates in CRM.** Select to block the CRM’s display of country rates.
- **Disable Username/Password in CRM.** If activated, this option prohibits username/password login (only PIN authentication will work).
- **Country/Minute Charge in CRM.** When set, displays the minute charge by country during a call. CRM is configured to calculate amounts to enable display.
- **CRM Call History.** Reporting to customer of all call attempts, successful calls only or no calls. If the last option is selected, Call History will be blank.
- **ANI/Caller ID in CRM.** Geared to SoftPhone use, permits ANI or Caller ID authentication for callers using SoftPhone module situated on CRM site.
- **Reseller/Corp. Client Batch Size via CRM.** Size of PIN batches that can be distributed via the CRM.
- **Online Batch Extension.** Allow or disallow extension of configured batch size (‘Allow’ increases previously set limit).
- **Display Time in CRM.** Actual or Revenue are display options. This is relevant for billing configurations where the customer is not charged for full length of call. In such cases, customer may mistake actual time for billed time. ‘Revenue’ time will always portray billed time accurately, no matter the customer’s call plan.
- **Setting Redirect Number in CRM.** Select ‘Allow’ to display the system redirect number.

- **Invoice Generation Period.** Specifies invoice generation frequency:
  - Never
  - Every Week (on Monday)
  - 1st and 16th of each month
  - 1st of every month
  - 16th of each month
- **Speed Dial Box in CRM.** Selecting this lets user configure a list of speed dial numbers for quicker dialing. When enabled, displays a Speed Dial Box in CRM ‘Profile’ section. Speed dialing programs a long number string into a single number, so that 1221843553 could be represented as setting “1”, and so on.
- **CRM Web Site Type.** Options are *Custom* or *Advanced*.

### Configuring CRM Settings

To configure CRM settings, follow this procedure:

- Step 1** Open the Navigator, if not currently available.
- Step 2** Select **Interface Customization>CRM Interface**.
- Step 3** Select **CRM Settings**.
- Step 4** Select **Open Folder**. The entry on the CRM Settings window will remain “CRM Settings.”
- Step 5** Now select **Edit>Edit Settings**. The edit dialog appears:



**Figure 1-101CRM Settings Configuration**

**Step 6** Set all desired parameters.

**Step 7** Select **Apply** to update the CRM Settings configuration to reflect changes.

---

**Note** All administrative work with this function is in an editing mode. There is also no ‘delete’ option as well because of the generic/global impact of these actions on CRM functionality and display.

---

## Custom Statements

Custom Statements is a useful CRM Interface feature. Just as the name suggests, it facilitates the configuration and modification of custom statements for select customers (as with each of the functions in this section, it affects *only* VoIP service customers who register and use the service via CRM sites).

Custom statement options include:

- Header definitions (parameters)
- Footer definitions
- Account tax settings

- Call details

### Add Custom Statement

To add a custom statement and define its contents, execute this procedure:

**Step 1** Select **Interface Customization>CRM Interface**.

**Step 2** Select Custom Statements.

**Step 3** Choose **Edit>Add Custom Statement**. The Custom Statement Form appears:

The screenshot shows the 'Custom Statement Form' dialog box. It has a title bar 'Add' and a main area titled 'Custom Statement Form'. The form contains the following fields:

- Statement Name: [Text Box]
- Master ID: [Text Box] (Value: 0)
- Active:  Active  Inactive
- Enable Repeat Header:
- Logo URL: [Text Box]
- Corp. Info Header: [Text Box]
- Statement Header: [Text Box]
- Statement Footer: [Text Box]
- Show Account Summary On Statement:
- Account Summary Header: [Text Box]
- Account Summary Footer: [Text Box]
- Show Account Activity On Statement:
- Account Activity Header: [Text Box]
- Account Activity Footer: [Text Box]
- Show Account Tax On Statement:
- Account Tax Header: [Text Box]
- Account Tax Footer: [Text Box]
- Show Call Details On Statement:
- Call Details Header: [Text Box]
- Call Details Footer: [Text Box]
- Disable Call Rates:

The base directory for the files is "/home/manager/upload/crm/templates/".

At the bottom are four buttons: Apply, Reset, Cancel, and Help.

**Figure 1-102Building a Custom Statement for CRM-Linked Customers**

**Step 4** Set the parameters for the all aspects of a custom statement (described in the previous section).

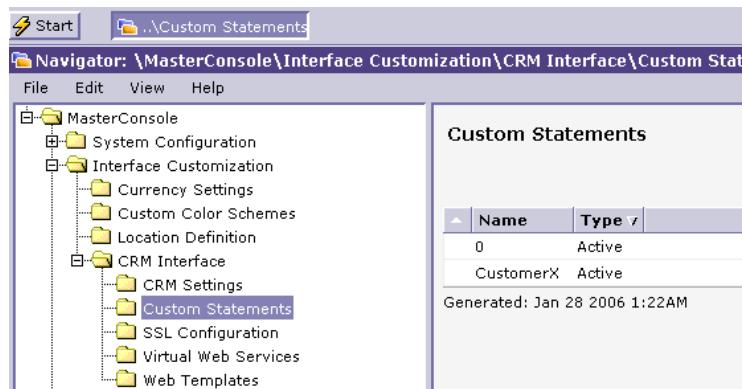
- Statement name and Master ID are mandatory.
- Define headers and footers as desired.
- Include or exclude account summaries per statement.
- Do the same for account activity, account tax and call details - and call rates.

- Step 5** Select **Apply** to save the statement definitions and add it to the stock of custom statements.

### Modify Custom Statement

To modify a custom statement:

- Step 1** Open the Navigator, if not currently open.
- Step 2** Select **Interface Customization>CRM Interface**.
- Step 3** Select **Custom Statements**, then select the statement to edit ('CustomerX' in this example):



- Step 4** Select **Edit>Edit Custom Statement**.
- Step 5** The same Custom Statement Form is again produced, this time with CustomerX parameters displayed:

The base directory for the files is "/home/manager/upload/orm/templates/".

**Figure 1-103CustomerX Custom Statement**

- Step 6** Change any parameter settings - radio buttons, check boxes and text entry definitions as required to effect desired changes.
- Step 7** Select **Apply** to redefine and save the Custom Statement.

### Delete Custom Statement

To delete any existing custom statement:

- Step 1** Open the Navigator, if not currently open.
- Step 2** Select **Interface Customization>CRM Interface**.
- Step 3** Select **Custom Statements**, then select the statement to delete.
- Step 4** Choose **Edit>Delete Custom Statement**.
- Step 5** Confirm the deletion at the prompt or cancel to abort it. Confirmation removes the statement from the Custom Statements list and from the system database.

## SSL Configuration

SSL is the means by which security functions and checks are applied to CRM sites. SSL certification established a secure login for those (customers) accessing the site while providing assurance that the data they provide (i.e., credit card information) will be safeguarded.

SSL configuration consists of three phases:

- **CSR File Generation.** This is in effect an application form for SSL certification. On completion, it is sent to a SSL authority for certification.
- **Certificate Installation.** This is the mechanism by which the Admin downloads certifying authority approval and activates SSL for the CRM site. This in turn breaks down into two general procedures:
  - Certificate Installation Download
  - Certificate Installation Upload

### CSR File Generation

The first step to configuring CRM sites for SSL (secure) operation is to generate the CSR file and send it to an SSL certifying authority. The authority verifies your firm's validity and issues the certificate.

To generate the CSR file:

- Step 1** Open the Administration Console and Navigator, as needed.
- Step 2** From the Navigator, select **Interface Customization>CRM Interface**.
- Step 3** Select **SSL Configuration**:

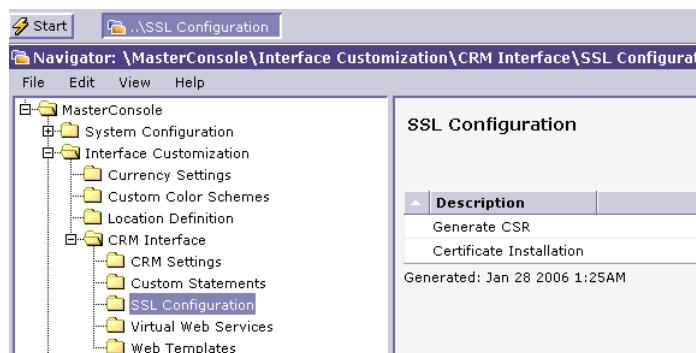


Figure 1-104SSL Configuration Functions in View

- Step 4** Select **Generate CSR**, then **Edit>Edit Settings**. The generation form is displayed:

Figure 1-105Generating a Certificate File

- Step 5** Enter all company contact information, including Web domain.

- Step 6** Select **Apply** to confirm changes.
- Step 7** Locate the E-mail address for the SSL certification authority (research and identify this authority now if you have not done so).
- Step 8** Send your certificate as a file attachment in an E-mail.
- Step 9** Wait for the authority to notify you that SSL certification is in force.

### Certificate Installation (Download)

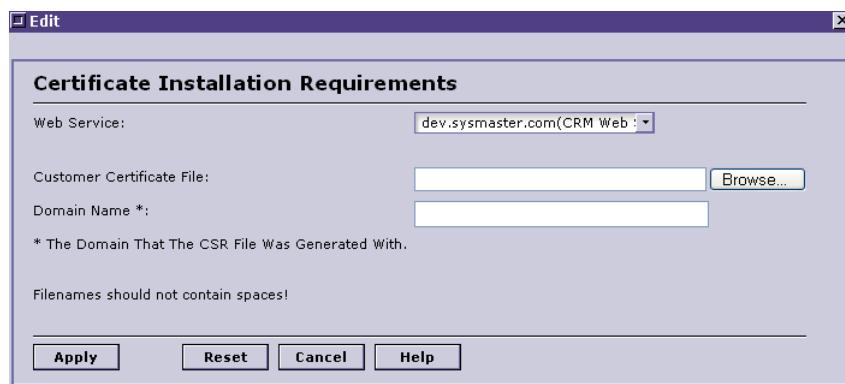
Once your firm has received notification of SSL certification, you can install the certificate.

---

**Note** The certifying authority must send you the file of certification before this procedure can be performed.

---

- Step 1** Open the Administration Console and Navigator, if necessary.
- Step 2** From the Navigator, select **Interface Customization>CRM Interface**.
- Step 3** Select **SSL Configuration**.
- Step 4** This time, select **Certificate Installation** from the SSL Configuration window.
- Step 5** Make **Edit>Edit Settings** your next selection. View the Certification Installation dialog:



**Figure 1-106** Downloading the SSL Certificate File

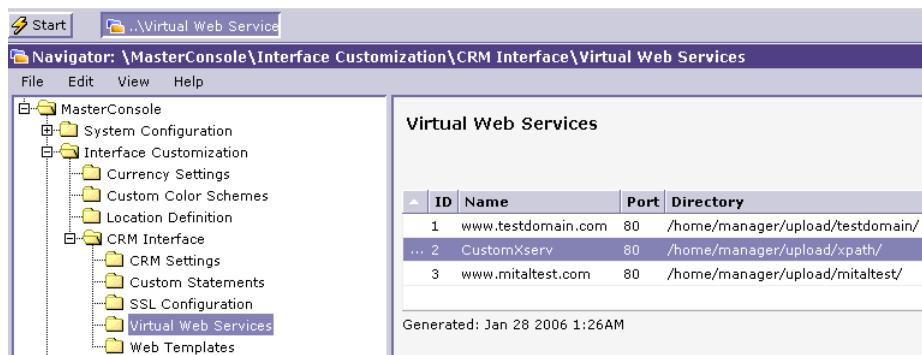
- Step 6** Identify the web service (default-selected) that you use to manage the CRM site.
- Step 7** Browse your directories to locate the Customer Certificate File, then open and load it into the Customer Certificate File entry box.
- Step 8** Enter the domain name used to generate the *CSR* file originally (previous procedure).
- Step 9** Select **Apply**. SSL certification for the CRM web site is now configurable. In the next section we describe how to upload the certificate file to the site, completing the process.

### Certificate Installation (Upload)

To upload the downloaded certificate file to the web site, thus activating SSL functionality:

- Step 1** Open the Administration Console and Navigator.
- Step 1** From the Navigator, select **Interface Customization>CRM Interface**.

**Step 2** Select Virtual Web Services and its window is activated:



**Figure 1-107Virtual Web Services List**

**Step 3** Select the URL/domain name that describes the CRM site for which the certification is intended (remember, multiple CRM domains may exist).

**Step 4** Select **Edit>Upload Cert Files**. The upload form displays:



**Figure 1-108Uploading an SSL Certificate File**

**Step 5** At the Customer Certificate field, select Browse to locate and load the certificate file received from the authority.

**Step 6** Alternately, browse, locate and load the CA Certificates File (a compilation of multiple certificate files).

---

**Note** Step 6 is necessary if the authority has sent multiple files of certification. **Before you can upload this group of files, you must first concatenate them into one file** (the file that you select in this step).

---

**Step 7** Select **Apply** to upload the file to the CRM domain/site. Certification is complete.

## Virtual Web Services

The Virtual Web Services function enables the management of the hosted CRM sites that are the point of contact between Web-using call customers and the VoIP service. It enables the configuration of the essential elements of such a service/site:

- Site URL that identifies the site in the language of the Web: <http://www.mycompany.com>
- Listening Port to accommodate HTTP requests (customer actions)

- Web site root directory.

### Add a Web Service

To configure a new Virtual Web Services

**Step 1** At the Navigator view, select **Interface Customization>CRM Interface**.

**Step 2** Select **Virtual Web Services**. View the window shown in Figure 5-59.

**Step 3** Choose **Edit>Add Web Service**. The interactive dialog is displayed:



**Figure 1-109Adding a Web Service**

**Step 4** Enter each parameter (described above):

- Web Service Name (URL)
- Listen Port
- Root Directory. (Please note instructions beneath this field within the dialog.)

**Step 5** Select **Apply** to confirm and save the new web service.

### Edit an Existing Web Service Configuration

**Step 1** Repeats Steps 1 and 2 from the previous section.

**Step 2** Select the Web Service from the Virtual Web Services page to edit.

**Step 3** Choose **Edit>Edit Web Service**.

**Step 4** View the dialog from Figure 5-61, with the currently configured parameters. Change any at will.

**Step 5** Select **Apply** to save changes.

### Delete a Web Service

To remove any service from the group of managed Web Services:

**Step 1** Navigate to the Virtual Web Services window, as explained in Add a Web Service above.

**Step 2** Select the specific service to delete.

**Step 3** Go with **Edit>Delete Web Service** from the Edit menu.

**Step 4** Confirm the deletion at the prompt.

## Web Templates

This last function within the CRM Interface folder facilitates the creation and modification of web templates that can be applied to managed CRM sites.

Each CRM interface is based around the program *if.cgi*. This is the mechanism that links the VoiceMaster database with the CRM site, for it pulls dynamic content out of the database and presents it through the web server. What the customer sees when he navigates to the CRM site is the result of that behind-the-scenes process.

The CRM site itself consists of both static and dynamic web pages. Static web pages are written in HTML and can be modified directly. Dynamic pages are created using template files, which can be modified to change the output of the *if.cgi* program.

The CRM web site is based on the Apache web server and uses this structure:

```
/home/manager
-->upload/crm --- this is the root directory for the web site.
-->upload/crm/templates --- this is the location of all template files used by
if.cgi
```

These directories are accessible via FTP. You can connect to them using a standard FTP Client to the VoiceMaster IP address.

Then login using:

```
username: manager
password: <serial number >
```

(the serial number is used by default, if you have changed the manager user password using the System Configuration, then you will need to use that password)

---

**Note** The Voicemaster includes a ‘starter’, sample website which can be modified or completely replaced.

---

### Template Structure

Each template has four sections, and each section, or area, is effectively a unique sub-template. The template results from combining these four sub-templates into a whole.

Template Areas:

- Header - the top and left menu of the page
- Submenu - the menu bar that lists the actions for the page
- Main - the main output of the *if.cgi* program
- Footer - the bottom of the page

What follows is the relevant source code for the page shown in the figure. The template files used for the page are shown as comments in the source.

```
<html>
```

```
<!--account-h.tl-->
```

```
<head>
<title>NORFA | Management</title>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
<link href="/nfstyles.css" type="text/css" rel="stylesheet">
<style type="text/css">
<body>
<!--prof-h.tl-->
<!--spo_welcome.tl-->
<!--account-f.tl-->
</body>
</html>
```

- Header - account-h.tl
- Submenu - prof-h.tl
- Main - spo\_welcome.tl
- Footer - account-f.tl

## Stylesheets

The fonts and colors of the CRM is mainly controlled by the stylesheet used for the page. Modifying a style sheet file will change the look of all the pages that reference it.

---

**Note** A page can have specific styles defined whether it is static or dynamic.

---

For example, the color of buttons in website forms are controlled by this portion of the stylesheet:

Determines the color, text parameters and border of a button when not pressed.

```
.classButOff{
    color:white;
    font-family: verdana,helvetica;
    font-size: 11px;
    font-weight: bold;
    border-bottom: #EE5700 1px solid;
    border-left: #FFB772 1px solid;
    border-right: #EE5700 1px solid;
    border-top: #FFB772 1px solid;
    background-color: #FF9B49;
    cursor:hand;
}
```

Determines the color, text parameters and border of a button when pressed.

```
.classButOn{
    color:white;
    font-family: verdana,helvetica;
    font-size:     11px;
    font-weight: bold;
    border-bottom: #FFFFFF 1px solid;
    border-left:  #660000 1px solid;
    border-right: #FFFFFF 1px solid;
    border-top:   #660000 1px solid;
    background-color: #EA6A00;
    cursor:hand;
}
```

---

**Note** For more information on Cascading Style Sheet standard attributes and their use please refer to:  
<http://msdn.microsoft.com/library/default.asp?url=/workshop/author/css/reference/attributes.asp>  
<http://www.htmlhelp.com/reference/css/>

---

## Template Definition Parameters

The key fields in the dialog box associated with creating templates (procedure follows shortly) include:

- Fields: Run - This is "run" value that is passed to if.cgi. This value determines which template definition will be used for the page. The parameters can be passed using HTTP GET or HTTP POST. Here is an example using HTTP GET:

`http://123.123.123.1/cgi-bin/if.cgi?run=welcome`

- Identifier - This is an optional parameter that can be passed to if.cgi in order create several versions of a page with different templates. For example, if you wanted to display an alternate welcome page for certain types of users, you would create a template definition like this:

`http://VM_IP_Address/cgi-bin/if.cgi?run=welcome&identifier=reseller1`

---

**Note** After setting up the template, you will need to create the “account-reseller1-h.tl” (template name) file in the /home/manager/upload/crm/templates directory. Once this is done, this alternate template will be used when the identifier is specified.

---

- Official Name - This is a descriptive field used to identify the template.
- Header - Specify the header template.
- Footer - Specify the footer template.
- Submenu - Specify the submenu template.
- Main - Specify the main template.

- Type - Specify which portions of the template will be displayed on the CRM site. (Secured is special type of template which will be used in future versions of the template system. Currently, this type is not used.)
- Script - Indicates a script that should be executed when the template is used.

---

**Note** NOTE: Most run parameters require that the user be logged into the CRM. This is tracked using a session id which can be generated by the login page:

---

[http://VM\\_IP\\_Address/cgi-bin/if.cgi?run=log](http://VM_IP_Address/cgi-bin/if.cgi?run=log)

## Dynamic Content

When a user calls a dynamic page, the if.cgi will query the database passing information obtained using HTTP POST or HTTP GET. It will then parse the template file and insert the content from the DB where specified by the template.

Each template has a predefined set of Variables, Zones and Tables. At the top of each template is a list of the dynamic content available for the template.

Template files make use of three types of dynamic content which are inserted by the if.cgi program:

- Variables - These are used to display a single field from the database. When including a variable in a template, it should begin and end with "##". Here is an excerpt:

```
<p class="note">  
    Account Number: <strong>##acctid##</strong> <br>  
    Account Type: <strong>##acct_type##</strong> <br>  
    Account Balance: <strong>##currency####balance##</strong> <br><br>
```

There are 4 variables used in this portion of the template:

```
##acctid##  
##acct_type##  
##currency##  
##balance###
```

When viewing this page, these get replaced with the value of the variables:

```
##acctid##= 1001002  
##acct_type##= Active User  
##currency##= $  
##balance###= -30.54
```

- Zones - These are blocks of html which are displayed or not displayed depending on the output of the if.cgi program. Zones are dependant upon System Configuration options as well as the modules installed on the Voicemaster.

---

**Note** If you disable a CRM option or do not have a required module, zone content will not be displayed.

---

Zones are defined using this format: <!-- #BEGINZONE zonename -->

In the welcome page, a zone is used to display the fields for the Custom Service Plan module. This module allows you to create recurring or signup charges. If you do not have the module installed, the content between #BEGINZONE and #ENDZONE will not be displayed.

<!-- #BEGINZONE plan -->

Plan Monthly Charge: <strong>##currency####monthly\_charge##</strong><br>

First Number Charge: <strong>##currency####first\_number\_charge##</strong><br>

Additional Number Charge: <strong>##currency####plus\_number\_charge##</strong><br>

Plan Account Limit: <strong>##batch\_size##</strong><br>

Current Accounts: <strong>##acctcnt##</strong><br><br>

<!-- #ENDZONE plan -->

- Tables - These are table rows and/or columns are need to be repeatedly created to display a list of variables. They are populated according to the number of rows and/or columns are returned from the database.

On the welcome page, a dynamic table is used to display the DID numbers a user has currently been assigned, and a drop down menu of routing actions that can be used for this number. If the user has only 1 number assigned, only 1 row will be shown and 2 rows for 2 numbers, etc.

```
<!-- #BEGINTABLE numbers -->
<tr><td width=30% align="left" valign=top class=normal
style="border-width:0;"><b>##dnis##</b></td>
<td width=70% align="left" class=normal style="border-width:0;" nowrap>
<form action=/cgi-bin/if.cgi method=POST>
<input type=submit value="Route This Number To My: " name=submit
style="height:22;width:200" class="classButOff" onFocus="this.blur()"
onMouseDown="this.className && (this.className
e=&#0039;classButOn&#0039;)" onMouseUp="this.className &&
(this.className=&#0039;classButOff&#0039;)" onMouseOut="this.className &&
(this.className=&#0039;classButOff&#0039;)">
<input type=hidden value="switchnum" name="run">
<input type=hidden value="##dnis##" name="number">
<input type=hidden value="##sub##" name="sub">
<select size=1 name=service_id class="formElement">
<option value=1 ##service1##>PBX/Centrex Service</option>
<option value=2 ##service2##>Voicemail Service</option>
<option value=4 ##service4##>Conference Service</option>
<option value=8 ##service8##>Follow-me Service</option>
<option value=32 ##service32##>Virtual Fax Service</option>
<option value=128 ##service128##>Virtual Office Service</option>
<option value=64 ##service64##>DID/ANI CallBack</option>
</select>
```

```

</form>
</td></tr>
<!-- #ENDTABLE numbers -->

```

## Templates Use With Virtual Web Services

For Voicemaster systems with the “Virtual Web Services” module, the template system works in a slightly different manner. When a Virtual Website is used, the web server will use an alternate directory as the web server root. In this case, the server will first try to locate templates in the Virtual Website root, and if it can not find the template in this directory, it will fall back to the default web server root.

For example:

```

(www.defaultdomain.com)
Default Web Site → /home/manager/upload/crm
Default Templates → /home/manager/upload/crm/templates

(www.virtualdomain.com)
Virtual Web Site → /home/manager/upload/site2
Virtual Templates → /home/manager/upload/site2/templates

```

In this configuration, when the URL http://virtualdomain is accessed, the webserver will look for the required templates (eg. account-h.tl) in the directory:

/home/manager/upload/site2/templates

If the template does not exist there, it will use the file in:

/home/manager/upload/crm/templates

## Adding a Web Template

To add a template to the stock of usable CRM templates, do the following:

- Step 1** Log in to the Console and open Navigator.
- Step 2** Select **Interface Customization>CRM Interface**.
- Step 3** Select Web Templates, and its window is displayed:



**Figure 1-110Web Templates Window**

- Step 4** Select **Edit>Add Template**. The creation dialog for templates comes into view:



**Figure 1-111Creating a Template**

- Step 5** Name the new template.
- Step 6** Define each parameter. *Refer to the section overview material for a refresher on any definitions/explanations for a given parameter.*
- Step 7** Mark all subtemplate types represented within the new template.

---

**Note** The types selected should match those configured above. Conversely, any template that does not include any subtemplate should have that ‘type’ box left unchecked.

---

- Step 8** Select **Apply** to save changes.

### Modify a Template

Just follow these steps to modify an existing template:

- Step 1** Log in to the Console and open Navigator.
- Step 2** Select **Interface Customization>CRM Interface**.
- Step 3** Select Web Templates, and its window is displayed.
- Step 4** Click on the template to modify. The Edit dialog displays:



**Figure 1-112**Editing a Web Template

**Step 5** Modify any parameter or field.

**Step 6** Select **Apply** to save changes.

### Web Template Deletion

Once you create a web template, you can *never* delete it (just kidding). To delete a template:

**Step 1** Log in to the Console and open Navigator.

**Step 2** Select **Interface Customization>CRM Interface**.

**Step 3** Select Web Templates and select the template to delete.

**Step 4** Choose **Edit>Delete Template**. Confirm the deletion and the template is erased.

## Miscellaneous Functions

A miscellaneous group of functions is a repository for some unique and important administrative activities. these items are located within the **System Configuration>Miscellaneous** folder on the Navigator tree hierarchy. They are:

- **Company Information.** This is the place where you define and describe company information for administrative use and reference.
- **Module Inventory.** Formerly known as “License Settings” in earlier releases, this is the repository or archive that lists all implemented VoiceMaster modules within the system. The status of each is included. This inventory is a key reference both as to the current state of the system and as guide to the purchase and implementation of modules not currently installed.
- **Network Printer.** Serves to configure the network printer, enabling administrative printing of relevant administrative data, including configuration, reports and logs.

## Company Info

The company information functions serve to collect and maintain corporate information related to your VoIP service company. Data collected is used in the generation of reports, such as Invoices and mail services.

Take these actions to configure or modify Company Info:

**Step 1** At the Navigator view, select **System Configuration>Miscellaneous**.

**Step 2** Select **Company Information**, the first function on the Miscellaneous window.

**Step 3** Select **Edit>Edit Settings** and the Company Info dialog pops up:



**Figure 1-113** Company Information

**Step 4** Assign parameters according to known company information:

- Company Name. The VoIP service company.
- Address. Its location (includes fields for street, city, state and country).
- Contact Info. This includes phone, fax, E-mail and URL/home page.

**Step 5** Select **Apply** to confirm the settings and save them.

## Module Inventory

Module Inventory displays specific listed information about modules currently licensed to operate on the VoiceMaster Platform. These are *licensed* modules. Each installed system module is defined and its status displayed alongside.

---

**Note** The Administrator should not attempt to change license settings under any circumstances. Any attempt to change a supplied module license will cause VoiceMaster to stop functioning properly. Module license settings do *not* restrict 1) the number of customers the system serves, 2) the number of possible phone connections or 3) PSTN phone lines.

---

To obtain a new license for a module not currently integrated into the system, please contact the SysMaster Support Team. Contact a SysMaster sales representative or technical support person to obtain a trial for any module. Once the module desired is explained and recorded by the SysMaster employee, it is readied for download to your system. (This of course requires an active Internet connection and an accessible VoiceMaster as the download ‘target.’)

---

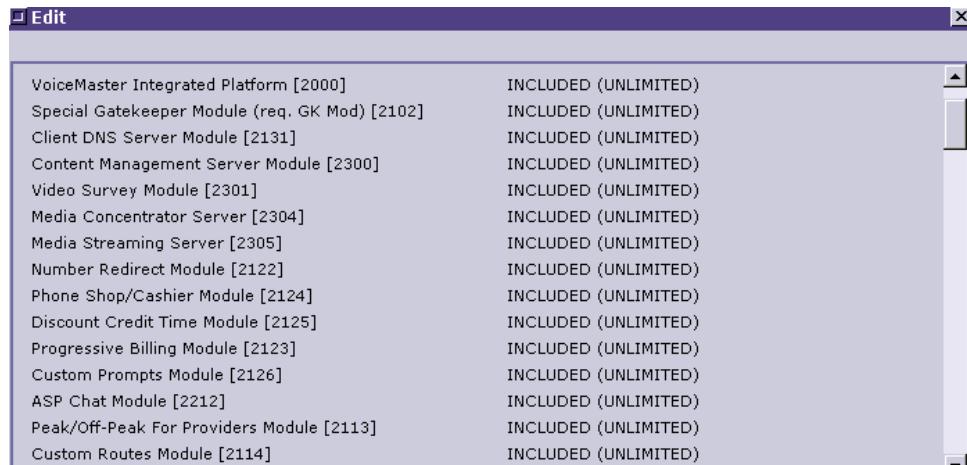
**Note** SysMaster permits the download of only two modules at a time for trial installation and operation.

---

Active modules are denoted by the **INCLUDED** heading. Most of these are marked “Unlimited” (duration), while special modules with termination dates are so indicated.

To view the current module inventory, follow these instructions to the letter:

- Step 1** At the Navigator view, select **System Configuration>Miscellaneous**.
- Step 2** Select **Module Inventory** from the Miscellaneous window.
- Step 3** Choose **Edit>Edit Settings**. The installed modules are listed in the following dialog:



**Figure 1-114Module Inventory Listing**

- Step 4** View the list. To print it, select the contents and copy them to a Notepad or Word file (etc.), then use the program’s Print function to create hard copy.
- Step 5** If a desired module is not installed or its trial functionality close to expiration, contact SysMaster.

---

**Note** Not all modules listed in the inventory are available for trial or integration. This is true only for a few modules, whose status is explained within the dialog.

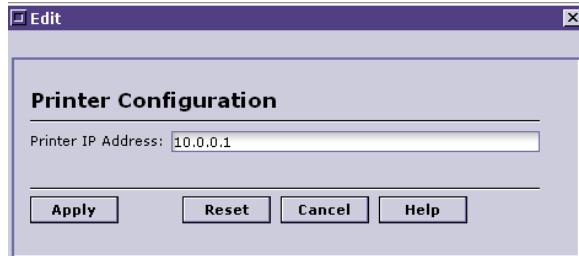
---

## Network Printer

The Network Printer option lets the Administrator configure a network printer which then can print out important configuration and management information as desired.

To configure the network printer:

- Step 1** At the Navigator view, select **System Configuration>Miscellaneous**.
- Step 2** Select **Network Printer** from the Miscellaneous window pane.
- Step 3** Select **Edit>Edit Settings**. The network configuration screen appears:



**Figure 1-115Configuring the Network Printer**

- Step 4** Enter the IP address for the network printer (the Administrator should know or be able to acquire this address).
- Step 5** Select **Apply**. The printer is configured.
- Step 6** Once the printer is configured, print any current visible window using **File>Print**.
- Step 7** The Windows Print dialog will request confirmation of the print job. Select **OK** and the requested job prints.

---

**Note** To print the contents of a dialog box (as explained in the Module Inventory section above), first save them to a file, then print the file.

---



# Chapter 5: Account Administration

---

## In This Chapter

This chapter includes the following sections:

- **Overview.** We look at the purpose and capabilities of VoiceMaster's Account Administration functions.
- **Administration Console Review.** A look at important functions and options related to Account Administration.
- **General Accounts Settings.** We describe general configuration settings for new and existing accounts.
- **Individual Accounts Administration.** The focus is on the administration of individual accounts:
  - Creating (configuring) new accounts, with procedures.
  - Managing existing accounts. Includes instructions for search (retrieval), modification and deletion of current accounts.

## Overview

The VoiceMaster Administration Console offers comprehensive Account Management facilities. These enable the comprehensive configuration and Administration of all system accounts:

- Creation of new system accounts. The descriptive parameters are a combination of account-specific settings and general account settings that apply to all accounts.

---

**Note** General Account settings, which apply to all new accounts, can be 'tweaked' for existing accounts to affects specific customer groups.

---

- Account Searches. VoiceMaster enables account searches using a wide range of search parameters - a critical capability when managing potentially huge numbers of system accounts.
- Account Administration. This is primarily the monitoring and administration (re-configuration) of existing account data. Any configuration changes can be tracked and viewed using the various Reports function. As an example, changes in a customer rate plan will be reflected in reports, statements, etc. Account deletion is another option.

The Console allows uniform management of accounts of different types. Similar functions and user actions are relevant, no matter the customer account type.

Account Management functions are closely integrated with Rate Management functions. This architecture accommodates the system's triple-layer centralized billing structure that includes:

- End Users
- Providers
- Agents (Resellers and Wholesalers)

Rate creation/configuration is linked directly to Account Management, for configured rates can be seamlessly assigned to corresponding account types. The system lets an Administrator aggregate multiple accounts into group entities ('batches') that correspond to specific resellers.

Account management incorporates a number of tools for administering accounts created.

- Account Info
- Account Balance
- Account Call History
- Account Adjustments
- Account Credit/Debit
- Account Effective Rates
- Account Statements

## Administration Console Review

Account Management functions are accessed through the Account Management folder. This is a top-level VoiceMaster Administration Console folder. To access it at any time:

- Step 1** Log in to the Administration Console.
- Step 2** Select Start>Navigator.
- Step 3** When the Navigator view opens, simply select the Account Management folder:

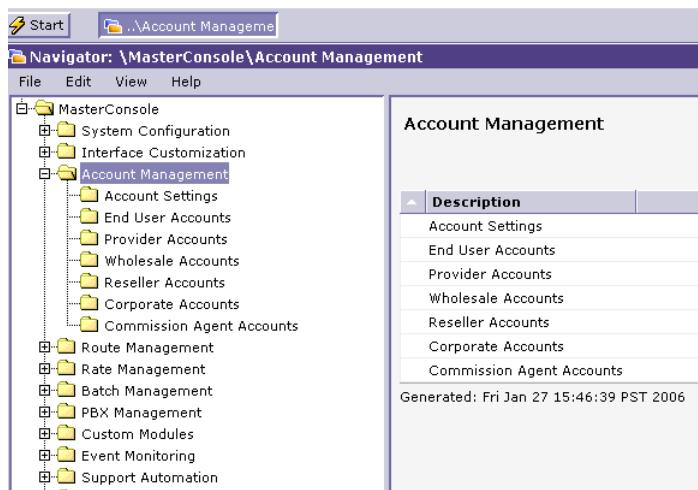


Figure 1-116Selecting Account Management

The Account Management functions are:

- **Account Settings.** This function has two aspects:
  - **New Account Settings.** Contains a range of generic settings that, when applied, will affect all new accounts on their creation.
  - **Existing Account Settings.** Includes a host of parameters that can be configured to apply to all existing accounts or to specific groups of accounts. Parameters like balance limits, account expiration dates and rate plans can be set to apply to blocks of accounts or even to all system accounts.
- **End User Accounts.** This is the first of the organization folders that group all accounts of a particular type. An ‘end user’ in the VoiceMaster system is a VoIP call customer (also referred to as a **subscriber** in this guide). The standard method for accessing a specific end user account is to search for it using any one (or more) of several search parameters.

The remaining Account Management folders (beneath End User Accounts in the Administration Console hierarchy) are:

- **Provider Accounts**
- **Wholesale Accounts**
- **Reseller Accounts**
- **Corporate Accounts**
- **Commission Agent Accounts.**

The category definitions reflect specific system accounts that are described in greater detail in previous chapters. Their functions and characteristics will be addressed within the appropriate subsection within [Accounts Administration](#) below.

## General Account Settings

General Account Settings Administration translates to the configuration and management of ‘macro’ or global settings for both new and existing accounts. (For a brief review of the location and purpose of each of the functions within Account Settings, see the preceding section.)

Administering generic settings has several purposes, among them:

- Establishing policy guidelines for accounts that fit overall administrative strategy. Can include general account parameters, methods of payment and call authentication methods.
- Defining different groups of clients and customers by virtue of distinct parameter configuration (relevant to Existing Accounts management). For instance, assign specific origination gateways to different types of user accounts or set account balance or expiration rules per account type.

### New Accounts (Global Settings)

Account administration can be shaped via the configuration of these global rules for new accounts. Settings configured using the New Accounts Settings functions are global - they affect all new accounts. A particular setting may impact a specific aspect of routing or rate policy implementation.

---

**Note** Any parameter can and will be overridden if 1) different settings are established for general settings for existing accounts or 2) a specific account (whether a user, wholesaler, etc.) has additional custom parameters (rules) assigned to it.

The critical parameters for these new account settings are:

- **Default Monthly Cap.** Calculated in call time, this is the maximum allowable calling limit for any new account.
- **Default Per Call Cap.** The maximum time allowed for a single call.
- **Default ISP Rate.** This is a preset monthly ISP charge for ISP accounts managed within VoiceMaster.
- **Default Balance Expiration Period (days).** Specifies the termination point, in days, for permitting account balances to be used (when the expiration point is reached, the account is frozen).
- **Default Hard Expiration Date.** Disables all accounts when this date (if configured) is reached. Should be used with caution, since it will effectively disable new accounts created after such a date.
- **Default Expiration Period (days).** Sets a number of days that, when reached, will trigger the disabling of any accounts reaching it. (In other words, sets a ‘timer’ to trigger future disabling of all accounts, the timer to start running from the day of account creation).
- **Multiple Calls Allowed.** Permits multiple calls from one account, meaning calls may be placed in parallel using the single PIN assigned to the account.
- **Enable Short Statements.** Generates the transmission of summary CDR records to be sent to all clients (no long statements to be sent).
- **Accept Credit Cards (Yes/No).** Globally enables or disables credit card processing. Generically permits or denies customer credit card use.
- **Default Authentication Method.** Globally assigns one of numerous available call authentication methods, from PIN prefix to IP address to Caller ID, DNIS and more. (Options visible when/if selecting method.)
- **Automatic User Emails.** Used to trigger email notification to all account holders for selected subcategory (shown here):
  - Monthly Statement.
  - Registration Confirmation.
  - Purchase Confirmation.
  - Password Modification.
- **Service Restrictions.** Used to set restrictions on one or more of a dozen types of calls.
  - Group Calls.
  - Local Calls.
  - Toll Free Calls.
  - Toll Local Calls.
  - International Calls
  - Operator Assisted Calls.
  - Directory Assistance Calls.
  - Special Services Calls.
  - Premium Services Calls.
  - Casual 1010XXX Calls.

- Internet Dialing Calls.
- Other Calls.

## New Account Settings

To configure generic settings for new accounts, follow this procedure:

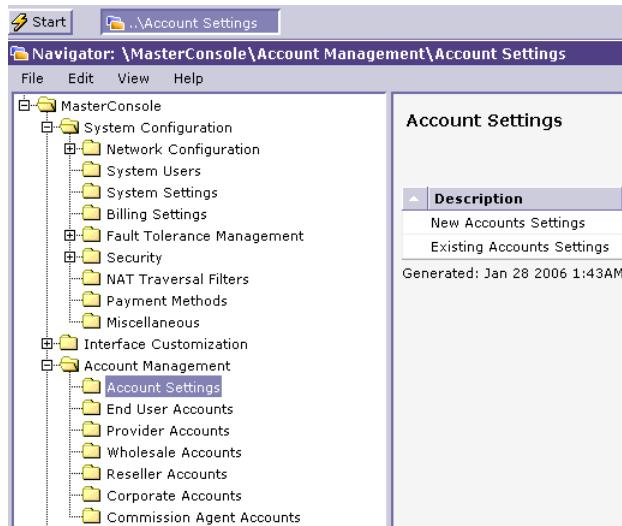
---

**Note** Configuring global settings for new accounts is of course an optional practice. It may well be useful to apply specific parameters, but is not required. The combination of General Configuration parameters (System Configuration>System Settings) and route and rate management settings may suffice. If you do set these parameters, be sure to refer to them when configuring individual rules for particular client or customer accounts.

---

**Step 1** Access the Administration Console and Navigator, if not currently available.

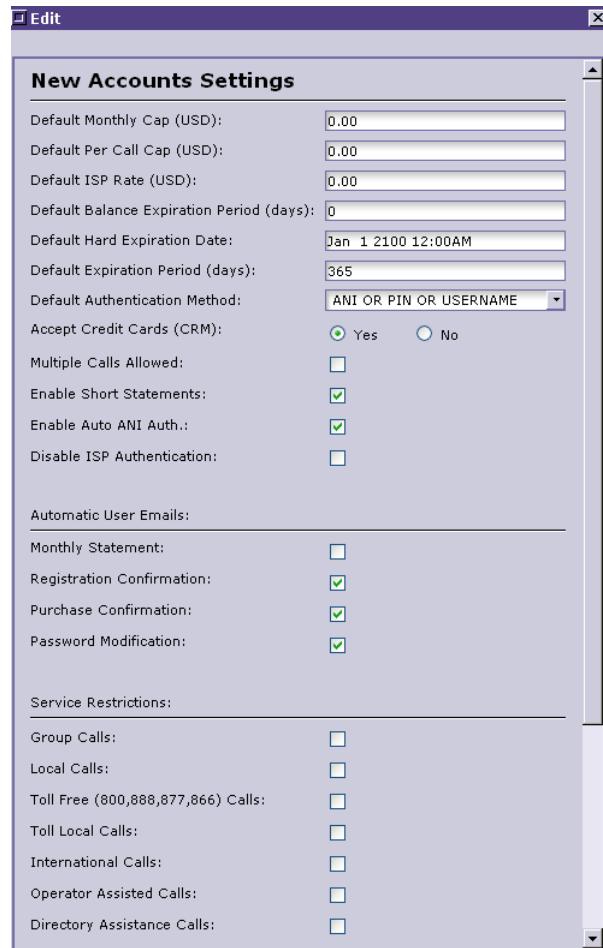
**Step 2** Select **Account Management>Account Settings**. The Account Settings window becomes the active Navigator window:



**Figure 1-117** Account Settings Selected

**Step 3** Select **New Accounts Settings**.

**Step 4** Choose **Edit>Edit Settings** to display the dialog.



**Figure 1-118New Accounts Settings (Identical to Figure 6-2)**

**Step 5** Define any of the parameters within the dialog (and summarized within the previous section). Configure call time limits, account expiration, multiple call permissions, authentication method, Email notification and service restrictions as desired.

---

**Note** The default authentication method is selected from the only pull-down menu in the dialog.

---

**Step 6** Select **Apply** to save changes and close the dialog.

**Step 7** If circumstances dictate, return to this function at any time during administrative functions and change parameters to meet current system needs.

## Existing Accounts Administration

Administering macro settings for existing accounts is similar to that for managing new accounts. A group of parameters is available, from which a desired subset (or all settings) can be applied to multiple accounts.

The primary conceptual difference is that new accounts settings apply to all accounts, where configuring existing accounts is more flexible in its execution. Generic settings can be applied to:

- A single account type
- Multiple account types
- All account types

---

**Note** Each Existing Accounts setting includes an “Overwrite” check box that appears to the right of the option within the Existing Accounts Settings dialog. The function of these check boxes is to explicitly overwrite previous settings for the selected parameters - as applied to the accounts.

---

The available configurable parameters include:

- Gateway. Specifies outgoing, origination gateway for designated account types.
- GK Authentication. Configures the kind of authentication to be used for PC-to-phone or PC-to-PC service (the full list of authentication options is displayed on selection of the parameter’s pull-down menu).
- Monthly Cap. Sets a total time cap for calls for the assigned account types.
- Per Call Cap. Fixes a per call time cap, per account type chosen.
- Min Balance. Sets a threshold beneath which affected accounts will be deemed inactive.
- Hard Expiration Date. Sets a fixed date after which affected accounts are disabled.
- Expiration Period. Assigns a set period after account PIN generation. Passing this threshold disables accounts assigned to it.
- Expiration Period Base Date. A default expiration period. If this is configured and not the previous parameter, this setting determines expiration.
- Billing Type. Specifies posptaid or prepaid billing.
- User Can Charge Credit Card. If set, lets affected users (of designated account types) use credit cards.
- Rate Plan. Specifies a rate plan to assign to selected account types (batches).
- Automatic User Emails. Triggers email notification to customers by type:
  - Monthly Statement
  - Registration Confirmation
  - Purchase Confirmation
  - Password Modification
- Enable Auto ANI Auth. Sets automatic ANI authorization
- Multiple Calls Allowed. Just like the new settings parameters of the same name. Permits multiple simultaneous calls for accounts/batches specified below.

## General Account Settings

- Enable Short Statements. Makes all statements sent to customers CDR compilation style (short).

### Configuring Existing Account Settings

To configure the general settings and apply them to specified client/customer groups, follow this procedure:

- Step 1** Access the Administration Console and Navigator, if not currently available.
- Step 2** Select **Account Management>Account Settings**. The Account Settings window becomes the active Navigator window:
- Step 3** Choose **Existing Account Settings**.
- Step 4** Select **Edit>Edit Settings**. The Existing Accounts Settings dialog becomes the active window:



**Figure 1-119Configuring General Settings: Existing Accounts**

- Step 5** Set those parameters for which you want to apply general settings to the targeted client group (when setting a particular parameter, keep the designated account type in mind). Review the parameter definitions above if you are uncertain about any individual setting.
- Step 6** Select **Apply** to save the settings.

Return to this function at any time to modify existing account settings.

## Individual Accounts Administration

In this section we review account management parameters and the procedures for configuring and administering individual accounts. A quick reminder: accounts exist for various types of clients and users in the system. These include:

- End Users
- Providers
- Wholesalers
- Resellers
- Corporate
- Commission Agents

---

**Note** Descriptions of each VoiceMaster client or customer (end user) type are found in the Guide Overview. They are further defined within the previous chapter on VoiceMaster Administration, and in the next chapters on route and rate management.

---

All client and customer accounts share the same definitional components (parameters), no matter the individual type. Parameters are:

- Account ID. Internal account identification number.
- PIN. The customer's assigned PIN number.
- Username. Customer username. Needed to authenticate/retrieve user billing (account) information.
- Password. User password. User must enter this password when interacting with his account via CRM site.
- User Type. Defines the user/account holder. **This is a critical field in the definition of all accounts; for instance, defining a provider as a provider in this field is absolutely essential when configuring rates and routes linked to a provider.** Selectable user types:
  - (a) Active User - specifies a calling customer who has registered for VoIP service and been authorized use the network for VoIP calls.
  - (b) Network Provider - specifies an termination partner (company) that participates in handling voice communications at the point of termination.
  - (c) Wholesaler- specifies a network partner that uses your networking facilities/infrastructure.
  - (d) Reseller - specifies a distribution partner that participates in selling the services of the Management company to end customers.
  - (e) Corporate Client - specifies a wholesale client with special prices for the end customers that will use the service through the Corporate Client's account;
  - (f) Commission Agent (need to hone this definition)
- ISP Plan. The ISP plan, if any, that the account is associated with.
- Billing Rate Plan. The Billing Rate plan associated with the account.

- Route. The route assigned the account.
- Custom Service Plan. A special service/billing plan that may be assigned the account.
- Signup Plan. Signup plan that the account's customer may have applied to him (designated at registration).
- Caller ID Distribution. Type of Caller ID, if any, associated with the account.

---

**Note** The following fields are self-explanatory.

---

- Company.
- Full Name.
- Address.
- City.
- Zip.
- State.
- Country.
- Email.
- Phone.
- Speed dial.
- Gateway. Origination gateway assigned to the customer.
- Caller ID (ANI). Enter this if 'Caller ID' is the authentication method for the particular customer.
- IP Address. Designates customer's IP address. Assumes that the customer makes VoIP calls using a PC-to-Phone or PC-to-PC service, and that his computer has a legitimate IP Address (without it these calls are impossible).
- Authentication Method. Sets the method, out of the several available, that will authenticate the customer's call attempts.
- Currency. How the customer is to be billed. If billing is in non-USD, exchange rates must be set by the Administrator through the Currency Settings function.
- Redirect Number. Relevant when gatekeeper authentication is DNIS Only, Then the user is authenticated by his dialing number and redirected to the number specified here.
- DNIS. When gatekeeper authentication is DNIS only, customer is authenticated by his source (phone) number. Enter the DNIS number here that will be used for authentication.
- Service Caller ID. Customer's phone number, relevant for Caller ID enabling.
- Authentication String. Authentication string: number encoded within; for authentication purposes.
- Enable Auto ANI Auth. Triggers ANI authorization method use.
- Balance Expiration. Sets number of days to trigger effective account disabling, even if balance remains.

- Binded Provider ID. Used for managed services scenarios in which all customers/users are ‘bound’ to designated providers so that system rate costs can be integrated into billing structure (passed on from VoIP owner to managed service client and his customers). ID entered will be account number ID of specified provider.
- Automatic Provisioning System - for configuration of special devices, such as IP phones.
- MAC Address.
- Terminal Type.
- Automatic User Emails (five types). Any and all email notification types checked leads to automatic ‘send’ of event to customer. For instance, ‘Password Modification’ enabled means that administrative changes to the customer’s password are transmitted automatically to the customer.
- Accept Credit Cards. (Yes/No). Let the customer use credit cards to pay his account balance, recharge it, etc.

In the sections that follow, we present the procedures for establishing new accounts of any type and administering those accounts.

## ACCOUNT CREATION

Creating an account in VoiceMaster is the same basic process no matter the account type:

- Step 1** Select the category for the account to create.
- Step 2** Access the dialog box containing account definition parameters.
- Step 3** Define all essential parameters and desired optional settings.
- Step 4** Apply the settings to save the account and add it to the stock of existing accounts.

In the previous section, we have already defined the parameters that can be applied to a new account (as Step 3 here suggests, the extent of settings configuration can vary). As with all other configuration sequences in VoiceMaster, no settings are permanent (though some are mandatory). It is always possible to return to an existing account and modify it. This is what makes system administration in VoiceMaster such a valuable tool...

---

**Note** There is one account type (provider) that triggers a slightly different account creation sequence than other account types. This modest and specific variation will be explained below.

---

To create a new client or customer account, follow these instructions:

- Step 1** Log in to the Administration Console if not currently logged in. Then open the Navigator (Start>Navigator).
- Step 2** At the Navigator view, select the Account Management folder.
- Step 3** Select any of the folders (other than Account Settings) that fits the type of account you wish to create. For this procedure, we have selected Wholesale Accounts.

## Individual Accounts Administration

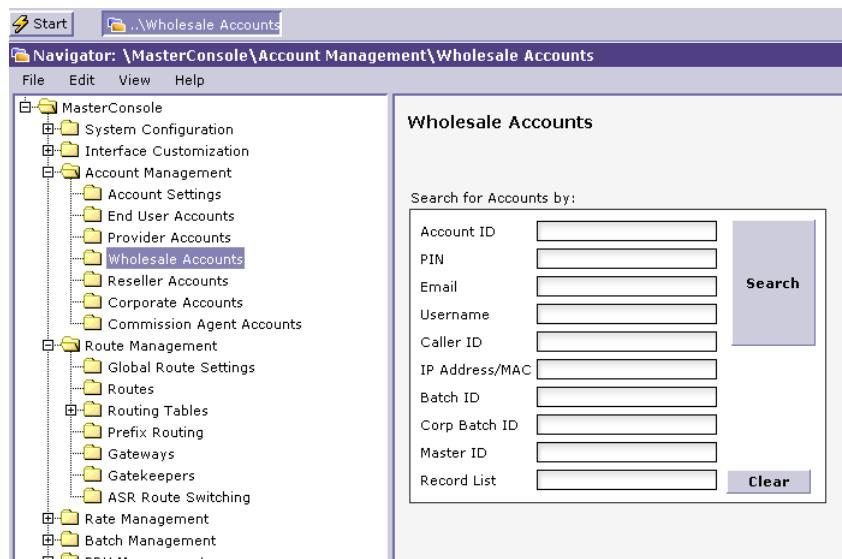


Figure 1-120 Wholesale Account Under Construction

**Step 4** Select **Edit>Add Account**. The Account Information dialog (identical no matter the account type selected) appears:

The 'Account Information' dialog box contains the following fields:

Username:	<input type="text"/>
Password:	<input type="password"/>
User Type:	Wholesale Client
Company Name:	<input type="text"/>
Full Name:	<input type="text"/>
Address:	<input type="text"/>
City:	<input type="text"/>
ZIP:	<input type="text"/>
State:	Not Selected
Country:	Not Selected
Email:	<input type="text"/>
Phone:	<input type="text"/>
Speed Dial:	<input type="text"/>
Gateway:	Any Gateway
Caller ID (ANI):	<input type="text"/>
IP Address:	<input type="text"/>
Authentication Method:	ANI OR PIN OR USERNAME
Currency:	UNITED STATES OF AMERICA
Redirect Number:	<input type="text"/>
DNIS:	<input type="text"/>
Balance Expiration(days):	0
Automatic User Emails:	<input type="checkbox"/>
Email Statement:	<input type="checkbox"/>
Registration Confirmation:	<input checked="" type="checkbox"/>
Purchase Confirmation:	<input checked="" type="checkbox"/>

Figure 1-121 Account Creation Dialog

**Step 5** Define the parameters that make up the new account profile.

---

**Note** In this example, the administrator has assigned username and password, and selected “Wholesale Client” as the user type.

---

**Step 6** Complete those fields and settings that are essential and appropriate to the specific account. Here is the same dialog box with additional parameters configured:



The screenshot shows a Windows-style dialog box titled "Edit Account Information". The dialog contains numerous configuration fields for an account, each with a label and a corresponding input field or dropdown menu. The fields include:

- AccountId: 104873
- PIN: (empty)
- Username: tela
- Password: tela
- User Type: Wholesale Client
- Rate Plan: System [0]
- Route Plan: System [0]
- ISP Rate Plan: (empty)
- Custom Service Plan: Master Plan
- Signup Plan: NONE
- Caller ID Distribution: NONE
- Content Plan: NONE
- Company: Tela
- Full Name: bp
- Address: (empty)
- City: (empty)
- ZIP: MH 1 9V
- State: Not Selected
- Country: Not Selected
- Email: test@sysmaster.com
- Phone: 5143958668
- Speed Dial: (empty)
- Gateway: SOFT PHONE ONLY
- Caller ID (ANI): (empty)
- IP Address: (empty)
- Authentication Method: PIN, CALLERID, SERVICEID
- Currency: UNITED STATES OF AMERICA
- Redirect Number: (empty)

**Figure 1-122** Progress Towards Wholesale Account Creation

**Step 7** Select **Apply** to save the settings and add the account to the portfolio of current accounts.

---

**Note** When creating a new account, the available descriptive parameters are extensive. However, additional settings are available when administering existing accounts.

---

## Provider Account Creation

Provider accounts are created using the same functions and options as other accounts. However, a provider's role is different as the supplier of bandwidth and termination endpoints to your VoIP service business.

Your relationship with the providers is essentially a contract for the supply of infrastructure. Providers are designated entities offering or extending their telecom infrastructure, such as gateways, termination, PSTN connectivity, etc. In return, service providers are compensated with a pre-negotiated rate that forms one of your primary expenses.

Because of this unique role that providers play in the system, the Administration Console deals with provider accounts differently.

---

**Note** Once a Provider Account has been added (a mandatory step in System Rates set-up), basic rates should be assigned to it. Rates can be set manually or via a bulk import. We cover this in [Chapter Three: VoIP Service Configuration](#).

---

Provider Account configuration requires:

- Add a Provider Account
- Assign (or import) basic rates
- Specify System Rate Adjustments

Some account parameters are not relevant to providers: authentication methods, redirect numbers, balance caps and expirations. The system acknowledges this reality by removing these once it recognizes that a provider account is under construction.

To create a provider account:

- Step 1** Log in to the Administration Console and open the Navigator (Start>Navigator).
- Step 2** At the Navigator view, select the **Account Management** folder.
- Step 3** Select **Provider Accounts**, then **Edit>Add Account**. The account creation dialog (Figure 5-6) is displayed.
- Step 4** Assign Username and password.
- Step 5** At the User Type window, select Network Provider from the type options. Immediately, the dialog box is condensed as shown:



**Figure 1-123** Network Provider Account Creation - Shortened Parameter List

- Step 6** Set the remaining parameters. Note that they are all account identification/contact information settings.
- Step 7** Select **Apply**. The account is created.

## CURRENT ACCOUNTS ADMINISTRATION

Administering current accounts is a combination of two basic actions:

- Modifying accounts
- Deleting accounts

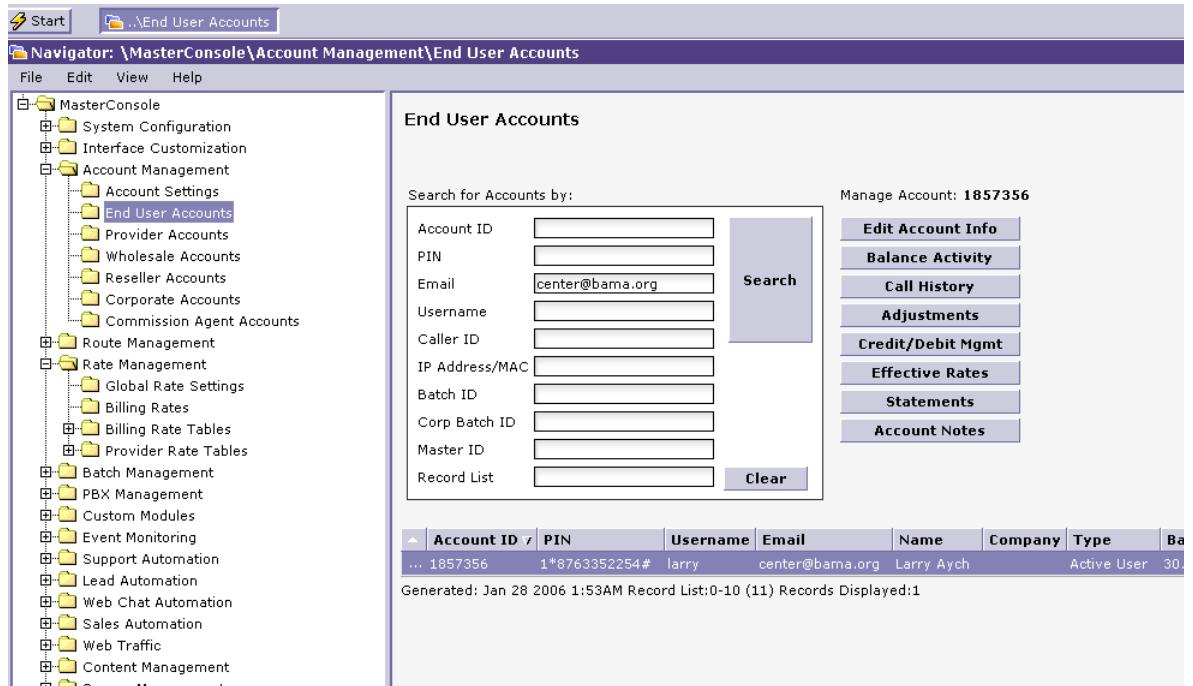
Both these actions are covered in this section, along with procedures. Naturally, the emphasis is on account modification, which presents a rich selection of administrative tools.

---

**Note** As with the accounts creation sections earlier in this chapter, the relevant procedures are common to all accounts regardless of type. We expect the reader to extrapolate from the discussion and apply its principles to all accounts - not just the sample account (End User) described here.

---

A range of administrative options is available for current accounts. This Administration Console view, resulting from the retrieval and selection of an active user, shows the full set:



**Figure 1-124Active End User Account Selected**

The management options fill the panels at window right:

- **Edit Account Info.** The most general and commonly used option, selecting it produces a dialog box containing all relevant account parameters for user modification.
- **Balance Activity.** Produces a snapshot view of account balance, activity and expiration settings. Contents will reflect settings configured for the specific account.
- **Call History.** Displays a window showing call/session history and monthly balance. Includes general and billing search options that are user-definable.
- **Adjustments.** This is another ‘edit’ option, for selecting it produces a dialog box that lets the Administrator set specific call time and per call adjustments, as well as expiration management and calling plan parameters.
- **Credit/Debit Mgmt.** Displays account balance and includes editable fields for voucher payment, reward points and account credit/debit. Here the administrator can take appropriate actions - credit the selected account, debit it or trigger payment.
- **Effective Rates.** A ‘view’ option that shows how various billing parameters play out in an actual call - how the various charges are calculated in a sample call.
- **Statements.** Produces a window with a search mechanism that lets you retrieve an account statement from a chosen period.
- **Account Notes.** When selected, offers a window with a text entry capability for notating the selected account.

---

**Note** Each of these options is also selectable as an Edit menu function in Account Management.

---

## Edit a Current Account

The most generic administrative action associated with existing accounts is to edit an account's individual configuration settings. This table presents all parameters in the Edit Account Information dialog.

**Table 1-2 Account Information Parameters**

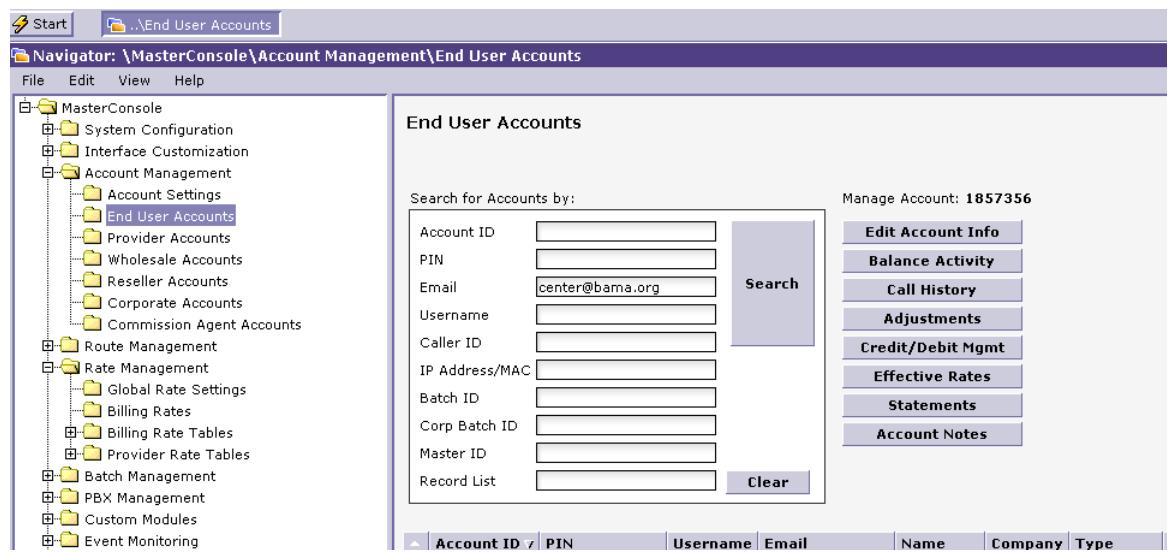
Account ID	Specifies the account identification number.
PIN	Specifies user PIN number that customer uses to access system.
Username	The username can include only alphanumerical characters. The username is required for customer access of the online billing and review system.
Password	Along with user name, needed to access online information regarding the customer account.
User Type	<p>Specifies the type of the user. Available options are:</p> <p><b>Active User</b> - a regular customer using the system. Active denotes that this user has an active status in the system;</p> <p><b>Network Provider</b> - a termination partner (company) that provides bandwidth/termination points/PSTN access;</p> <p><b>Wholesale Client</b>- a network partner using the VoIP service facilities/infrastructure;</p> <p><b>Reseller</b> - Distribution partner that sells your VoIP services to customers;</p> <p><b>Corporate Client</b> - Wholesale client that sets special prices for customers who use the service through the single Corporate Client account;</p> <p><b>ISP Provider</b> - specifies an internet service termination partner (company);</p> <p><b>ISP User</b>- specifies a customer using the internet service provider services;</p> <p><b>Disabled</b>- disables the account blocking it to use the system;</p>
Billing Rate Plan	A rate plan associated with the account.
Route	A route associated with the account.
Company	(Customer) company name, for reference by partners.
Full Name	The person representing either a regular customer or a business partner.
Address	That person's address.
City	Specifies the city of the user.
Zip	Specifies the ZIP code of the user.
State	Specifies the state of the user.
Country	Specifies the country of the user.
Email	Specifies the email of the user.
Phone	Specifies the phone of the user.
Gateway	Specifies the gateway assigned to the user to service her/his calls.

Caller ID (ANI)	Caller ID (ANI) specifies the phone number from which the customer will make calls. If a Caller ID (ANI) is configured, it is used to authenticated customer calls.
IP Address	An IP address by which the customer is authenticated.
Balance Expiration Period	Specifies the date after which the account balance is locked, the account disabled.
Authentication Method	Specifies the keys through which the user will be authenticated for the PC-to-Phone or PC-to-PC service: Available options are:  IP Address Only; IP Address Only & Account Name; IP Address Only & Phone Number; IP Address Only & PIN Prefix; Account Name Only; Phone Number Only; PIN Prefix Only; DNIS Only; NONE (Calls Not Allowed) ANI or PIN or USERNAME
Monthly Email Statement	Check this box to specify that the customer will receive a monthly statement via email.
Accept Credit Cards (CRM)	Check to specify that the customer can use her/his credit card at the CRM.
Currency	Specifies the currency based on which the system will charge the account. (Exchange rate will determine calculations if chosen currency is non-USD).
Redirect Number	Number to which caller is redirected if gatekeeper authentication is set to DNIS Only. Caller is identified by the DNIS number, then redirected.
DNIS	Number to be authenticated when gatekeeper authentication is set to DNIS Only.

To view or modify existing configuration settings for an account, follow this procedure:

**Note** We describe modification of an active (end) user account. The steps are identical no matter the account type.

- Step 1** Log in to the Administration Console, as necessary, and open the Navigator.
- Step 2** Select **Account Management>End User Accounts**. The active window reflects your selection.
- Step 3** Search for the desired account. Enter a search variable or variables and select Search.
- Step 4** Click on the account entry (below the Search box) when it is retrieved. Administrative options are shown:



**Figure 1-125 Retrieved Account Selected, Administrative Buttons Available**

**Step 5** Select the **Edit Account Info** button. (Alternately, select the same option from the **Edit** menu. We recommend the habit of button selection for faster administration.). The **Edit Account Information** dialog for the selected account appears:

**Edit**

**Edit Account Information**

AccountID:	1857356
PIN:	1*87#
Username:	larry
Password:	larry
User Type:	Active User
Rate Plan:	1 [21]
Route Plan:	1 [12]
ISP Rate Plan:	System [0]
Custom Service Plan:	postpaidtest [5]
Signup Plan:	NONE
Caller ID Distribution:	NONE
Content Plan:	NONE
Company:	
Full Name:	Larry Aych
Address:	123 Count Court
City:	Centerville
ZIP:	
State:	Alabama
Country:	United States of America
Email:	center@bama.org
Phone:	
Speed Dial:	
Gateway:	Car310
Caller ID (ANI):	
IP Address:	
Authentication Method:	IP ADDRESS ONLY
Currency:	UNITED STATES OF AMERICA
Redirect Number:	

**Figure 1-126Edit Account Information: Account Modification Dialog**

- Step 6** Modify any parameters or fields desired. (Alternately, simply view settings without modifying them.)
- Step 7** When you are satisfied with any and all modifications, select **Apply** to save changes.

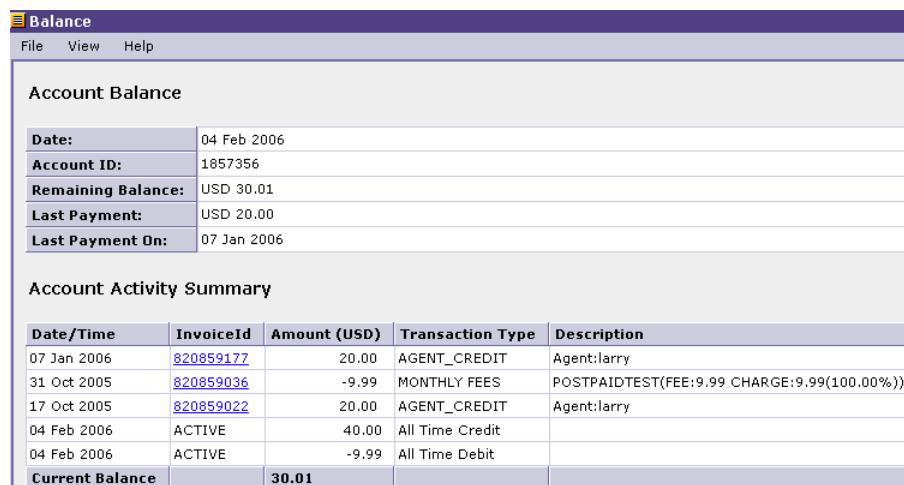
### Balance Activity

The **Balance Activity** option is useful for retrieving a snapshot of current account activity. This summary view includes:

- Account balance information, including remaining balance and last payment
- Account activity summary
- Balance expiration settings (if configured)

To view balance activity:

- Step 1** Repeat Steps 1-4 in the previous section to retrieve and select the desired account for administration purposes.
- Step 2** Select the **Balance Activity** button. The active window is replaced with the Balance Activity display parameters:

**Figure 1-127Balance Activity View**

- Step 3** Use the File menu to save, export or print the file for reference.
- Step 4** Close the window when you have completed visual reference.

### Call History

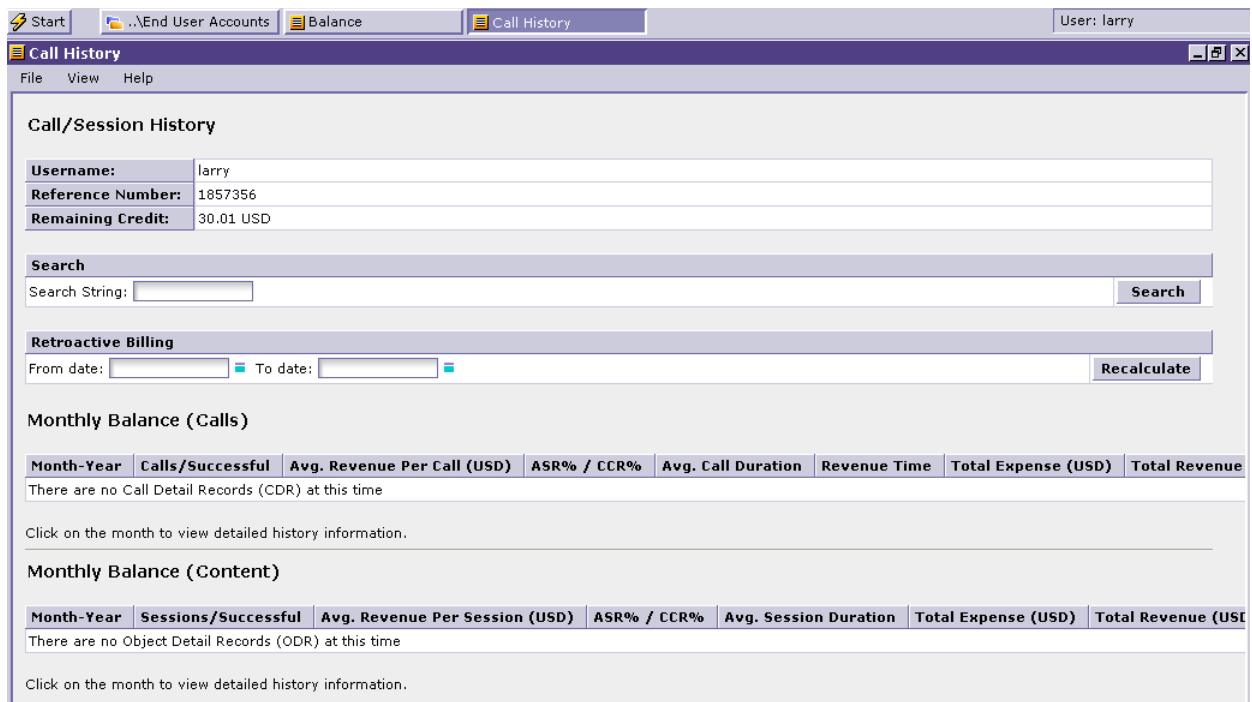
The Call History option is another useful view into account activity. On selection, it displays a window containing call/session history and monthly balance.

To recall the Call History view:

- Step 1** At the Navigator view, select Account Management and the account type that matches the account you wish to retrieve.
- Step 2** Use the search facility to retrieve and display the account.

**Step 3** Select it to display the administrative option buttons.

**Step 4** Select **Call History**. The Call History window appears:



**Figure 1-128Call History Open**

**Step 5** Enter a search string to retrieve specific call/session history records (**Larry - what are the search parameters available/required?**). Press the Search button to retrieve the records.

**Step 6** Search past billing records by entering retroactive billing search parameters, then choose Recalculate to view the records.

**Step 7** Save, export or print the call history. **Do this after specifying specific record searches** (as appropriate).

**Step 8** Close the window when done.

## Adjustments

The next option is another critical administrative tool that can affect the definition and behavior of an individual account. It can be used to set special or custom charges to the account, set balance requirements and limits and account expiration periods. The range of configuration options available can be divided into:

- Billing administration
- General account definitions/restrictions

Adjustments parameters include:

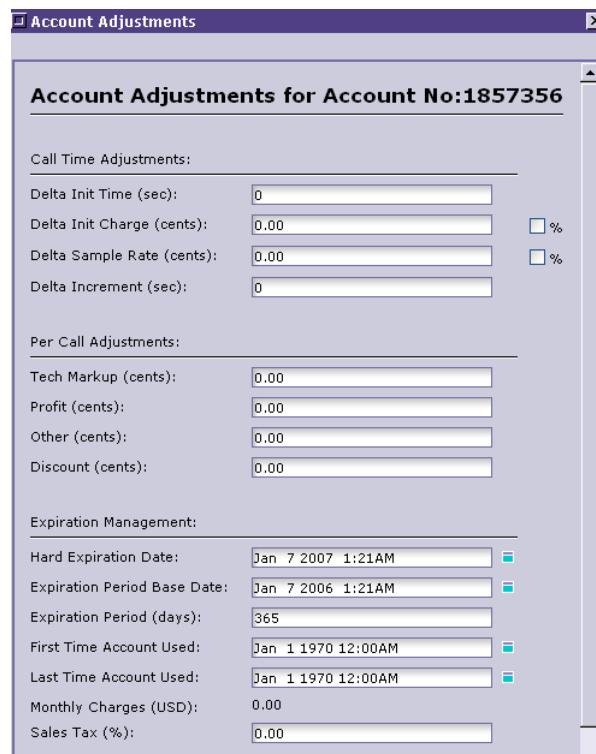
Delta Init Time	Sets initial time interval used to calculate custom billing charge, etc.
-----------------	--

Delta Init Charge	Specifies an additional (delta) charge (in US cents) during the initial time (Init Time). Enables implementation of a flexible billing model where custom rates are assigned the customer without linking them to provider rates. The value can also be a percentage of the pre-defined Init Charge.
Delta Sample Rate	Specifies an additional (delta) charge (in US cents) on top of the already defined Sample Rate charge. Similarly detached from any changes in provider rates charged VoIP service itself.
Delta Increment	Adds defined seconds to the Increment parameter.
Tech Markup	Specifies additional charge(s) (in US cents) as a technology fee to compensate for the cost of utilizing equipment or services obtained by a third party provider.
Profit	Specifies absolute profit to make regardless of call rates applied.
Other	Miscellaneous additional charges applied.
Discount	Fixed discount for customer, used mostly with Reseller clients.
Hard Expiration Date	Specifies a firm end date after which the account will be considered invalid and void.
Expiration Period Base Date	Specifies account expiration period. If overwrite is not checked, current data will not be changed.
Expiration Period	Specifies the number of days that the account will be active after PIN-generation date.
First Time Account Used	Date on which the account was first used.
Last Time Account Used	Date on which the account was last used.
Monthly Charges	Accumulated amount in current month.
Sales Tax	Specifies an additional tax amount that is added at the end of the call.
Multiple Calls Allowed	Permits multiple simultaneous calls from the customer account.
Max Concurrent Calls	Sets a maximum of calls if multiple calls are allowed.
Total Allowed Monthly Minutes	Another time cap.
Enable Short Statements	Configures combined CDR summary statements for account.
Monthly Cap	Specifies the allowed monthly time limit for using the service.
Per Call Cap	Specifies allowed call time on a per call basis.
Min Balance	Specifies a minimum balance beneath which the account is considered inactive.
Billing Type	Specifies the type of billing for the account. <b>Prepaid</b> - the customer pays for call time in advance. Usually refers to calling card purchase. <b>Postpaid</b> - the customer pays for call time at the end of month.

<b>Calling Plan Information</b>	
Monthly Usage Time	Specified usage time per month (custom)
Monthly Time Left	Assign value for remaining time.
Call-Termination Time	view only
Monthly Plan Time	view only
Monthly Time Cap	view only

To use the Adjustments feature:

- Step 1** At the Navigator view, select Account Management and the account type that fits the account you wish to retrieve.
- Step 2** Use the search facility to retrieve and display the desired account.
- Step 3** Select it to display the administrative option buttons.
- Step 4** Select Adjustments. The Account Adjustments dialog is displayed:



**Figure 1-129 Making Account Adjustments**

- Step 5** Make any adjustments by category or section:

- Call Time Adjustments
- Per Call Adjustments
- Expiration Management
- Calling Plan Information

- Step 6** Select **Apply** to save changes.

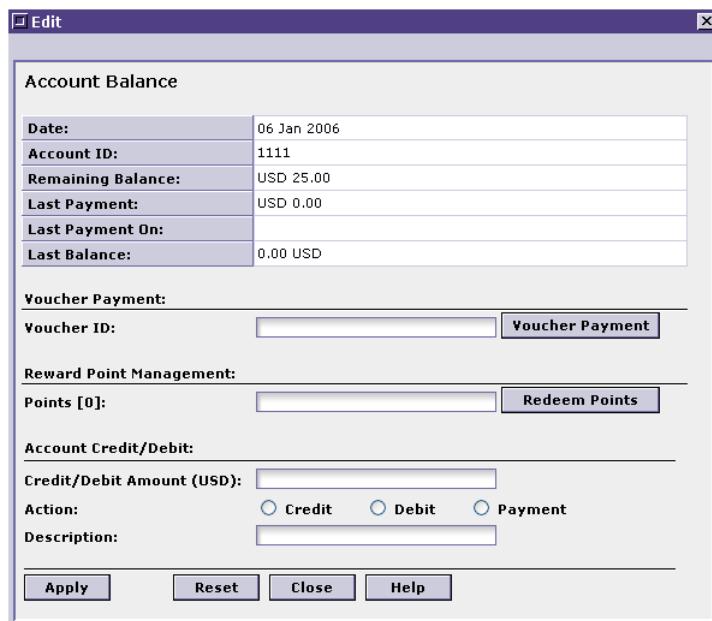
## Credit/Debit Management

Credit/debit management lets the Administrator redeem voucher payments and reward points. Most importantly, it facilitates the crediting or debiting of accounts to reflect current account status. This is a flexible means of implementing custom financial measures on specific accounts.

Displays account balance and includes editable fields for voucher payment, reward points and account credit/debit. Here the administrator can take appropriate actions - credit the selected account, debit it or force payment of a customer bill. (**Larry - assume that the customer has signed up for Admin auto-payment - that this is the implementation of the 'Recharge Acct' type of parameter from General Config**).

To apply credit/debit policies to a specific account:

- Step 1** From the Navigator view, select **Account Management>[Account Type]**.
- Step 2** When the active window changes to reflect your choice, search for and retrieve the desired account. Select it so the management buttons are displayed.
- Step 3** Select **Credit/Debit Mgmt** from the button display. The following dialog appears:



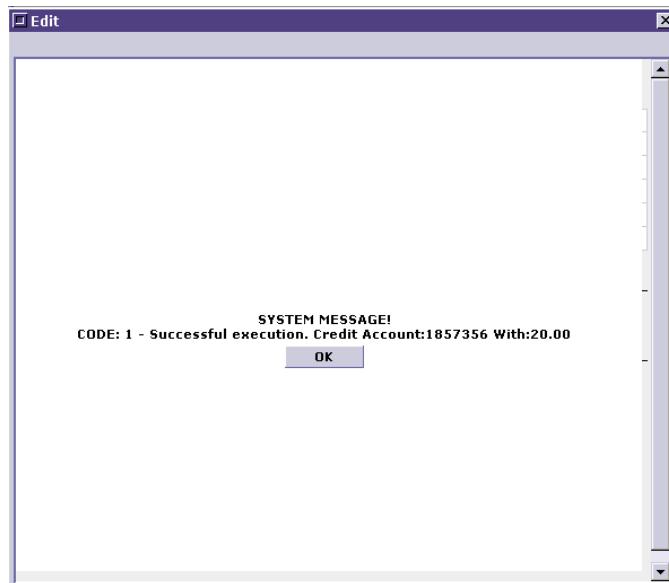
**Figure 1-130 Credit/Debit Management**

- Step 4** View the account balance summary.
- Step 5** If appropriate, activate a voucher payment or redeem points earned by the customer.
  - (a) For Voucher Payment, enter the ID of the payment voucher, then select the **Voucher Payment** button.
  - (b) For Reward Points Management, enter the points the customer has earned, then choose **Redeem Points**.
- Step 6** To credit or debit an account or make a (customer) payment:
  - (a) Enter an amount in the Credit/Debit Amount entry box.
  - (b) Select the radio button adjacent to the action that you are taking.

(c) Describe the action in the next box (if desired).

**Step 7** Select **Apply** to save your actions and close the dialog.

Any successful actions result in the following message display on performing Step 7:



**Figure 1-131Successful Action Message**

## Effective Rates

Effective Rates offers a practical, real-world look into how the various rates applied to an account come into play during an actual call. It shows a breakdown of charges - the charges being the sum of those currently configured for calls from the selected account.

To view these rates:

- Step 1** Select Account Management from the Navigator and the account type for the account desired.
- Step 2** Search and locate the account in question.
- Step 3** Select it from the Account Management window.
- Step 4** From the Account Management buttons, click **Effective Rates** and view:

Area Code	Location	Init Time	Init Charge	Sample Interval	Charge per Interval	IncTime	Call Orig Charge	Call Term Charge	Tech Markup	Profit	Discount	Other	ProviderID
359	Bulgaria	0.00	0.0000	60.00	0.2000	1.00	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0
9	local	0.00	0.0000	60.00	0.0000	1.00	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0
1	us	0.00	0.0000	60.00	0.0000	1.00	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0

\*Additional fees may apply. All rates in USD

**Figure 1-132Effective Rates**

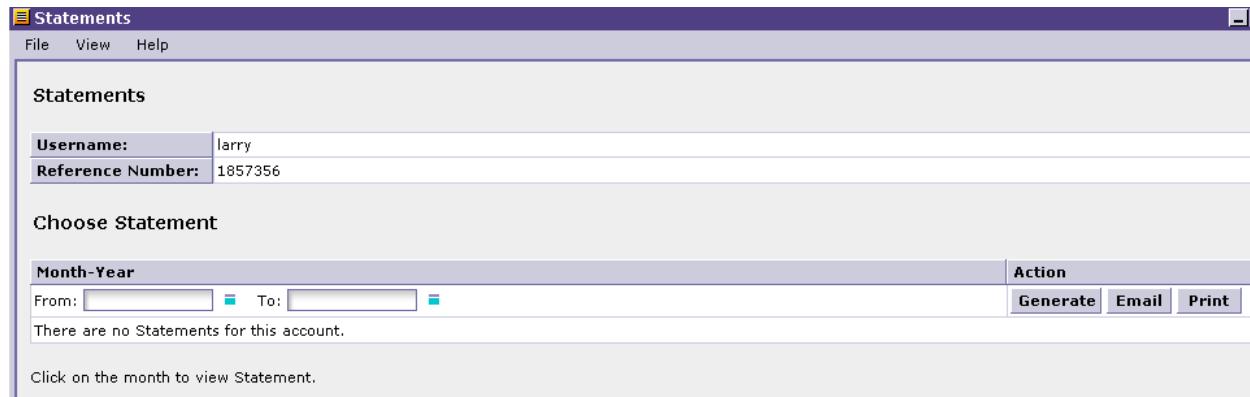
- Step 5** View the breakdown of charges.
- Step 6** Save, export or print the data as desired.
- Step 7** Close the window when ready.

## Statements

The Statements option can be used to summarily generate, print or email a customer statement on demand. (The Email option is only relevant if you have configured statement notification during the account setup process.)

To use this facility:

- Step 1** Navigate to the Account Management function, select the account type desired and search and retrieve the target account.
- Step 2** Select it when it is recovered to produce the Account Management button list.
- Step 3** Select Statements. This window appears:



**Figure 1-133Statements**

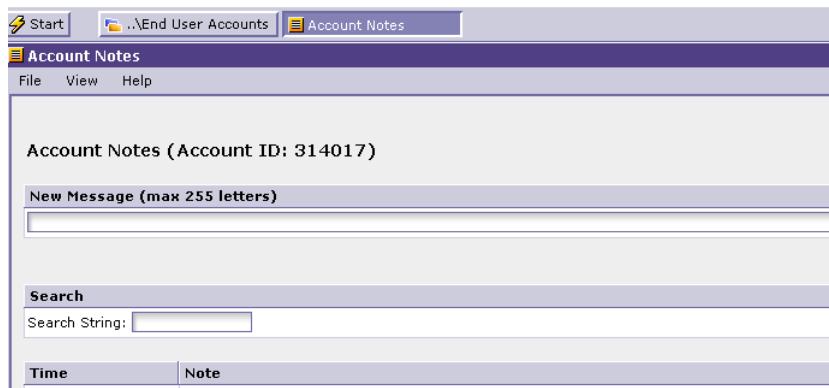
- Step 4** Recover and display statements by entering From/To parameters in the Month-Year fields.
- Step 5** Select **Generate** to generate the parameter-defined statement.
- Step 6** Select **Email** or **Print** to perform those actions, or use the File menu to save or export the generated statement in file format.

## Create Account Notes

The final option is to write informational notes about a particular account. This may be useful for unusual accounts or to remind yourself of impending deadlines, etc.

To write account notes:

- Step 1** Bring up the desired account using the now-familiar selection procedure. Click on it to display the Account Management buttons.
- Step 2** Select **Account Notes** from the list. This window appears:



**Figure 1-134** Writing Notes

- Step 3** Type a descriptive message in the **New Message** text box (it is limited, as shown).
- Step 4** Select **Apply** to save it and attach it to the account.
- Step 5** Alternately, search for and recall a previously created message:
  - (a) In the Search box enter a search string with a word or phrase from the saved message.
  - (b) Choose **Search**.
  - (c) The message is retrieved for editing or viewing.
- Step 6** When your administrative notetaking is accomplished, close the window

## Delete an Account

To delete any account from the system:

- Step 1** Log in and open Navigator, if it is not currently available.
- Step 2** Select **Account Management>(Account Type)** (for instance, **Wholesale Accounts**).
- Step 3** Use the search facility to locate and retrieve the desired account.
- Step 4** Select **Edit>Delete Account**.
- Step 5** Confirm the deletion by clicking **OK** when the confirmation message is displayed, or cancel the deletion.

---

**Note** Once you confirm deletion, the account will be permanently removed from the system. Exercise caution when deleting accounts from VoiceMaster.

---



# Chapter 6: Event Monitoring

---

## In This Chapter

Event Monitoring contains a valuable set of administrative tools for monitoring network activities both in real time and historically. It includes a special tool (Call Calculator) that simulates calls, system alerts that notify administrators when specified events occur, and a variety of logs and reports permitting different ‘view angles’ into the living network.

These functions provide timely information that is key to subsequent administrative actions. They are basically a collection of snapshots of current configurations and performance that may trigger policy actions.

The Event Monitoring functions are:

- **Call Calculator.** This function is configured per account. When generated, every call calculator produces a summary of a simulated call. The summary includes results for a sequence of relevant parameters, from calling and called station identification to call duration to gateway used and mapping and batch information.
- **System Alerts.** Three types of configurable alerts provide an administrator with notification of events that can trigger administrative response. These events range from balance level (threshold) violations to gateway performance and API (Application Programming Interface) alerts that trigger script activation.
- **Real-Time Stats.** Statistics are divided into several categories. Call performance and status is the focus, but routing component status is also presented. A full break-down of these statistical functions and how to use them is included in the [Real-Time Stats](#) section below.
- **Real-Time Logs.** This folder provides an impressive array of specific logs in which data is collected and displayed per system function. As with real-time stats, the specific logs and their purposes are traced within the section discussion.
- **Reports.** Four basic kinds of reports exist in VoiceMaster:
  - Rates. Provides rate information on a system basis (organized by termination of calls), on an area code basis (all rates charged for calls to specific codes), and by customer account type. In other words, view rates from 1) an endpoint perspective 2) for individual customer accounts, by type.
  - Stats. A heterogeneous representations of statistics - on a systemwide basis, per account, or per PINs or batches (both are variations of account views, as they correlate to accounts).
  - System Reports. Another thorough display of reports, including by call history, console sessions, fraud detection (this report collects fraud instances configured through security settings, as explained earlier in the chapter), by balance and by two kinds of messages - system and call message. Refer to [System Reports](#) for the full explanation.

- Accounting Reports. Financial reports are presented as general accounting reports or by invoice.

Event monitoring provides a truly rich set of administrative resources. They are general and visual enough to be used to survey and monitor a well-configured system. Yet, they are detailed and specific enough to hint at remedial actions in the case of awkward configuration or performance issues.

## Call Calculator

The Call Calculator is a concise and varied display of a simulated call. When generated, the calculator displays how the VoiceMaster processes a call.

It is really a mechanism to test different aspects of the call process:

- Authentication
- Routing
- Billing

The user (administrator) effectively configures the Call Calculator to focus on one aspect or another by virtue of how he configures the report (before generating it).

Each of these component tests is discussed in turn.

### Authentication

The calculator can test the call authentication process. This comes about when the Administrator does not specify an account number when building the report. The calculator recognizes the absence of caller identification (account number) and attempts authentication based on other included parameters (for instance, PIN number).

An example of a calculator that is generated without an Account ID is the following:

```
Reference Name: "Testing PIN 1234"  
Account ID: 0  
Keyword: pin=1234#;dn=15104208837
```

The user now creates a new report without an Account ID but with a known PIN number. After creating and applying the report, he generates it and gets a result that shows:

- The authentication method includes “PIN”
- The pin number is set to “1234#”

The account is identified, despite the lack of an account number.

### Routing

The Call Calculator can be used to predict a route that will be used for a call when multiple routes are configured for a desalination. In other words, the result generated shows what route is currently the primary (first choice) route for a call to Destination X when multiple endpoints are available and the system selects a route based on user-set routing priorities.

---

**Note** Using the Call Calculator in this fashion assumes that the routing mode is not set to Static (in which case the same route is selected until the user ‘manually’ selects a different default route).

---

To prepare the Calculator to return a route-oriented result, the Administrator would define the source (Account ID) and destination (number called and, optionally, the termination gateway IP address). The specific Calculator is configured. When generated, it returns a result showing essential route characteristics such as destination gateway IP.

## Billing

The heart of the Call Calculator displays billing calculations that the system performs in the course of a call. These calculations can be split into separate categories:

- Revenue. Shows charges applied to end user, in detail. Initial, sample and fixed charges - all culled from billing rate definitions - are used. Adjustments, if configured for this customers, are added. All billing elements are expressed in the total revenue shown for the call.
- Expense. Displays a similar calculation, but breaks down *your* expenses for the call, based on the relevant Provider Rate table.
- Profit. Shows the calculation that results from subtracting expense from revenue.

The Admin gives a reference name to a billing-focused Calculator report such as ‘Testing Bill 1’ and ties it to a specific account, then assigns the destination number as a keyword. The Calculator is created. Upon generation, it provides the billing results just outlined.

---

**Note** If custom billing modules are included in your system and applied to the customer whose call is the subject of a Call Calculator, the impact of specific (configured) module rules are also displayed. For instance, if you have the Progressive Billing module and have defined a rule that includes this customer, an increase in the Sample Charge (from applying the custom rule) is visible.

---

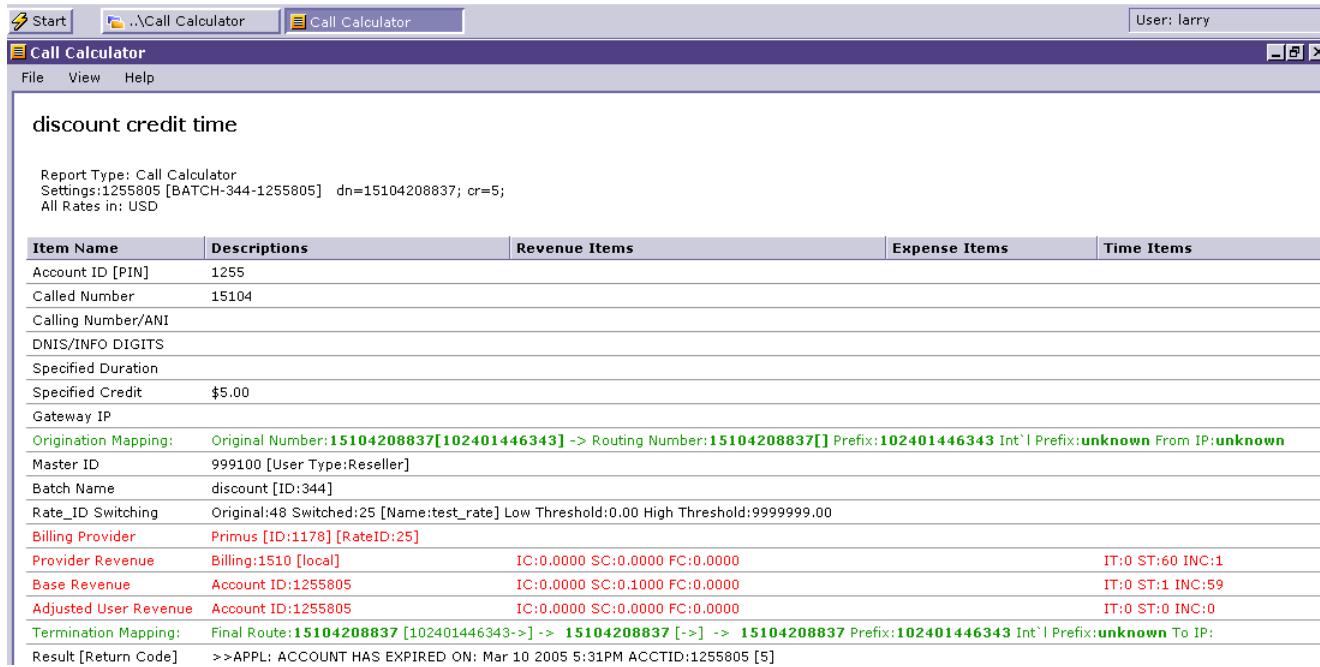
## Call Calculator Configuration/Generation

In this section, we look at the parameters that make up a Call Calculator report, and describe how to create and generate the actual reports.

The Call Calculator produces a summary that includes these parameters:

- Account ID. Identifies the caller’s account.
- Called Number. Specifies the number called.
- Calling Number/ANI. Describes the calling number.
- DNIS/INFO DIGITS. Specifies the DNIS prefix, as appropriate.
- Specified Duration. Sets out the call’s length.
- Specified Credit. Credit that exists for the account, if any (can be applied to the call).
- Gateway IP. Termination gateway IP Address.
- Origination Mapping. If mapping is involved, specifies details of origination mapping.
- Master ID. Relevant for resellers and wholesalers (agents in the Managed Services implementation).
- Batch Name. Name of the batch to which the caller account belongs, if any.
- Termination Mapping. Details of any termination mapping applied.
- Result. Shows result of call (success or failure).

## Call Calculator



**Figure 1-135Call Calculator**

The Call Calculator is activated when generated (one of the several relevant Edit menu options). Each call calculator must be configured before it can be generated. Once configured, it can be run (generated) multiple times.

The relevant Edit menu options are:

- New Call Calculator
- Edit Call Calculator
- Delete Call Calculator
- Generate Call Calculator
- Export Call Calculator

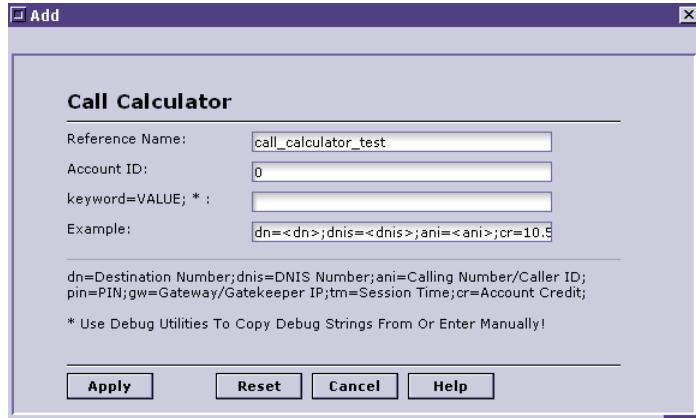
Each option is presented as a separate topic, to follow.

### New Call Calculator

The first step to generating a call calculator is creating it. This really means assigning identifying parameters that serve as reference when you generate the calculator or want to modify its definition.

To create a new call calculator:

- Step 1** Open the Console and Navigator, if you have not done so.
- Step 2** Select Event Monitoring>Call Calculator.
- Step 3** Choose Edit>Add New Call Calculator. The edit dialog is displayed:



**Figure 1-136New Call Calculator Definition**

- Step 4** Assign a name (reference name).
- Step 5** Set an Account ID.
- Step 6** Assign a keyword string, copied from debug settings or manually entered.
- Step 7** Set sample (Example) parameters that will be displayed in the generated report.
- Step 8** Select **Apply** to save changes and create the new calculator.

### Edit Call Calculator

To edit an existing call calculator:

- Step 1** At the Navigator, select **Event Monitoring>Call Calculator**.
- Step 2** From the Call Calculator window, select the specific entry (calculator) to edit.
- Step 3** Select the Edit option **Edit Call Calculator**.
- Step 4** The edit dialog appears. Edit any setting desired.
- Step 5** Select **Apply** to save changes.

### Delete Call Calculator

- Step 1** At the Navigator, select **Event Monitoring>Call Calculator**.
- Step 2** From the Call Calculator window, select the specific entry to delete.
- Step 3** Select **Edit>Delete Call Calculator**.
- Step 4** Confirm the operation at the Windows prompt, and the selection is deleted.

### Generate Call Calculator

Generating a call calculator produces the actual call simulation report. To generate a call calculator:

- Step 1** At the Navigator, select **Event Monitoring>Call Calculator**.
- Step 2** From the Call Calculator window, select the specific calculator to generate.
- Step 3** Select **Edit>Generate Call Calculator**.
- Step 4** The report is generated (see Figure 6-1).
- Step 5** Save, print or export the calculator for future reference.

**Step 6** Close the calculator window when done.

### Export Call Calculator

You can also export a call calculator, which is a way of 1) saving the report 2) sending it to another location for future reference and recall.

VoiceMaster provides two ways to save a calculator. The first method uses the Edit menu:

- Step 1** At the Navigator, select **Event Monitoring>Call Calculator**.
- Step 2** From the Call Calculator window, select the specific calculator to export.
- Step 3** Choose **Edit>Export Call Calculator**.
- Step 4** The Windows File Download dialog appears. Select **Save**.
- Step 5** The **Save As** window is displayed. Select a target directory to save to, and select **Save**.

The second Export option is available after you generate the calculator itself:

- Step 1** Generate the specific calculator you wish to export.
- Step 2** From the Call Calculator's File menu, select Export.
- Step 3** Now repeat Steps 4 and 5 from the previous instruction.

# System Alerts

As described, three basic types of system alerts are available for an Administrator to configure:

- **Account Alerts** provide the administrator notification when selected clients have failed balance thresholds or whose accounts are ready to be recharged.
- **Gateway Alerts** allow configuration of alert notification in the case of 1) Latency threshold breaching, 2) ASR (average success rate) failures, and 3) access point monitoring.
- **API Alerts**. API alerts activate custom scripts or application when the designated event occurs. This is also where fraud notification is configured in the event of fraud (remember, fraud detection is configured through Security Settings and the Fraud Detection option).

We describe each alert type in its own section, including configuration instructions.

## Account Alerts

Account alerts notify the Administrator when client accounts drop below an acceptable balance level or reach a recharge threshold requiring administrative action (add funds to the account).

Alerts may be set for different groups of clients. You can set a Balance alert for a set of clients, then a Balance with Recharge alert for another group of clients.

---

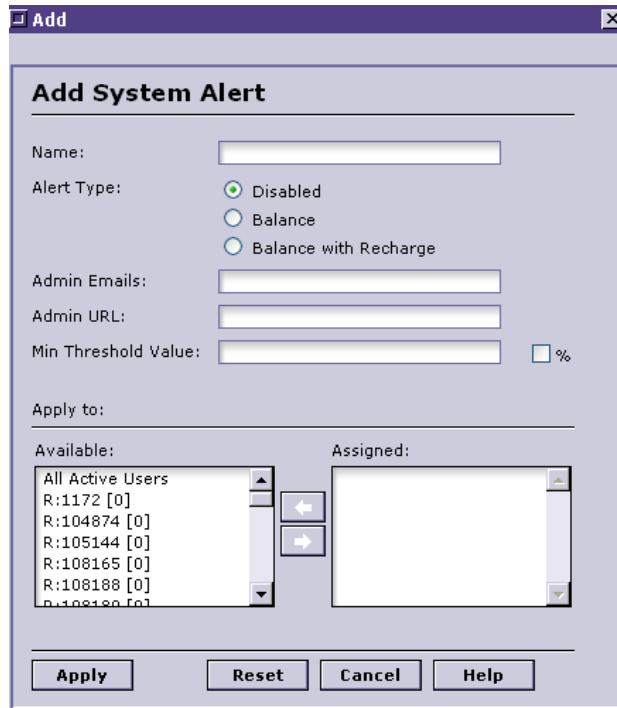
**Note** As the dialog box selection options show, one or the other of these account balance alerts may be configured. By definition, these alert types serve different purposes.

---

To configure an account alert:

- Step 1** At the Navigator, select **Event Monitoring>System Alerts**.
- Step 2** Choose **Account Alerts** from the System Alerts window.

- Step 3** Once the Account Alerts window is visible, select **Edit>Add System Alert**. The configuration dialog is displayed:



**Figure 1-137Creating an Account Alert**

- Step 4** Assign the new alert a name.

- Step 5** Select Alert Type, where the two basic options are *Balance* and *Balance with Recharge*.

---

**Note** Selecting Disabled as the alert type means that you must select the alert and activate it for it to take effect. That is done by choosing one of the two Alert Type options and applying the settings.

---

- Step 6** Assign administrative E-mail address and URL as destinations when the configured alert occurs.
- Step 7** Set a minimum threshold value (in dollars) to trigger the alert.
- Step 8** Assign users to the alert.
- Step 9** Select **Apply** to save changes and configure the alert.

To modify an existing Account Alert:

- Step 1** At the Navigator, select **Event Monitoring>System Alerts**.
- Step 2** Choose **Account Alerts** from the System Alerts window.
- Step 3** Select the specific alert to modify.
- Step 4** Select **Edit>Edit System Alert**. The same dialog is presented, except in its currently configured form.
- Step 5** Change any current settings and apply changes.

---

**Note** Refer to these alert modification and deletion instructions when reading the sections on Gateway and API alerts. Just apply the same procedures, remembering to select the appropriate alert type in Step 2 above.

---

To delete an alert:

- Step 1** At the Navigator, select **Event Monitoring>System Alerts**.
- Step 2** Choose **Account Alerts** from the System Alerts window.
- Step 3** Select the specific alert to delete.
- Step 4** Select **Edit>Delete System Alert**.
- Step 5** At the confirmation prompt, confirm the deletion to remove it.

## Gateway Alerts

Gateway alerts set notification for events related to gateway performance:

- Latency. Triggers administrator notification if gateway processing performance lags the configured threshold.
- ASR (average success rate). Configures alert when call success rates for the selected gateway fall below the threshold.
- Access point monitoring. (Future implementation)

To configure a Gateway alert, follow this procedure:

- Step 1** Select **Event Monitoring>System Alerts**.
- Step 2** Choose **Gateway Alerts** from the three options.
- Step 3** Select **Edit>Add System Alert**. The configuration dialog specific to gateways appears:



**Figure 1-138Adding a Gateway Alert**

- Step 4** Assign the IP Address for the gateway to be monitored.

- Step 5** Select an alert type: Latency, ASR, or Access Point Monitoring (as with Account Alerts, selecting ‘Disabled’ means you need edit the alert after configuration to activate it).
- Step 6** Set the destination/contact information to be notified on alert incidence.
- Step 7** Set a threshold value, relevant to Latency and ASR alerts. For latency, the threshold is a time, measured in seconds. In the ASR alert instance, the threshold is a percentage. If calls routed through the target gateway fall beneath this level, the alert occurs.

---

**Note** For ASR Alerts, check the percentage box next to the Min. Threshold Value field. Otherwise, alert configuration is not set.

---

- Step 8** Select **Apply** to confirm changes.

To modify or delete a gateway alert, follow the same procedures shown in the previous section on Account Alerts. Just be sure to select the Gateway Alerts folder when choosing a specific alert to modify or delete.

## API Alerts

API alerts trigger custom scripts or applications based on an instance of a configured event. When the event occurs, VoiceMaster sends a HTTP POST request and/or an E-mail to the address/URL specified in the API Alerts configuration dialog.

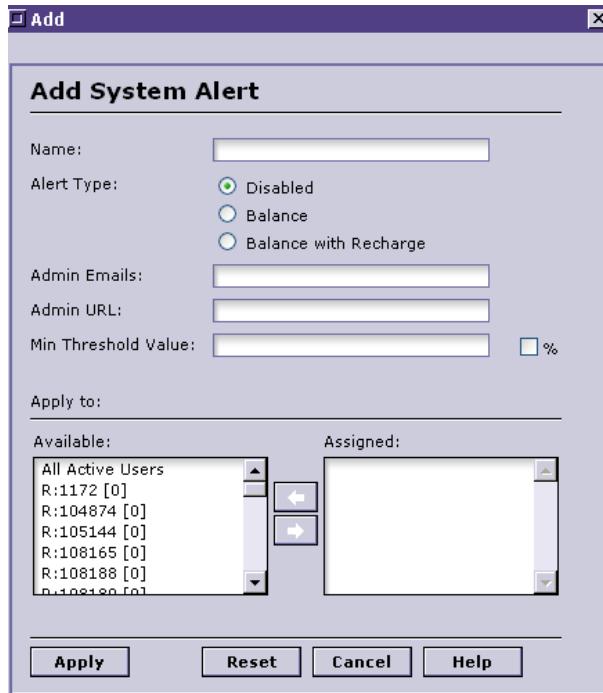
The specific API alert types are:

- Service API - Account Management. Sends alert to notification destination when an account is created, modified or deleted.
- (*Service API - Service Management*). Used for NORFA subscription/unsubscription (see NORFA documentation or contact VoiceMaster Tech Support).
- Service API - CDR Management. Sends an alert whenever the system receives a call.
- (*Service API - E.911 Management*). For wireless functionality, not in purview of this Guide.

In addition to facilitating configuration of API alerts by type, this dialog lets you trigger fraud notification, a key piece of the security administration. This will be discussed in procedural context.

To create an API alert:

- Step 1** At the Navigator, select **Event Monitoring>System Alerts**.
- Step 2** Make **API Alerts** your selection from the three alert options.
- Step 3** When the API Alerts window displays, select **Edit>Add System Alert**. The configuration dialog specific to API alerts is produced:



**Figure 1-139API Alert Creation**

**Step 4** Give the alert a name.

**Step 5** Select a type.

- (a) To establish a standard API alert, select either the first or the third ‘Service API’ options, depending on whether the alert is for 1) account management 2) CDR management.
- (b) To set a general fraud trigger that will notify the Admin when fraud detection settings have been breached, choose that radio button instead.

**Step 6** Define the administrator E-mail or URL for notification purposes.

**Step 7** Assign users to the alert.

**Step 8** Apply the settings to save the alert rule. Only if you selected Disables as the Alert Type will it not be immediately active.

# Real-Time Stats

Real-time Stats, the third option within Event Monitoring, offers a thorough set of views into network performance. The various statistics offer snapshots of call performance, of device registration, traffic distribution and active system redundancy (route failover). They include a current registry of endpoint registration and gateway performance on a *per gateway* basis.

We survey each of the individual options and how to use them in the targeted sections that follow.

## Current Calls

Current calls summarizes all current calls in the system. It shows calling and destination number, as well as routing and billing information.

The display is of all calls that have been placed but not finished. In other words, authorization has occurred and the call has gone through. A conversation is currently in progress.

## Finished Calls

Finished calls displays just that - the latest group of successful calls, now concluded.

## Hung Calls

Hung calls is a display of calls which have been made and then disconnected in progress. In other words, a failure occurred or a call was forcibly disconnected because of configuration settings that detected a user violation (fraud, account balance threshold violation, etc.).

Periodically the records of such calls are cleared from the system.

## Current EP Registry

The Current EP Registry displays all endpoints that have registered with - or been registered by - the VoiceMaster's gatekeeper functionality. This is a list of gateways and gatekeepers authorized to originate and terminate VoIP calls.

What this means in practice is that such devices 1) route call traffic to and from the Internet [IP network] after first compressing it [for the IP link] or decompressing it for transmission to a receiving station (telephone device).

---

**Note** See [Chapter One: Overview](#) or the Routing Management chapter for more details on endpoints, their functionality and how the VoiceMaster relates to and manages them.

---

## Current Internet Sessions

The Current Internet Sessions option not only provides 'live' statistics on ISP customer connection/use activities, it also enables related administrative actions.

We include procedural instruction for all referenced administrative options.

These options include 1) physical termination of a selected session 2) specific billing actions performed on the selected session. Every option (but the last) 'mixes' these two user-controlled actions. Each stops a session or all sessions. Depending on the specific option selected, the act of terminating a session does/does not trigger customer billing.

**Note** Each of these Edit options is irreversible, once confirmed. No intermediate steps or dialogs are part of these functions.

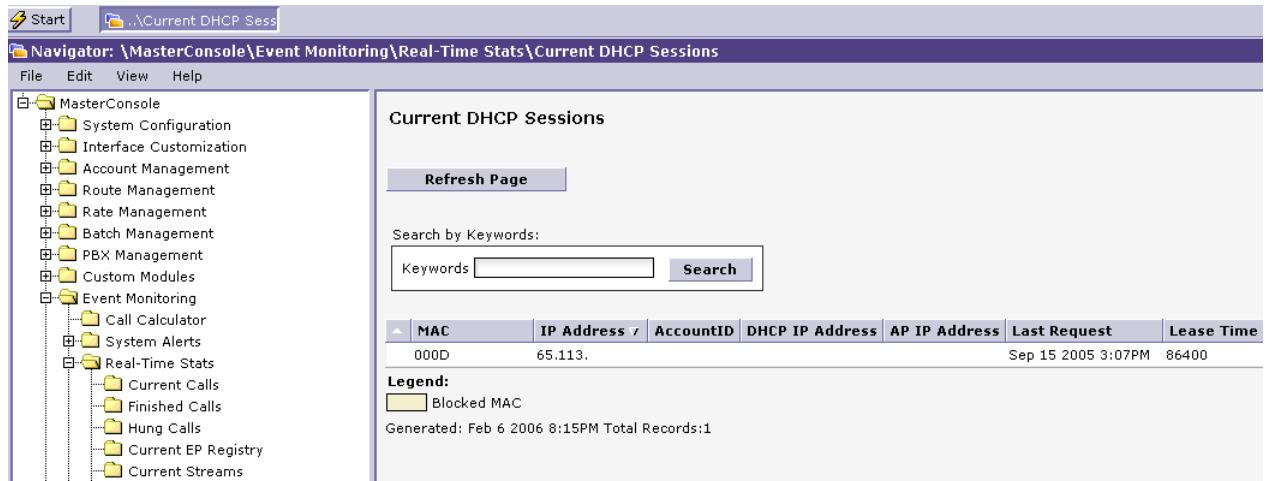
Specifically, the related Edit menu options are:

- **Stop Session and Bill**. Halts the selected session and bills user.
- **Stop All Sessions and Bill**. Terminates all sessions and bills all customers.
- **Stop Session - Do Not Bill**. Stops a session without billing it.
- **Stop All Sessions - Do Not Bill**. Stops all sessions (no billing).
- **Reset (Sync) Session Filters**. Resets current session filters. This is a safety measure that will synchronize session data between the system database and the operating system that works with it.

To work with Current Internet Sessions:

**Step 1** Select Event Monitoring>Real Time Stats.

**Step 2** Select Current Internet Sessions. The list of current user sessions is displayed (here a single user/single session):



**Figure 1-140**Current Internet Sessions List

**Step 3** Select the desired user/session.

**Step 4** Select the desired Edit menu option to act on the highlighted user session. Refer to the menu descriptions list before this procedure before choosing any options.

**Step 5** No matter the option selected, you will be asked to confirm it at a Windows prompt. Confirm to execute.

## Current Conference Sessions

Current Conference Sessions, the next Real-Time Stats options, displays all current conference (call) sessions. These are calls that involve more than two parties (in most cases) and use conferencing technology (typically, these are audio or audio-video session).

The administrative functions that relate to conferences are:

- Stop Session
- Stop All Sessions

No billing aspects are included.

To manage current conference sessions:

- Step 1** Select Event Monitoring>Real Time Stats.
- Step 2** Select Current Conference Sessions, then the specific session desired.
- Step 3** Select the Edit menu and then the desired option to stop a single session or all current sessions.

Alternately, you can just select the option and view current session status. As with all event monitoring option, you can do pure monitoring or combine observation with administrative action.

## GW/GK Traffic Distribution

This is an abbreviation (you guessed it) for Gateway/Gatekeeper Traffic Distribution. The name is fairly self-explanatory. Selecting this option from the Real-Time Stats page produces a list of all currently active gateways and gatekeepers. Here is a sample result displayed:

The screenshot shows the 'Navigator' window of the MasterConsole. The left pane is a tree view of the navigation structure, showing 'MasterConsole' expanded to include 'System Configuration', 'Interface Customization', 'Account Management', 'Route Management', 'Rate Management', 'Batch Management', 'PBX Management', 'Custom Modules', 'Event Monitoring' (which is expanded to show 'Call Calculator', 'System Alerts', and 'Real-Time Stats' which further expands to 'Current Calls', 'Finished Calls', 'Hung Calls', 'Current EP Registry', 'GW/GK Traffic Distribution' (which is selected and highlighted in blue), 'Routes Failover', 'Gateway Monitor', and 'Call Shop Monitor'), and 'Call Shop Monitor'. The right pane is titled 'GW/GK Traffic Distribution' and contains a table with the following data:

EP ID	IP Address	Type	Provider
SPTNET-S	127.0.0.1:1	Gateway	Spectrum
SPTNET-R	127.0.0.1:1	Gateway	Spectrum
SPTNET-PL	127.0.0.1:1	Gateway	Spectrum
SPTNET-B	127.0.0.1:1	Gateway	Spectrum
SPTNET-BA	127.0.0.1:1	Gateway	Spectrum
SPTNET-PLE	127.0.0.1:1	Gateway	Spectrum
SMCISCO01	127.0.0.1:1	Gateway	DUMMY
SPTNET-VARNA	127.0.0.1:1	Gateway	Spectrum
reseller-agent	127.0.0.1:1	Gateway	DUMMY
gwt1	127.0.0.1:1	Gateway	ResellerAg
gwt2	127.0.0.1:1	Gateway	test_Provic
nikotel	127.0.0.1:1	Gateway	Primus

Figure 1-141 Sample GW/GK Traffic Distribution

Here is the full set of descriptive parameters per endpoint device:

- EP ID: Device name, created on initial configuration.
- IP Address: The endpoint's IP address.
- Type: Gateway or Gatekeeper.
- Provider: Name of Provider associated with the device.
- Priority: (if relevant)

- Connections: Number of available connections
- Ports: Number of available ports
- Utilized%: Port utilization percentage
- Alarm: Shows if an alarm has occurred on the device.
- Daily Calls
- ASR%: Rate of call success through device as percentage of Average Success Rate.
- Latency: Amount of delay, if any, through endpoint.
- Avg.In KB/sec. Average incoming data flow.
- Avg.out KB/sec. Average outgoing data flow.
- Total Traffic KB. The sum of avg.in and avg.out = the average amount of total traffic, per second.

## Routes Failover

Routes Failover presents a comprehensive view of current route failover instances. All instances of failover are shown. Specific failover descriptions are included, such as:

- IP Address
- Area code
- Disconnect cause
- Last occurrence
- Count of total failovers per gateway/gatekeeper.

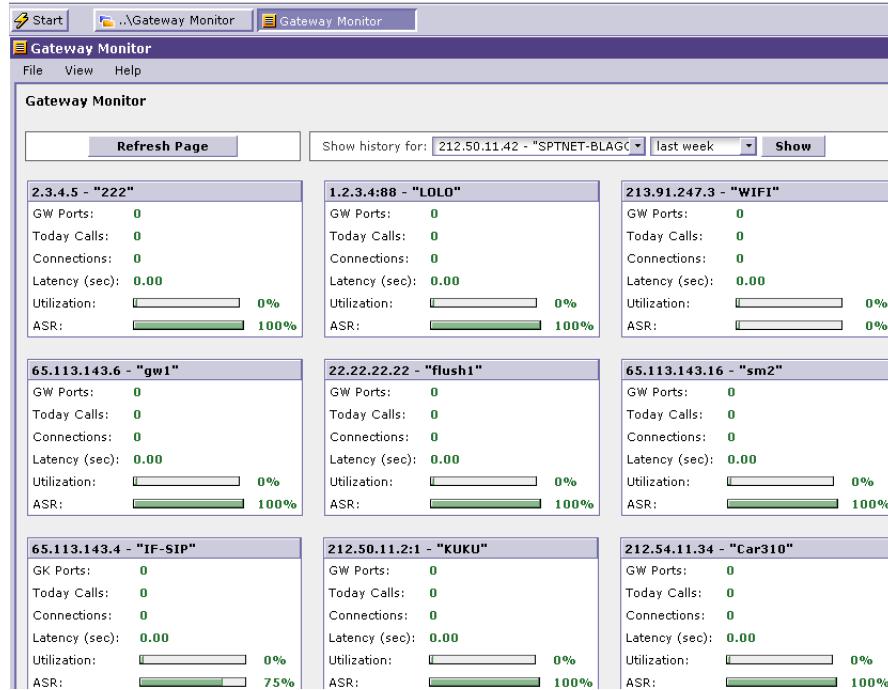
## Gateway Monitor

The Gateway Monitor function shows a graphical display of all system gateways. Besides offering a global display of all registered gateways, it offers historical views by gateway.

To use the Gateway Monitor function:

**Step 1** Select Event Monitoring>Real Time Stats.

**Step 2** Select **Gateway Monitor**. The current window is replaced with this view:



**Figure 1-142**Gateway Monitor

- Step 3** View the statistics per monitor.
- Step 4** Select a historical view for a specific monitor:
- Select a specific gateway from the **Show History For** option.
  - Choose a historical display period. A Gateway History window replaces that in Figure 5-75, with several graphs of different gateway functions:
    - ASR%
    - Average Profit
    - Total Calls/Successful Calls
    - Revenue/Expense
- Step 5** Close the Gateway History window.
- Step 6** Close the Gateway Monitor to return to the Real Time Stats view.

## Call Shop Monitor

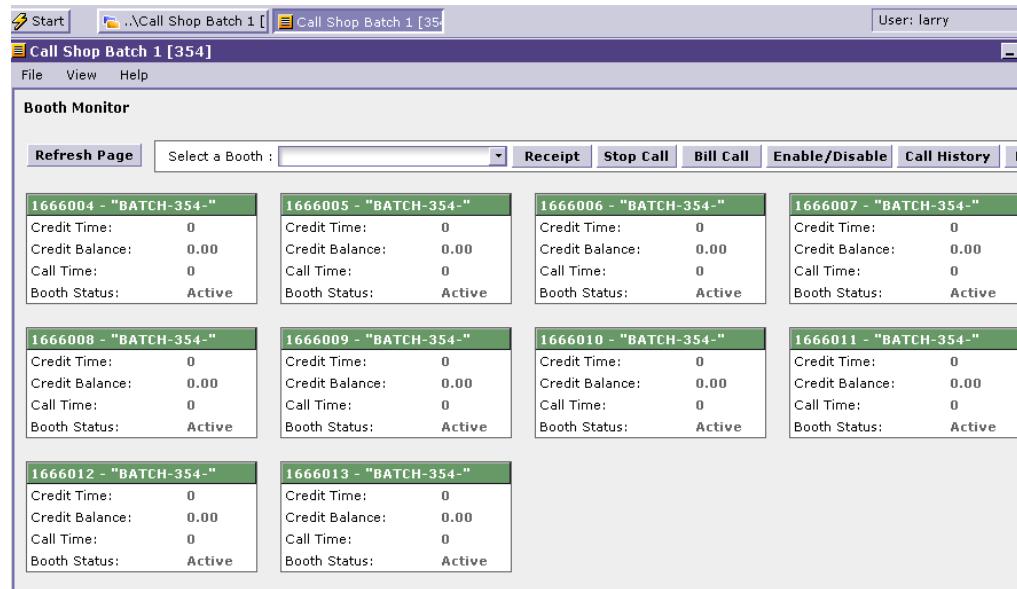
The Call Shop Monitor, the final statistics monitoring function, requires inclusion of the Call Shop module. (If your VoiceMaster does not include this module, the function will not appear in the Real Time Stats list.)

Call Shop Monitor also depends on the existence and utilization of VoIP Booth batches. A Booth Monitor view shows the status of VoIP use on a per-booth within a VoIP 'kiosk.'

The Monitor is more than just a monitor, though: an Administrator can then both view aspects of a booth status and manage them.

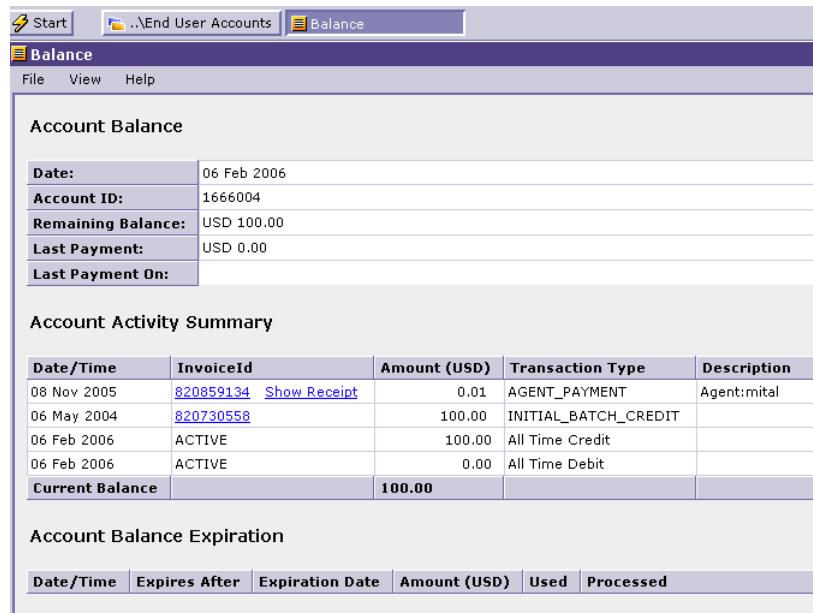
To use the Call Shop Monitor:

- Step 1** At the Navigator view, select **Event Monitoring>Real Time Stats**.
- Step 2** Select **Call Shop Monitor**.
- Step 3** Select the kiosk to view (each contains a set of booths). The Booth Monitor appears:



**Figure 1-143Booth Monitor**

- Step 4** View the set of current booth parameters.
- Step 5** Use the “Select a Booth” option to ‘load’ a particular booth, then use the options to the right to manage the selection:
  - Choose the **Receipt** option to open the latest invoice for the booth.
  - Select **Stop Call** to terminate calls currently in progress from that booth.
  - Select **Bill Call** to administer billing functions relevant to the booth. An Account Balance window opens (this should be familiar from the Account Administration chapter):



**Figure 1-144 Bill Call (Account Balance) Window**

Use the various options as desired:

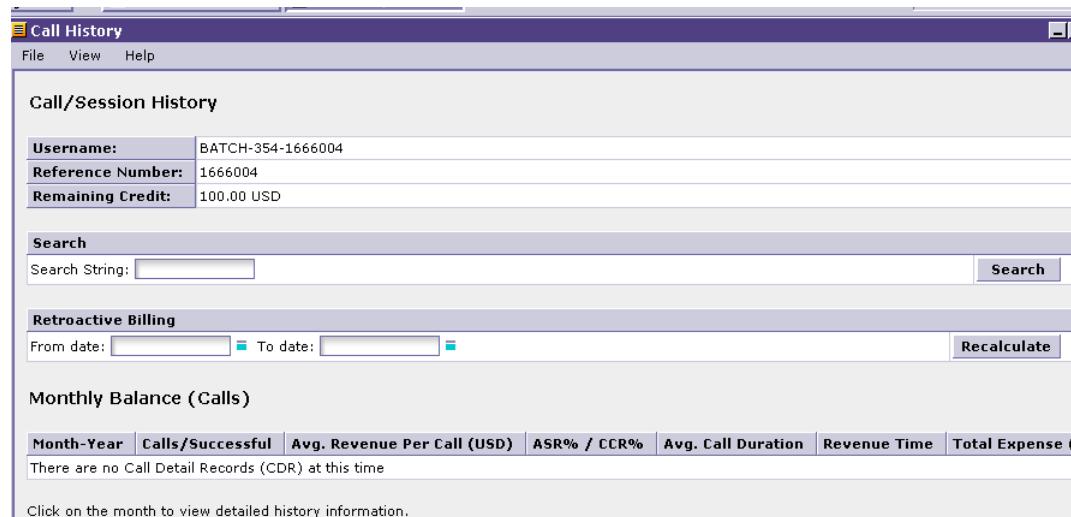
- Apply a Voucher Payment
- Redeem customer points at the Reward Point Management field
- Credit or debit the account.

---

**Note** Account Balance functions are discussed in [Chapter Five: Account Administration](#).

---

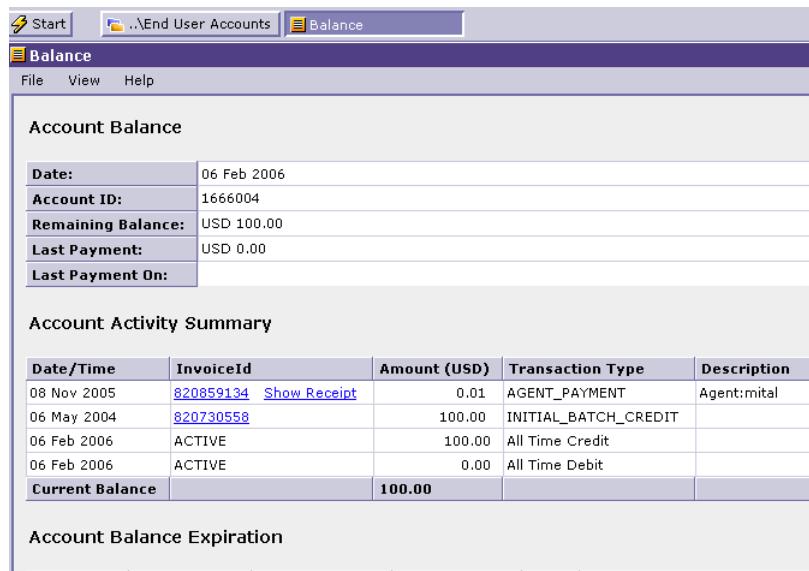
- Enable or Disable calls from the booth.
- View Call History. Select this to display this window:



**Figure 1-145Call History**

Now search for particular periods of booth activity or use the Retroactive Billing field to recalculate billing charges for a selected period. Enter From and To dates and select the Recalculate options. All found records are retrieved as a resource to correct the relevant billing records.

- Use the final option, **Balance**, to return an updated account balance view for the current caller:



**Figure 1-146Balance Window**

- Step 6** Close the window for the currently selected booth (or batch) to return to the base Call Shop Monitor view.

## Real-Time Logs

Real-time logs provide summary information for a variety of critical routing, billing and database functionality. All logs are accessible through the Real-Time Logs folder.

**Note** Certain logs must be configured (enabled) by the Administrator in order that the system will generate them. (Other logs are generated automatically, without user intervention.) The H323 Gatekeeper and SIP Registrar/Proxy logs are examples of user-enabled logs. How to enable them will be described in the appropriate sections.

The VoiceMaster real-time logs include:

- **SIP Proxy**. This log, enabled through the System Configuration/System Settings/Gatekeeper Configuration function (dialog), shows all SQL (database) queries related to the processing of SIP proxy calls.
- **FTP Messages** is a log that summarizes all FTP (File Transfer Protocol) access attempts to the system.

- **Database Monitor** log provides a split-screen summary of both current database load parameters and a listing of all currently running processes.
- **Credit Card Activity** shows all current credit card activity on the system (most of this CRM related).
- **APS Log**
- **Backup Log** displays all system components that have been backed up (master to slave) as part of the system redundancy functionality.
- **CDR Extract Log** displays call data records, specifically error instances.
- **Web Access Log** shows all web template creation and modification instances.
- **Radius** visually summarizes all Radius call authentication activity in the system. The Radius log is only displayed if first enabled via System Configuration/Billing Settings/Call Configuration. A specific setting in the associated dialog lets you enable this log.
- **H323 Gatekeeper**, like the corresponding SIP log, lists queries made to the server as part of processing H323 call requests. Also enabled at System Configuration/System Settings/Gatekeeper Configuration.

## Using Logs

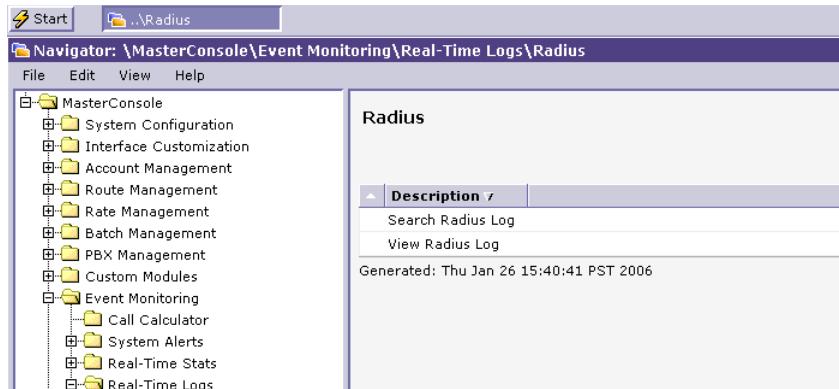
Accessing and viewing VoiceMaster logs is a fairly straightforward process. However, depending on the particular log, user options can vary.

The first and most typical log selection process involves:

- 1 Selecting **Event Monitoring>Real-Time Logs** from the Navigator.
- 2 Selecting the specific log that you wish to view.

For some logs, the user is offered the ability to define the result (to select a specific group of records to view). For these logs (Radius) is one example, a view-or-search option is added. This changes the selection procedure to:

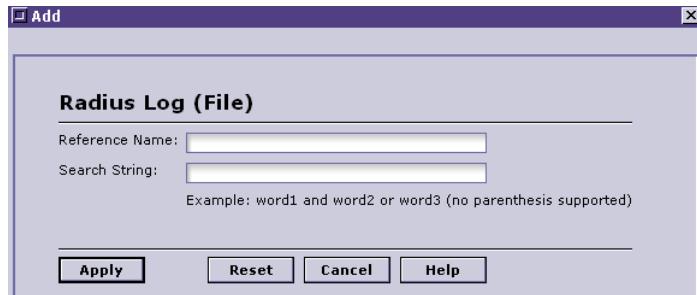
- 1 Navigate (select) Event Monitoring>Real Time Logs.
- 2 Select the log to view. The active window shows the log name and then a View and Search option, as here:



**Figure 1-147Radius Log Selection**

- 3 To view the entire log, just select **View Radius Log**. The entire log is presented, with results undifferentiated.

- 4 To display a selected subset of the entire log:
  - (a) Select **Search Radius Log**.
  - (b) Choose **Edit>New Report**. Use this dialog to define search boundaries:



**Figure 1-148Radius Log Definition**

- (c) Assign a reference name (searching the specified parameter requires creating the search entity, analogous to creating any other entity such a route or rate).
  - (d) Set a search string.
  - (e) Select Apply. The search entity, delimited by the string, is saved to the Search Radius Log window.
- 5 To generate the log and view its results:
    - (a) Select it from the Search Radius Log window.
    - (b) From the Edit menu, choose **Generate Report**.
    - (c) The log creation process (and viewing) involves downloading the file to your system. You are asked to confirm File Download. Select Open to view the file, or Save to save it to a specified location on your system.
    - (d) No matter which open you choose, the log is opened in Notepad or an alternate (default) text viewing program.

# Reports

Reports are the ‘flip side’ to real-time statistics and logs. Another valuable source of information about VoiceMaster events, reports are distinguished by their *historical*/nature. They provide information that summarizes events and actions after they occur.

Reports are no less valuable because of this. They offer a variety of different ‘looks’ into system performance, tendencies and characteristics. Their *use* may differ: an administrator may view and reference reports when the system is running smoothly or in order to gain an overall impression of operations before making changes in configuration settings.

Together with real-time statistics and logs, and special functions such as call calculators and system alerts, reports provide a stock of valuable clues and insights about network and system status.

Several kinds of report categories are available:

- **Rates**

Includes a variety of summaries of rate charges by VoiceMaster entities, or roles:

- System Rates shows all rates of all providers servicing a particular area code.
- Wholesaler displays rates of all wholesalers associated with the system.
- Reseller displays rates for all resellers, the same for Corporate Clients.
- Provider displays all provider rates - a summary of basic rates for every provider associated with your VoIP business.
- Area Code Termination shows all providers and rates set for a particular destination area code.

- **Stats**

These are post-event statistics that divide into several (selectable) functions:

- System stats, showing all calls in the a selected period.
- Account stats displays account (balance, etc.) stats for the designated time frame.
- PIN stats displays a variety of stats about a targeted PIN batch.
- Batch stats shows statistics for individual batches (another way to organize PIN viewing).
- MLM stats displays a report of any multi-level marketing programs used to sell VoIP service.

- **System Reports**

This is a miscellaneous category with a number of unique report views:

- Call History
- Call Messages
- Console Sessions
- Disconnect Causes
- Fraud Detection
- Low Balances
- System Messages
- Transactions

We will discuss the purpose of System Reports in more detail in the associated section.

- **Accounting Reports**

Accounting reports are of two types, or categories - Accounting and Invoices. Each of these in turn splits into very specific reports. We elaborate the full list of options and the differences between them in the Accounting Reports section.

---

**Note** In the following sections, we look at each Reports category in more detail. Read the Rates section carefully; it includes a ‘template’ for creating and generating VoiceMaster reports. E. However, specific procedures and dialog boxes are described where report creation differs from the ‘template’ instruction.

---

## Rates

Rates reports provide three different views, or angles, into available rates within the system:

- System-wide view, available through the first, System, option
- Views by entity type. Each type of participant in the system plays a part in overall rates, and the next group of options lets you peek at each of these: wholesaler, reseller, corporate client and provider.
- By termination endpoints serving specific area codes. This is a route-oriented rates perspective, showing available rates for calls to a particular area code,

### Using Rates (A Template for Report Creation/Generation)

As with any report type (and here you can refer to the Call Calculator and Radius log reports discussed earlier), Rates reports must be created before they can be generated. The procedures in this section describes both report creation and generation.

Let’s take a quick look at the Edit menu options when a user selects the Rate option. The basic options are common to each available VoiceMaster report.

- New Report
- Edit Report
- Delete Report
- Generate Report
- Export Report

---

**Note** We will include a ‘template’ procedure for one of the Rates reports. The identical procedure is applicable to the various Rates reports.

---

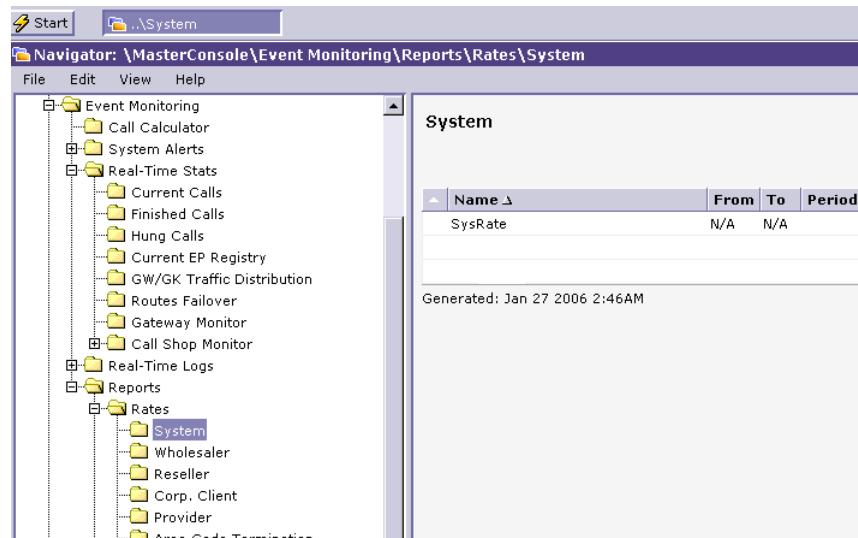
To create a Rates report, do the following (the report in this example is System Rates):

- Step 1** From the Navigator, select **Event Monitoring>Reports**.
- Step 2** Choose **Rates>System**.
- Step 3** Select **Edit>New Report** to work with this dialog:



**Figure 1-149Creating a Report**

- Step 4** Enter a reference name.  
**Step 5** Apply creates the new report, saved as named:



**Figure 1-150SysRate1 Report**

To generate any existing report:

- Step 1** From the Navigator, select Event Monitoring>Reports.  
**Step 2** Choose Rates>System.  
**Step 3** From the System (Reports) window, select the report to generate.  
**Step 4** Select Edit>Generate Report. The report is displayed:

The screenshot shows a software window titled 'System'. The menu bar includes 'File', 'View', and 'Help'. The main area displays a report titled 'Report Type: Area Code Termination Rate Report'. It shows a table with the following data:

Dial Code	Location	Provider	InitTime	InitCharge	SampleInterval	SampleRate	IncrementTime	CallOrigCharge	CallTermCharge
1510	local	Primus	0.00	0.0000	60.00	0.0000	1.00	0.0000	0.0000
1510	United States - California	Primus	30.00	0.0130	60.00	0.0260	6.00	0.0000	0.0000
1510	Emeryville	Primus	0.00	0.0000	60.00	0.0300	0.00	0.0000	0.0000
1510	emeryville	Primus	0.00	0.0000	60.00	0.1200	1.00	0.0000	0.0000
1510	bay area	Primus	0.00	0.0000	60.00	0.1500	60.00	0.0000	0.0000
1510	emeryville	Primus	0.00	0.0000	60.00	0.1500	1.00	0.0000	0.0000
1510	emeryville	Primus	0.00	0.0000	60.00	1.5000	1.00	0.0000	0.0000
1510	emeryville	Primus	0.00	0.0000	60.00	1.5000	1.00	0.0000	0.0000
1	USA	Primus	0.00	0.0000	60.00	0.0000	1.00	0.0000	0.0000
1	1	Primus	0.00	0.0000	60.00	0.0100	1.00	0.0000	0.0000
1	USA	Primus	30.00	0.0085	60.00	0.0171	6.00	0.0000	0.0000
1	usa	Primus	0.00	0.0000	60.00	0.0195	1.00	0.0000	0.0000
1	US	Primus	0.00	0.0000	60.00	0.0200	1.00	0.0000	0.0000
1	US	Primus	0.00	0.0000	60.00	0.0200	1.00	0.0000	0.0000
1	North America	Primus	30.00	0.0130	60.00	0.0260	6.00	0.0000	0.0000
1	USA	Primus	0.00	0.0000	60.00	0.0300	20.00	0.0000	0.0000

**Figure 1-151Generated System Report**

**Step 5** View the report (every report will have a different set of contents).

**Step 6** Use the File menu to save, print or export the contents.

This procedure applies to every type of Rates report.

## Stats

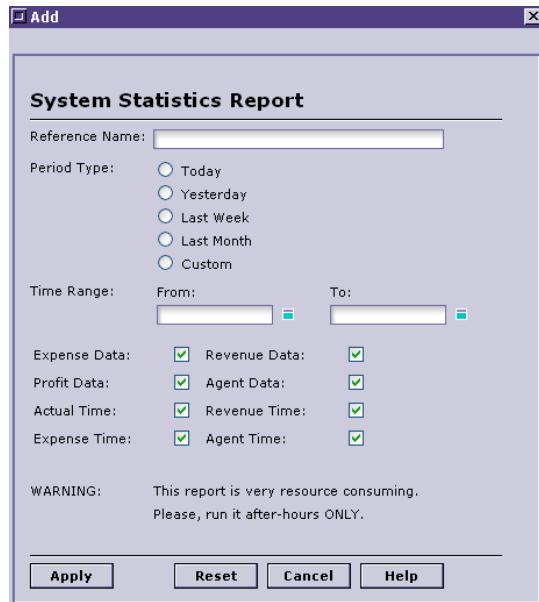
Stats, the second Reports category, itself divides into several types of statistical report views:

- Account Stats
- Batch Stats
- MLM Stats
- PIN Stats
- System Stats

Each of these is described in the overview that preceded discussion of each Reports category.

The procedure for creating or running (generating) any of these reports is the same. Refer to the Rates procedural template. However, please note that the report creation dialog boxes differ from the simple Rates report dialog.

If, for instance, your selected Stats report category is System Stats, selecting Edit>New Report brings up this dialog:



**Figure 1-152Add System Stats Dialog**

This dialog includes strict period definitions and time ranges. It also lets the user select different data view options (expense and profit). Additionally, you can filter how time is presented.

---

**Note** Please observe the WARNING at the bottom of each Statistics report creation dialog. These reports are very resource-intensive and should be run when system resources are not taxed.

---

Each stats report creation dialog is unique. We show the Account Stats creation dialog as an example:



**Figure 1-153Account Stats Report Definition**

No matter the specific Stats function for which you define and generate reports, the basic procedure for creating and generating reports remains the same.

## System Reports

System Reports provide a full range of specific looks into system performance.

---

**Note** Just as with statistics, system reports consume system resource intensively. Please generate these reports only after hours or when the current system load allows it.

---

They include:

- **Call History.** This report, which can be produced in interactive or file form, displays recent calls in the system. The interactive form appears in an application window, the file form in a text (Notepad) file.
- **Call Messages.** Call messages lists all failed calls by account number, specifies call parameters and provides a reason for the failure (such as ‘no route available’).
- **Console Sessions.** This is really a log of all Administration Console users (administrators and other roles) who have logged in during the current day. It includes their name, session start time and IP address.
- **Disconnect Causes.** This lists disconnected calls within a designated period, and reports endpoint device used, the cause itself, and how the disconnect was noted (Radius).
- **Fraud Detection.** The Fraud Detection report is activated if the fraud detection measures (System Configuration/Security/Security Settings) are enabled and configured. If fraud is detected, the system 1) acts against it, 2) notifies the Administration if notification is enabled and 3) compiles the results in this report.
- **Low Balances.** This report displays all accounts where balance amounts are either ‘in the red’ (below zero) or below a threshold set for those accounts.
- **System Messages.** This report goes the Console Sessions report one better. It displays all Console logins, but also specific configuration actions and associates them with the users who performed them.
- **Transactions.** Displays all system transactions.

As with any other reports, producing the System Reports requires 1) report definition/creation 2) report generation. The dialog boxes used to configure these reports are similar to those used to create Stats reports. However, each is a little different and will have one or more of these parameters:

- Reference Name. Creates an ID for the report.
- Period Type (day, week, month, etc.)
- Time Range. Actual time frame for which the report will generate results.

Specific reports will have fewer or more parameters, depending on their purpose, depth and breadth. Other reports will have unique, specific parameters and fields.

For instance, the Call History report ‘Add’ dialog asks the user to define the data and time presentation parameters by type (expense data, revenue data and so on).

The Disconnect Cause report requests user selection of specific gateway(s) for which to return disconnect results.

The Low Balances report requires that you set a threshold (accounts reporting amounts lower than the specified threshold will appear in the report).

The Transactions Report requires the user to specify the batch of customers for whom to report transaction results.

## Accounting Reports

Accounting Reports, on the surface, is a simple set of reports that summarize aspects of accounting and invoices. The two main Accounting Report types are:

- Accounting
- Invoices

Beyond these report headings are a full complement of reports. Accounting Reports is the repository for a full set of reports, and includes:

- Revenue
- Expenses
- Agents
- Gateways
- Traffic

Each of these has its own sub-reports, which will be covered in the appropriate sections.

**Invoices** is a simpler category, in that it has only one function, Outstanding Payments.

Most of this section is devoted to explanation of the ‘Accounting’ option and its sub-options.

### Revenue

This first Accounting function harbors several perspectives into overall revenues. It presents specific revenue sources as well as total revenue. The specific revenue reports are:

- *Users* summarizes data for individual customers within a specified time frame.
- *Wholesalers* returns similar results (individual parameters to be specified by the Admin).
- *Resellers* - again, customized revenue data for specific resellers within specified time periods.
- *Corporate Clients* Specified corporate client revenue is returned.
- *Total Revenue* shows all revenue within the specified period (again, customized by data type and time view).
- *Internet Revenue* displays all ISP service revenue within delimited time parameters.

To create and generate any of these reports, use the familiar steps:

- 1 Navigate to the desired report function. For instance, to select Users you would (from the Navigator) select Event Monitoring>Reports>Accounting Reports>Accounting>Revenue>Users (a long path, but it’s worth it).
- 2 Select Edit>New Report and receive the report configuration (Add) dialog. In the case of the (Revenue) Users report, it looks like this:



**Figure 1-154Add User Report (Report Definition)**

- 3 Set all the parameters:
  - (a) Reference Name
  - (b) Account ID
  - (c) Period Type
  - (d) Time Range
  - (e) Specific accounting data, including billing-related time parameters
- 4 Select Apply and the report is created.
- 5 When ready to generate the report, navigate to the Users window by selecting the folders in the order described in Step 1.
- 6 Then select the specific report (created in Steps 1-4) to generate.
- 7 Choose **Edit>Generate Report**. The report is returned as specific parameters (in each revenue report, these will differ).
- 8 View the report. Save, export or print it as desired.

## Expenses

Accounting expenses reports provide views both of system expenses and by specific billing component and location. When generating any of these reports, the VoiceMaster will look for and return call records corresponding to report parameters.

The Expenses reports categories are:

- **Providers.** Administrator can configure provider reports to display costs of using provider services. Select specific provider (or all providers) and customize report to generate desired results in graph form.
- **Termination Gateways.** Shows charges to a selected gateway or gatekeeper within selected time period. Customizable to show desired data and time expenses.

- **Total Expenses.** Identical configuration options to the more specific expense reports, except will return results, in graphs, for the entire system.
- **Internet Expenses.** The final Expenses report is another ‘full-system’ view of expenses, this time for costs related to ISP service. The difference between this report and the previous (Total Expenses) is that instead of call statistics (ASR, etc.), the Admin will view IP traffic stats (kilobytes and packets) along with the various expenses.

Procedures for producing these reports are identical to those for creating user reports. The report configuration dialogs are also remarkably similar, as this Provider report dialog demonstrates:



**Figure 1-155Provider Expense Report Under Construction**

As with any other VoiceMaster report, adding a report means configuring the parameters. Reports can not be generated until first labeled and defined, as the user is doing in this example. Once configured, a report can always be modified and generated again. The Console and its functions are designed to place full control in the user’s hands.

## Agents

Agents reports return expenses for the different types of agent:

- Reseller
- Wholesaler
- Corporate Clients
- Commission Agents
- Routing Providers

Expenses, profits and revenues may all be produced and viewed.

Report configuration and generation are identical to those for other reports.

## Gateways

Gateways reports can be generated for both kinds of gateways in the system:

- Origination Gateways
- Termination Gateways

The user selects specific gateways for which to create and generate reports. Returned results show the configured report on a per-gateway basis, with selected parameters (expenses, profits, revenues, etc.) displayed.

## Traffic

Traffic reports are of four different kinds:

- Users. System traffic (calls) pertaining to specific users, identified by accounts, is produced when this report is generated.
- Termination Providers. All traffic for a selected termination provider over a specified time period can be configured and generated for review.
- Gateways. Traffic results are generated for selected, individual gateways or for all gateways.
- Special Numbers. This final Accounting report displays traffic results for particular ‘special’ numbers through user-identified gateways. This may be useful to track specific customer behavior, often in association with security policy (fraud monitoring and detection).

## (Accounting) Invoices

The second main category within Accounting Reports, Invoices, contains one Report option or function. This is Outstanding Payments.

Outstanding Payments requires the configuration of a report that specifies an individual account and a time period within which to return results. When generated, it shows what this customer owes.

---

**Note** Just as with certain other report generation, this report is processing intensive. It may occupy system resources while searching for its results, so use this facility after hours or when plenty of system resources are available.

---

# Chapter 7: Route Management

---

## In This Chapter

The relevant sections are:

- **Administration Console Overview.** A quick survey of key routing functions and options.
- **Routing Concepts & Configuration.** Routing in VoIP and in VoiceMaster.
- **Uniswitch.**
- **Special Routing Topics.** Included are discussions of unique and important routing topics:
  - Route Failover
  - Two-Stage Routing
  - Internal Routing
  - Virtual IP Addresses

## Console Overview

Routing is an important and prominent component of VoiceMaster's Administration Console. Most functions and actions associated with routing occur within the Route Management.

They include:

- **Global Route Settings.** This generic function has a single option, Global Route Management. This is used to configure a unique routing pattern by which all system routes are forced to the endpoints of a single provider.
- **Routes.** The Routes function is the starting point for system route management. Use it to add a custom routing table to the system.
- **Routing Tables.** Stores all individual routes, grouped by tables. Prioritize individual routes (assign 'preferred' status), import and export routes, synchronize a route (activate it on demand) or delete a route.
- **Prefix Routing.** Use this function to assign area codes to recognized (registered) gateways. Gateway area code assignment is a prerequisite towards creating a working VoIP calls.
- **Gateways.** This is the repository of all gateways known to the VoiceMaster system. Adding a gateway is another essential step in building a network. Defining gateway functional parameters (routing and billing) is a key aspect of this process.

- **Gatekeepers.** Used to store gatekeepers that are active within the system, either as complements to or in place of gateways. (A provider termination device, for instance, may be either a gatekeeper or a gateway.) A parallel function to Gateways, and similarly facilitates modification or deletion of individual gatekeepers within the list.
- **ASR Route Switching.** Used to configure, modify or delete ASR route switching functionality. ASR route switching involves the configuration of performance (success) thresholds for termination gateways/gatekeepers. Breaking thresholds causes the route to be switched to the designated alternate endpoint.

---

**Note** Much routing functionality (and flexibility) in VoiceMaster assumes the inclusion of the Custom Routes module. Without this module, only a single, system route is available. With Custom Routes, a variety of route management possibilities is available.

---

## Routing Concepts And Configuration

Basically, routing encompasses the registration of origination and termination endpoints (gateways and/or gatekeepers) and their assignment to a custom route (Route Table).

Registration of origination and termination endpoints are analogous processes. Both are essential ‘bookends’ to the IP link at the heart of the VoIP calls. By assigning them to a route, an administrator is configuring the data link portion of such calls.

These endpoints also link the PSTN (traditional phone) call segment and the data link.

- Origination gateways take the analog signal arriving from the customer and convert it into digital form, compressing it into data packets.
- The voice data travels to the termination gateway, which receives the digital signal, decompresses and translates it into an analog signal for the trip to the receiving telephone device.

Seen from this point of view, a VoIP call is a series of voice-data-voice transmissions. The person originating the call starts this cycle after the call is authenticated and routed. Say ‘hello’ and the process begins. When the called party responds (for example, with ‘How are you?’) the same route is traveled. The same translation from analog to digital to analog signal is executed.

---

**Note** Area codes are NOT assigned to origination gateways, only to termination gateways.

---

By default, VoiceMaster performs least cost routing. Least cost routing encompasses the selection of several parameters when selecting a route.

VoiceMaster filters these parameters when selecting a route:

- Longest prefix match
- Preferred Route flag
- EP priority number
- Route cost (least cost)
- Number of connections
- Average Success Rate (ASR)
- Connection latency

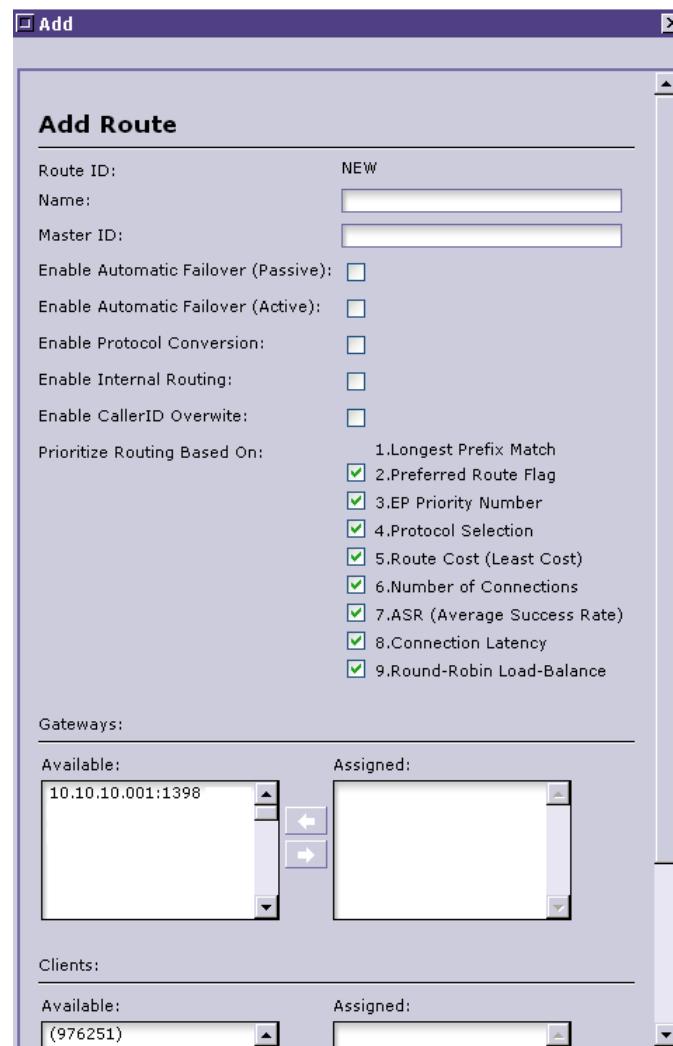
- Round-robin load-balance

---

**Note** We explore the meaning of these parameters in more depth later in this chapter.

---

An Administrator can select those parameters desired when routing calls, as is seen here:



**Figure 1-156Priority Routing Options: Selectable Parameters in Route Creation**

Setting route priorities by enabling desired ‘priority parameters’ is part of an Administrator’s route definition privilege. When a client assigned to the route initiates a call, a route is selected. The system uses an algorithm to check route preferences. Each enabled priority routing parameter is evaluated, and the route selected when the a checked parameter’s condition, or requirement, is met.

## The Role of Gateways

Gateways are network devices that provide call termination and origination services. Gateways are physical devices, usually small in profile, and include not only has port functionality but also essential software. The gateway is designed to include at least one conventional telephone port and another Ethernet port.

There are many types of gateways in existence today, ranging from those that support a dozen or so analog ports to high-end gateways with simultaneous support for thousands of lines. VoIP gateways, also called *media* gateways, are devices that bridge traditional telephone networks and their equipment to VoIP networks.

In the most common VoIP scenario, two gateways operate simultaneously. Each has data connectivity to the Internet and phone connectivity to the local Telco companies. A prime example of a gateway is the PSTN/IP gateway, connecting a H.323 terminal with the (telephone) switched circuit network.

On one side, the gateway interacts with its associated telephone devices through standard analog communication. On the VoIP side, the gateway communicates digitally with IP-fluent devices (gatekeepers, other gateways). It sends and receives IP packets with segments of conversations tucked away inside. ‘Talking’ with two different worlds and ‘languages’ requires the ability to translate between them. Gateways translate from analog to digital (IP) mode by compressing data using CODECs. In the other direction, it decompresses packet data and turns it into analog form for transmission over the PSTN link.

More specifically, a gateway:

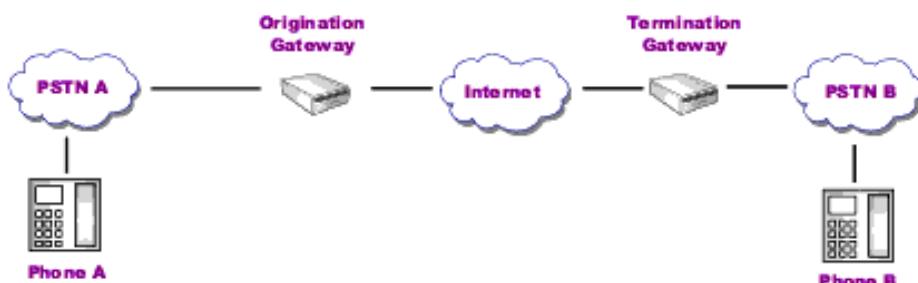
- Translates signaling messages
- Compresses and decompresses data:
  - Compresses analog (voice) data into digital form for IP transport (gateway-to-gateway)
  - Decompresses digital data and converts it back to analog for the PSTN segment (gateway-to-endpoint).

Depending on the network configuration, a gateway may originate and terminate VoIP calls for many endpoints.

Gateways also perform additional essential functions:

- Authenticating calls using in-built RADIUS functionality
- Providing an IVR (Interactive Voice Response) platform with queued messages that inform prospective callers of call authentication and authorization status.
- Recording call data and passing it to its associated gatekeeper for processing. Gateways function as ‘agents’, sending data that an administrator can use.

The following figure shows the placement and role of gateways within VoIP call architecture:



### Figure 1-157 Call Architecture

The call process works like this:

- **Phone A** makes the outbound call via **PSTN A**, the local Telco service that connects subscriber phones and gateways, using an analog service;
- The **origination gateway** receives the analog signal, authorizes the call (using AAA), converts it via compression to data (digital) form, and sends it through the Internet ‘cloud’ to the **termination gateway**;
- The termination gateway takes the compressed digital packets and decompresses them, converting the packets into analog voice signal.
- This signal travels via **PSTN B** to **Phone B**. (PSTN B is the equivalent Telco to PSTN A, servicing the receiver’s geographic area.)

The VoIP administrator must provision phone lines to the local Telco companies on both ends of this connection as well as data links to the internet for both gateways.

### Gateways and Routes

The process of routing encompasses the registration of origination and termination endpoints (gateways and/or gatekeepers) and their assignment to a custom route (Route Table). Area codes are assigned to specific gateway so that calls intended for those area codes are routed through the associated gateway (assuming the gateway is assigned to the route).

---

**Note** Area codes are not assigned to origination gateways.

---

In VoiceMaster, custom routes functionality allows administrators to specify call routing per client(s). In essence, custom routes map clients against one or more gateways. To do this, the administrator sets up relevant clients with their own routing tables (resellers, corporate clients or wholesalers).

Upon creation of a Custom Route (Route Table), system administrators must specify all origination and termination parties (gateways and gatekeepers) that participate in the route. Calls are routed only for the origination and termination parties specified. After origination and termination entities are added to the Rate Table, clients are assigned.

By default the VoIP Platform performs least cost routing. Least cost routing encompasses the selection of several parameters when selecting a route. The following parameters are filtered when selecting a route:

- Match longest area code
- Select routes with preferred status
- Select routes with highest EP priority
- Select routes with least cost
- Select routes with highest ASR
- Select routes with least latency

## Endpoint/Gateway Registration

A key part of the VoiceMaster's intelligent routing functionality is to identify termination devices and register them with the system. In most cases, this endpoint will be a gateway. Gateways can be origination gateways, that is, for use as the device that routes your customers' calls onto the IP network.

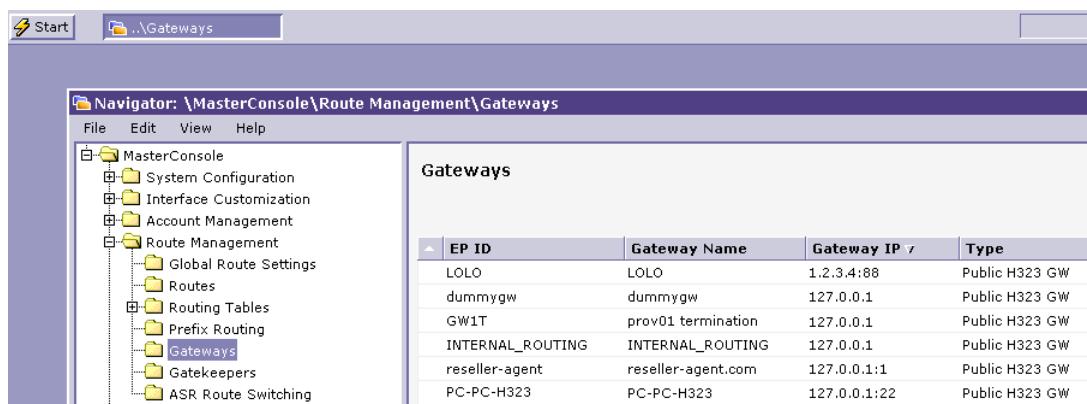
Prior to registering termination gateways, the administrators should obtain the following essential gateway attributes from the service provider(s).

- H323 Gateway ID
- Gateway IP
- Gateway Port
- Gateway Origination Map
- Gateway Termination Map

## Registering (Adding) Gateways

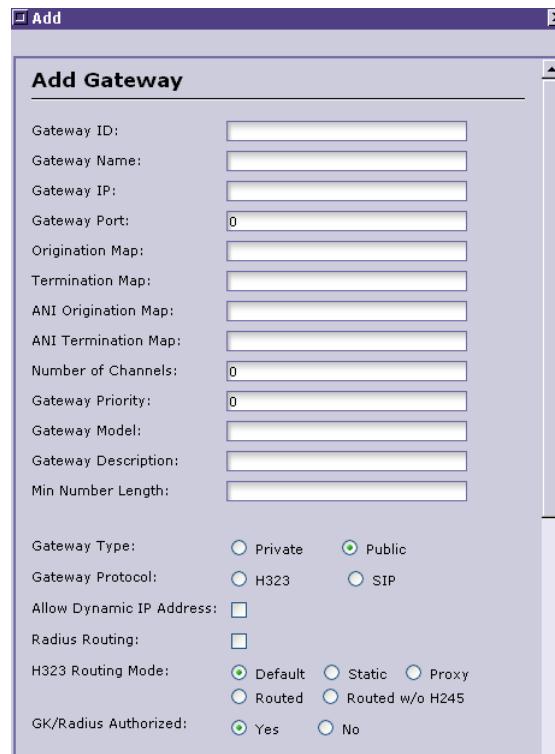
To add an individual gateway to the system, follow these instructions:

**Step 1** Select **Route Management>Gateways**. The Navigator view changes:



**Figure 1-158Route Management/Gateways Selection**

**Step 2** Select **Edit>Add Gateway**. The Add Gateway dialog appears:



**Figure 1-159Add Gateway Dialog**

**Note** Use the scroll bar to navigate within this and similar lengthy dialogs to view and edit all relevant parameters.

**Step 3** Define relevant parameters:

- (a) Gateway ID and name
- (b) Gateway IP address and active VoIP port
- (c) Origination and Termination map definitions (if relevant)

---

**Note** Mapping is used to normalize call origination/termination information and create compatibility with international standards.

---

- (d) Number of channels (if none, enter '0')
- (e) Gateway priority, if any;
- (f) Gateway model and description
- (g) Minimum number length
- (h) Gateway type (private or public)
- (i) Gateway protocol (H.323 or SIP)
- (j) Dynamic IP address (enable, if used)
- (k) Radius routing (only relevant if GK/Radius is set 'yes' in next step)
- (l) GK/Radius authorized (yes/no)
- (m) Gateway Owner/Provider (name)

---

**Note** You must identify the gateway owner in Step (m) or the new gateway will not be added to the Prefix Routing list. This is critical to building a route.

---

- (n) Radius Shared Secret (password)
- (o) Call Billing Management (Billing Call Legs). Call Billing settings determine which 'legs' of a call are billed. Select all billable legs.
- (p) Call Time and Per Call Adjustments. Define (optionally) additional charges.

**Step 4** Select **Apply** to save entries and add the provider gateway to the Gateways list.

### Critical Gateway Parameters

There are several important parameters to note when registering Gateways.

#### Gateway Origination Map

The Gateway Origination Map field specifies a set of rules used by the VoIP Gatekeeper for phone number translation. This is a routing procedure during which phone numbers are separated gatekeeper from any prefixes they might have. (The prefixes are stripped.)

---

**Note** Gateway Origination Map is used only when the registered gateway functions as an origination gateway. The number translation is performed by the VoIP gatekeeper before it routes a call over the IP network to the designated endpoint.

---

The Gateway Origination Map enables swift redirecting of calls. Its sophisticated functionality includes:

- Prefix Stripping and Pre-pending
- Arbitrary String Replacement (when the phone number is a string of numerical symbols)
- Removing certain parts of the phone number.

---

**Note** Gateway Origination Map functionality adheres to the E.164 number format standard. It is designed to enforce conformity to this standard, in which country code + city/area code + local number form the structure of any number. All international phone numbers should start with a country code. Prefixes do not fit this standard, which is why mapping is enabled (so they can be removed prior to call routing).

---

Some examples of gateway origination maps include:

**1510 = 1925;**

, where 1510 is the source phone number string to be replaced  
(e.g. source phone number: 1510222333 | target phone number: 19252223333)

**1510=;**

, where 1510 is the source phone number string to be deleted.  
(e.g. source phone number: 1510222333 | target phone number: 2223333)

**001#=;**

, where 011# is the prefix to be stripped  
(e.g. source phone number: 011#1510222333 | target phone number: 15102223333)

**=423#;**

, where . (dot) indicates a source phone number and 423# indicates the prefix to be pre-pended.  
(e.g. source phone number 1510222333 | target phone number: 423#15102223333)

**001# = 1510;**

, where 001# indicates the prefix to be replaced  
(e.g. source phone number 011#222333 | target phone number: 15102223333)

### Gateway Termination Map

Gateway Termination Map field, like its partner Gateway Origination Map, defines a set of rules for phone number formatting/transformation conducted by the VoIP Gatekeeper.

---

**Note** Gateway Termination Map is performed after Gateway Origination Map is completed. Number transformation is done on phone numbers supplied.

---

Here is a full Origination and Termination mapping scenario:

Existing Endpoints: GK - VoiceMaster Gatekeeper

**Gateway A** - defined as the origination gateway in the VoiceMaster system with an Origination map: **001#=;**

**Gateway B** - defined as the termination gateway in the VoiceMaster system with a Termination map: **.=8876#;**

Scenario:

A call coming from Gateway A reaches GK in the following format: **001#15103459987**. These steps ensue:

GK strips the origination map for Gateway A 001# and finds in its routing table that Gateway B serves area code 1510.

GK prepends the termination map for Gateway B to the number and routes the call in the following format to Gateway B: 8876#15103459987.

Gateway B strips the prefix 8876# and terminates the call.

**Table 1-3      Gateway Parameters**

H323 Gateway ID	The gateway ID for H.323 protocol communication; may be comprised of alphanumeric symbols.
Gateway Name	The gateway name consists of alphanumeric symbols.
Gateway IP	Specifies the IP address of the gateway.
Gateway Port	Specifies port used for VoIP traffic; typically this is 1720
Gateway Origination Map	Specifies rules used by the VoIP Gatekeeper for phone number transformation, which is the stripping of prefixes from numbers. Gateway Origination Map is relevant when the gateway is used to originate calls. Routing occurs only after the number translation.
Gateway Termination Map	Translation at the termination point, performed only after the origination map is applied and number translation occurs.
Number of Ports	Specifies the equivalent number of T1 (1.54Mbits/sec) ports connected to the Internet. This parameter is applied when load balancing is configured.
Gateway Priority	Specifies a gateway's priority in relation to additional participating devices. The higher the number, the higher the priority.
Gateway Model	Supplied by vendor.
Gateway Description	Specifies additional details as necessary.
Gateway Type	Specifies the type of the gateway.  Private - Private gateways are your gateways. Public - Public gateways are all those your company does not own.
Gateway Protocol	Specifies the protocol that gateway will use to communicate. Available options are: H.323 or SIP
Allow Dynamic IP Address	If a dynamic IP address is used for the gateway, VoiceMaster matches gateway parameters based on H.323 Gateway ID only. The fixed public IP address is negated and the current dynamic address applied.
Radius Routing	Enables Radius Routing..
Radius Failover	Enables Radius Failover module (duplication). In addition radius failover must be specified under System Management > System Information > Radius Failover
Gatekeeper Authorized	Enables the gateway to "talk" to the Gatekeeper on a local level.
Gateway Owner / Provider	Specifies the owner/provider of the gateway. It is imperative that a gateway is associated with a network provider.
Radius Shared Secret	Specifies the shared secret of the radius.

Billing Call Legs (Orig)	<p>Group of parameters relating to either the origination or termination party respectively.</p> <p><b>Billing Telephony:Answer</b></p> <p>This is a telephony termination message (leg) from the termination gateway to the gatekeeper/RADIUS server.</p> <p><b>Billing Telephony:Originate</b></p> <p>This is a telephony termination message (leg) linking origination gateway to gatekeeper/RADIUS server.</p> <p><b>Billing VoIP:Answer</b></p> <p>This is a VoIP termination message (leg) from the termination gateway to the gatekeeper/RADIUS server.</p> <p><b>Billing VoIP:Originate</b></p> <p>This is a VoIP termination message (leg) from the termination gateway to the gatekeeper/RADIUS server.</p> <p><b>Billing VoFR:Answer</b></p> <p>This is a Voice over Frame Relay termination message (leg) spanning termination gateway and gatekeeper/RADIUS server.</p> <p><b>Billing VoFR:Originate</b></p> <p>This is a Voice over Frame Relay termination message (leg) from the termination gateway to the gatekeeper/RADIUS server.</p> <p><b>Billing GK:Originate</b></p> <p>This is a VoIP origination message (leg) for the origination gatekeeper to gatekeeper/RADIUS server link.</p> <p><b>Billing GK:Terminate</b></p> <p>This is a VoIP termination message (leg) from the termination gatekeeper to the gatekeeper/RADIUS server.</p>
Billing Call Legs (Term)	Mirror to Origination Billing Call Legs.
Delta Init Time(sec)	Sspecifies the initial time interval starting when a user establishes a connection.
Delta Init Charge (cents)	Specifies an additional (delta) charge (in US cents) that a user would be charge during the initial time (Init Time) period. This is a custom billing charge that is not affected by changes in provider rates. Can be also set as a percentage of the pre-defined Init Charge.
Delta Sample Rate (cents)	Specifies an additional (delta) charge (in US cents) that a user would be charge on top of the already defined Sample Rate charge. Also independent of provider rate changes and also configurable as a percentage.
Delta Increment (sec)	Specifies the delta rate for the Increment Time in US cents. When the user is connected to the communication network he/she is charged by time units defined by Sample Rate. Upon call termination, the system uses the Increment Time to make rounding of the number of time units used by the user for the call.
Tech Markup (cents)	Specifies additional charge(s) (in US cents) imposed to compensate for your infrastructure costs, etc.
Profit (cents)	Specifies the amount (in US cents) of profit to be earned. Overrides an actual call profit if the latter is less than this amount.
Other (cents)	Specifies additional charge(s) (in US cents) on top of the already defined base rate(s).
Discount (cents)	Specifies discount, used mostly with Reseller clients.
Country	Specifies gateway's country location; enables the imposition of varying charges depending on source of call.

# Gatekeepers

Gatekeepers are essential entities within a VoIP network. A gatekeeper works with multiple providers and destinations to perform intelligent routing within its managed zone while shuttling calls to and from neighboring zones. Gatekeepers can make routing policy decisions based on sets of parameters, enforcing algorithms that seek the best path (for instance, based on speed or cost).

Each gatekeeper has responsibility for a finite number of gateways and endpoints within its *zone*. Gatekeepers can recognize when new devices seek to join the network, then qualify or disqualify them as part of *device registration*. Gatekeepers constantly monitor activity in its zone and forwards calls accordingly. Routing tables and reports, often dynamically updated, provide information about gateway status, load and overall patterns of traffic flow and congestions.

The expanded role of gatekeepers is a function of the proliferation of gateways and endpoints. As devices increase, so do routing demands. As networks grow, gatekeepers can be added to facilitate load-balancing. Typically, endpoints join zones on their own (if their requests are accepted). Such devices are unconcerned with the overall network management structure.

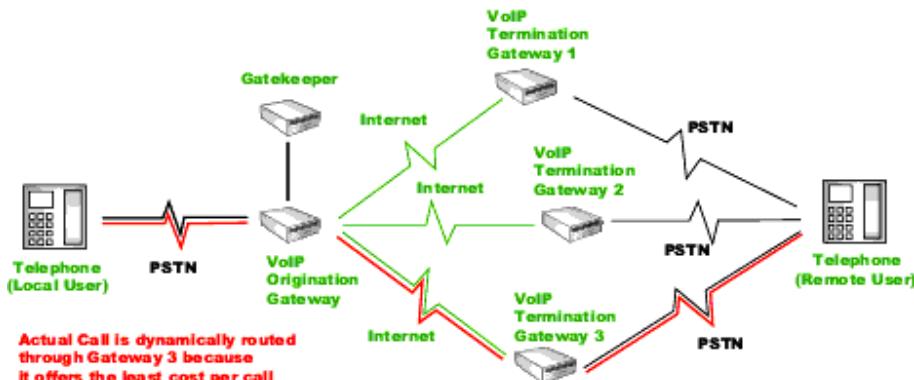
It is the coordinated policy actions of the gatekeeper and administrator that organize this growth intelligently, designing routes to best accommodate the plethora of devices seeking connectivity. Besides adding gatekeepers, a network administrator can also configure a powerful centralized gatekeeper that possesses a registry of different zones and coordinates LRQ-forwarding.

During call setup procedure, the Gatekeeper acts as a management control station. Customer entry of authorization data and country/area code (destination gateway) triggers the routing request. The Gatekeeper is invoked to determine the best path based on standard routing protocols and policies (such as least cost routing).

Several gatekeeper modes exist in VoiceMaster:

- **Static Gatekeeper**

Static gatekeeper supports static call routing tables and simply resolves code area numbers to IP addresses of Termination gateways. With static gatekeepers, all H.323 voice and control flows are passing from both ends participating in the Internet communication (gateway to gateway or PC to gateway). The Static gatekeepers are only used by the gateways upon initial call establishment for initial route resolution. Static gatekeepers do not allow dynamic call routing based on call rates. Changing their routing tables requires manual intervention. Even after the tables are updated, the basic gatekeeper mode is unchanged, though it may process routes more efficiently.



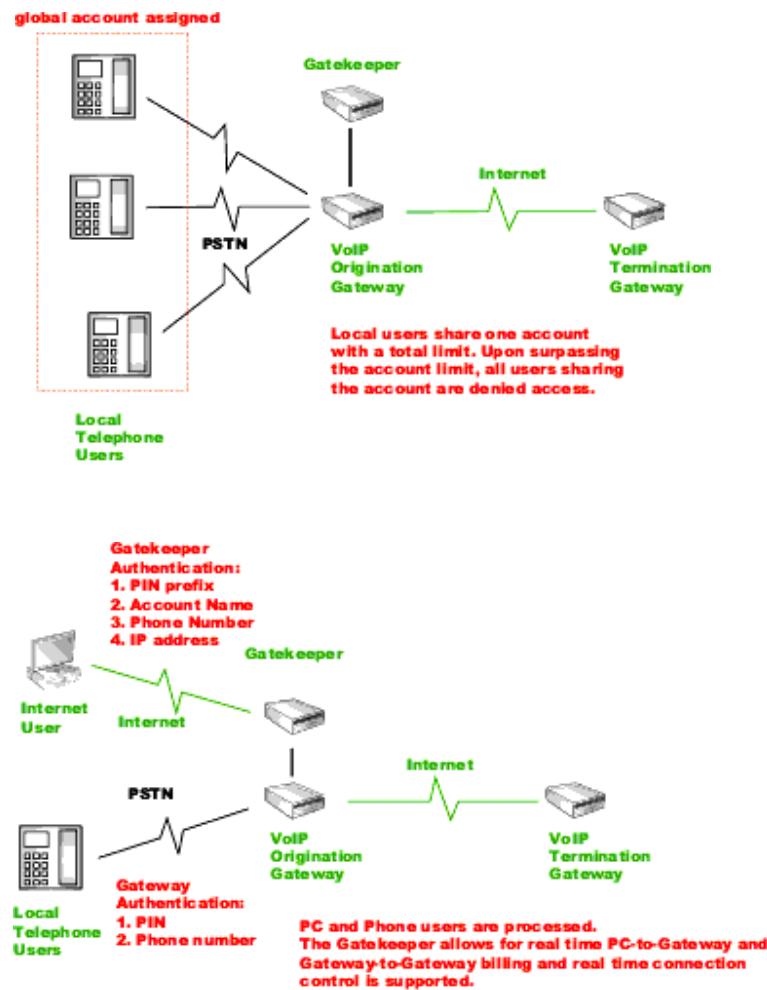


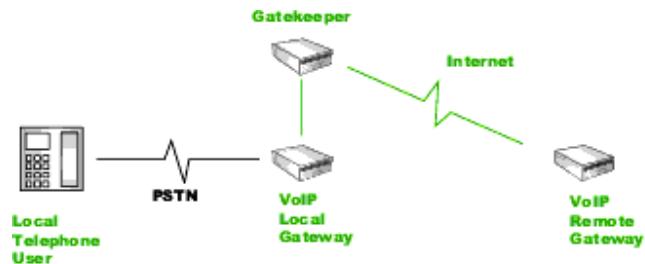
Figure 1-160 Gatekeeper Role in the Network

- **Routed Gatekeeper**

Routed gatekeeper has two major advantages over static gatekeepers.

- A Routed Gatekeeper can dynamically updating its routing tables and provide Optimized Routing services.
- It permits call management in real-time via RAS routing/proxy call services.

Routed mode is based on dynamic routing table adjustments based on current provider rates stored in the VoIP Platform database. The gatekeeper extracts routing information from the VoIP Platform system via a TCP/IP call and prioritizes call routes based on current provider rates. In addition, the Gatekeeper functions as a proxy to exchange system call information (RAS) between gateways in real-time. This lets the gatekeeper terminate calls when specified conditions occur in real time - from balance depletion to call cap adjustments to a reduction in authorized destinations.



**A Gatekeeper can be used as a proxy to a gateway in the case of PSTN originated calls.**



**A Gatekeeper can be used as a proxy where all system and data flows pass through it.**

- **Proxy Gatekeeper**

A proxy gatekeeper acts as a proxy between two communication ends. This facilitates the passing of all traffic based on TCP/UDP/IP through the gatekeeper. This mode is useful when a VoIP provider wants customers to have access to a Termination gateway that can only be reached from certain gatekeepers. In effect, customers using PC-to-phone are masked behind the gatekeeper. Both dynamic charging and call management are permitted in Proxy Gatekeeper mode.

The Gatekeeper provides for the authentication of PC users making PC-to-PC or PC-to-Phone voice calls as well as for VoIP Gateways authentication in Gateway-Gateway communications. It dynamically controls all inbound and outbound calls in routing/proxy mode. Yet call data flow still travels directly from gateway to the gateway.

In addition, the Gatekeeper allows flexible call authentication by one of these means:

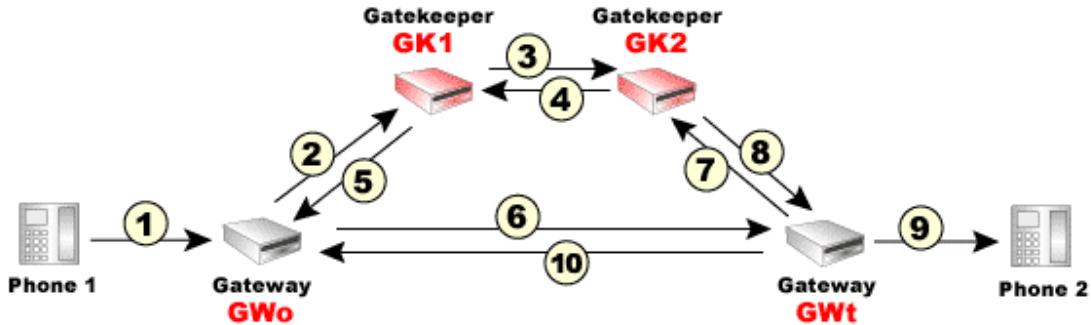
- IP Address
- Call Origination Phone Number
- Call Origination Account Name
- PIN Prefix Recognition

Traditional PIN numbers can be used in this particular call authentication model. There is support for PIN numbers on both Radius/AAA and Gatekeeper levels. This supports full call management capabilities even in environments that lack standard gateways.

Billing based strictly on Radius/AAA permits call origination and call termination only via Radius-compatible gateways. This limits greatly the application flexibility. Such applications can not dynamically process calls to allow PC-to-Phone billing, PC-to-PC billing, and Wholesale Network Billing.

In contrast, Voicemaster allows flexible call billing in all environments. The ability to configure different routing modes greatly enhanced intelligent routing capabilities and real-time adjustments.

## . Gateway to Gatekeeper Call Flow

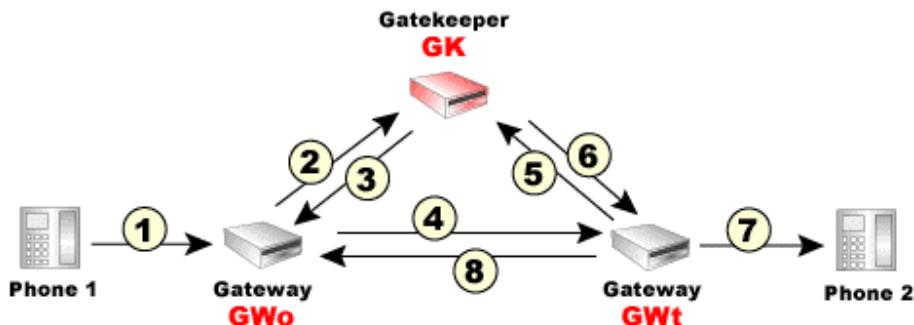


**Figure 1-161Call Flow**

VoiceMaster gatekeeper supports both **Intra-zone** and **Inter-zone** setups for the three modes of work: direct mode, routed mode and proxy mode.

**Intra-zone** setups denote cases when two gateways establish H.323 virtual channel using only one gatekeeper i.e. they share one gatekeeper responsible for their common zone.

### Intra-zone Setup Call Flow



**Figure 1-162Intra-Zone Flow**

In this setup, GK is a VoiceMaster gatekeeper, GWo is an origination gateway managed by GK1. Gwt is a termination gateway. GWo and Gwt can be either Cisco, or Lucent or Quintum gateways.

#### Steps:

- 1 Phone 1 dials the phone number 510-333-7777 for Phone 2, where 1510 is the area code.
- 2 Gateway GWo, an origination gateway, sends gatekeeper GK an ARQ request asking for permission to call Phone 2. In this stage the number that reaches the gatekeeper can be either straight 510-333-7777 or XXX#510-333-7777 where XXX represents a PIN number of the user.
- 3 If a PIN is provided, GK performs the necessary authentication and strips the number from the attached PIN. Next, GK looks up into the origination map entered for GWo (GWo should have an entry in the billing system) and performs the indicated mapping operations on the phone number. GK then takes the processed phone number (in our case that is 925-333-7777) and looks up its routing tables to find a suitable gateway that can put through the call. If there is more than

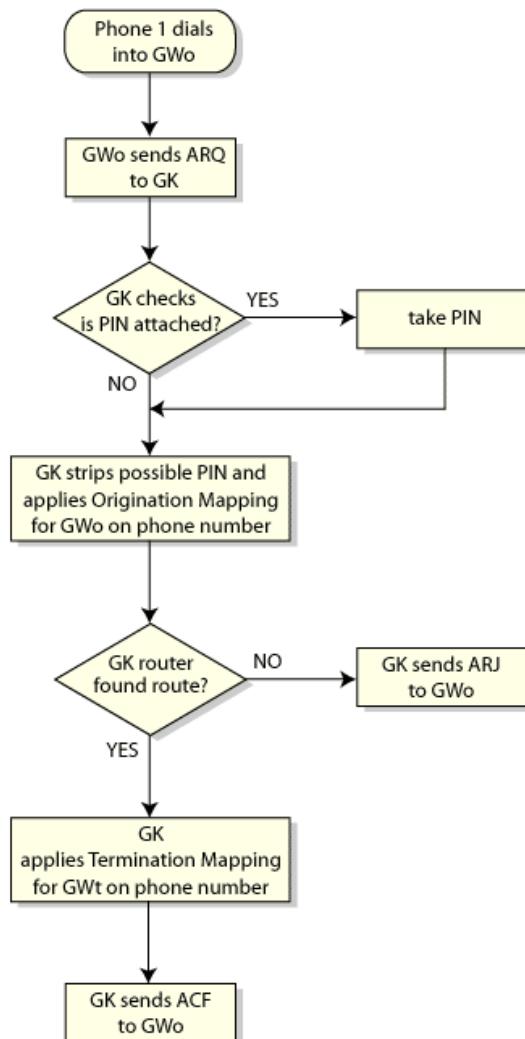
one entry for one area code (i.e. for the 925 area code), GK picks the first matched gateway to place the call (in our case this is G<sub>Wt</sub>). Here G<sub>Wt</sub> is a termination gateway.

G<sub>Wt</sub> should have an entry in the billing system (where it must have an origination and termination map specified) and also it should be registered with GK.

Next, GK looks up into G<sub>Wt</sub> termination map settings and returns an ACF response with the IP address of G<sub>Wt</sub> and also returns the number with the necessary tech prefix attached (e.g. 452#925-333-7777). This tech prefix is necessary so that G<sub>Wo</sub> authenticates itself to the G<sub>Wt</sub>.

- 4 G<sub>Wo</sub> sends a Q.931 Call-Setup request to G<sub>Wt</sub> with the phone number as supplied by the gatekeeper GK (according to the example: 452#925-333-7777).
- 5 G<sub>Wt</sub> sends GK an ARQ, asking permission to answer G<sub>Wo</sub>'s call.
- 6 GK returns an ACF response with the IP address of G<sub>Wo</sub>.
- 7 G<sub>Wt</sub> sets up a POTS call to Phone 2 at 925-333-7777.
- 8 When Phone 2 answers, G<sub>Wt</sub> sends Q.931 Connect to G<sub>Wo</sub>.

The flow chart illustrates the call flow from the above example, steps 1, 2 and 3.



## Inter-zone Setup Call Flow

**Inter-zone** setups denote cases when two or more gateways establish a H.323 virtual channel using two gatekeepers. Each is responsible for its respective zone.

In this setup, GK1 is a VoiceMaster gatekeeper, GWo is an origination gateway managed by GK1. GK2 and GWt can be either VoiceMaster gatekeeper or Cisco, or Lucent, or Quintum gatekeeper and gateway respectively.

### Steps:

- 1 Phone 1 dials the phone number 510-333-7777 for Phone 2, where 1510 is the area code.
- 2 Gateway GWo sends gatekeeper GK1 an ARQ request asking for permission to call Phone 2. GWo is an origination gateway to the gatekeeper GK1. The number that reaches the gatekeeper can be either straight 510-333-7777 or XXX#510-333-7777 where XXX represents a PIN number of the user.
- 3 If a PIN is provided, GK1 performs the necessary authentication and strips the number from the attached PIN. Next, GK1 looks up into the origination map entered for GWo (GWo should have an entry in the billing system) and performs the indicated mapping operations on the phone number.

For instance, the conversion of 510 to 925 can be specified, but this is optional. GK1 then takes the processed phone number (in our case that is 510-333-7777) and looks up into its routing tables to find a suitable gateway/gatekeeper to make the call. GK1 finds that GK2 is responsible for the area code 510 and is a termination gatekeeper. GK2 should have an entry in the billing system as a neighbor gatekeeper (where it must have an origination and termination map specified) and it should be registered with GK1.

Next, GK1 looks up into GK2 termination map settings, performs the necessary transformations and sends LRQ request together with the number and the resulting (if any) tech prefix attached (e.g. 452#510-333-7777). This tech prefix is necessary so that GK1 authenticates itself to GK2.

- 4 GK2 looks up in its routing table and finds that GWt is registered with it and that GWt is responsible for the area code 1510. GK2 returns an LCF response containing the IP address of GWt. GK2 also returns the number + the prefix that should be used. Before this, GK2 should strip all previous prefixes. Thus in this example it will return 274#510-333-7777.

If GK2 was a VoiceMaster gatekeeper it would apply the GK1 Origination Mapping on the phone number. After that, it would perform phone number routing look-up, then GK1 Egress mapping on the phone number. Finally, it would apply GK1 Termination mapping and send LCF to GK1.

- 5 GK1 applies GK2 Egress mapping and returns ACF response with the IP address of the GWt and the phone number with the prefix that GK2 put.
- 6 GWo sends a Q.931 Call-Setup request to GWt with the phone number as supplied by the gatekeeper GK1 (according to the example: 274#510-333-7777).
- 7 GWt sends GK2 an ARQ, asking permission to answer GWo's call.
- 8 GK2 returns an ACF response with the IP address of GWo.
- 9 GWt sets up a POTS call to Phone 2 at 510-333-7777.
- 10 Phone 2 answers and GWt sends Q.931 Connect to GWo.

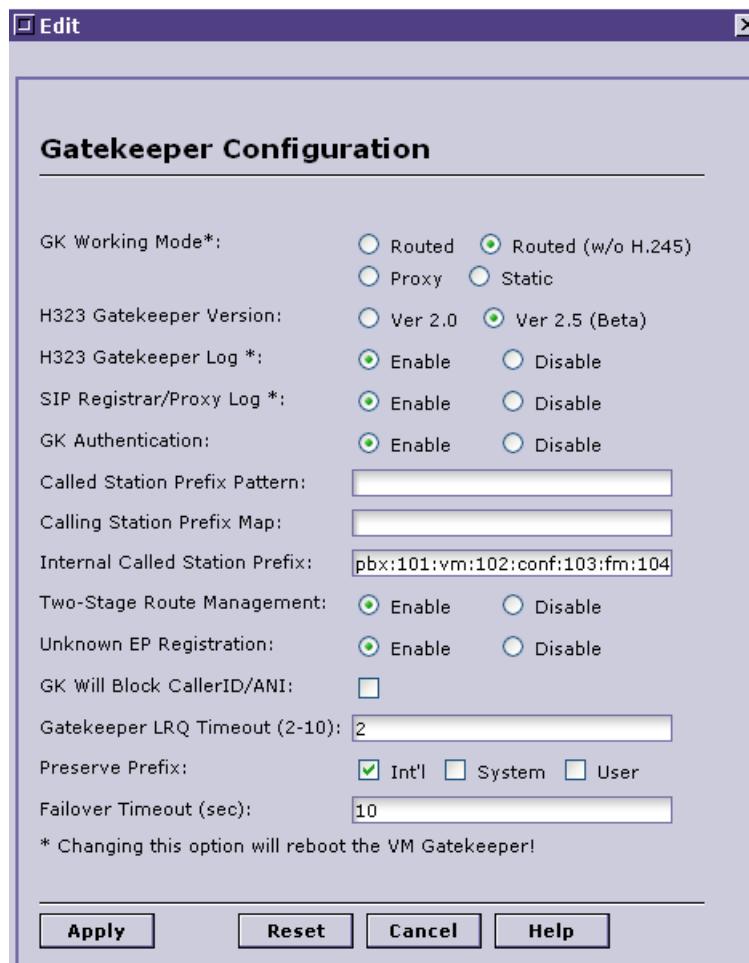
## Configuring Gatekeeper Routing Mode

The Administrator must specify the gatekeeper routing mode in order for VoiceMaster to perform the functions associated with the desired mode (see previous discussion). The routing mode is configurable through this navigation path:

- System Configuration>System Settings>Gatekeeper Configuration>Edit Settings

To configure gatekeeper settings, including routing mode, do the following:

- Step 1** Log in to the Administration Console and open the Navigator.
- Step 2** Select **System Configuration>System Settings**.
- Step 3** Select **Gatekeeper Configuration** from the System Settings list.
- Step 4** Choose **Edit>Edit Settings**. The Gatekeeper Settings dialog is presented.



**Figure 1-163Gatekeeper Settings Dialog**

- Step 5** Set the Gatekeeper Working Mode.

Routed

Routed (w/o H.245)

Proxy  
Static

---

**Note** Changing the current Working Mode restarts the VoiceMaster.

---

- Step 6** Assign the H323 Gatekeeper version.
- Step 7** Enable the H.323 and SIP logs as appropriate. **Note that enabling these options also restarts the system.**
- Step 8** Enable GK Authentication. (required (for authenticating users)).
- Step 9** Enter called and calling map definitions to enable gatekeeper mapping.
- Step 10** Set an Internal Called Station Prefix string if Internal Routing is activated.

---

**Note** See the section on Internal Routing later in this chapter.

---

- Step 11** Enable two-stage route management as desired. See the related section later in the chapter.
- Step 12** Configure the gatekeeper to block caller ID, as desired. (Check the check box.)
- Step 13** Set an LRQ timeout period.
- Step 14** Allow prefix preservation (no stripping) for calls of the designated types.
- Step 15** Set a failover timeout. At the end of the period entered, the system returns from an alternate (failover) route back to the primary route.

### Per-User Gatekeeper Authentication

- Step 1** Select Account Management from the Navigator.
- Step 2** From the right window select the desired user account to configure/modify.
- Step 3** Click on the Account Info button to open the Account Info Page.
- Step 4** At the bottom of the page locate the Authentication Method drop down menu and select the Authentication method. This will be the method the gatekeeper uses to authenticate calls from this account.
- Step 5** Select **Apply** to save changes.

## Routing Tables

Routing Tables contain the information necessary for routing of calls. Each folder within the Routing Tables function contains a set of tables containing information for all possible routes.

To modify any route within a particular routing table:

- Step 1** From the Navigator, select **Route Management>Routing Tables**.
- Step 2** Select the routing table from the Routing Tables window to work with, as in this example (the table is displayed):

Area Code	EndPoint IP	EP Type	Rate (USD/minute)	P
1510		SIP GW	0.1200	11
3592		H323 GW	0.0700	11
3592		H323 GW	0.0700	11
35930		H323 GW	0.0800	11
35930		H323 GW	0.0800	11
35931		H323 GW	0.0800	11
35931		H323 GW	0.0800	11

Figure 1-164 'New Primus' Routing Table

**Step 3** Select any route to modify.

**Step 4** Use the Edit menu options perform any action on the given route (including deletion).

## Configuring Gatekeepers as Endpoints

VoiceMaster has its own gatekeeper functionality. Gatekeepers may also serve as call termination endpoints instead of gateways (refer to [Chapter Four: VoIP Service Configuration](#), for the complete process of building a call network).

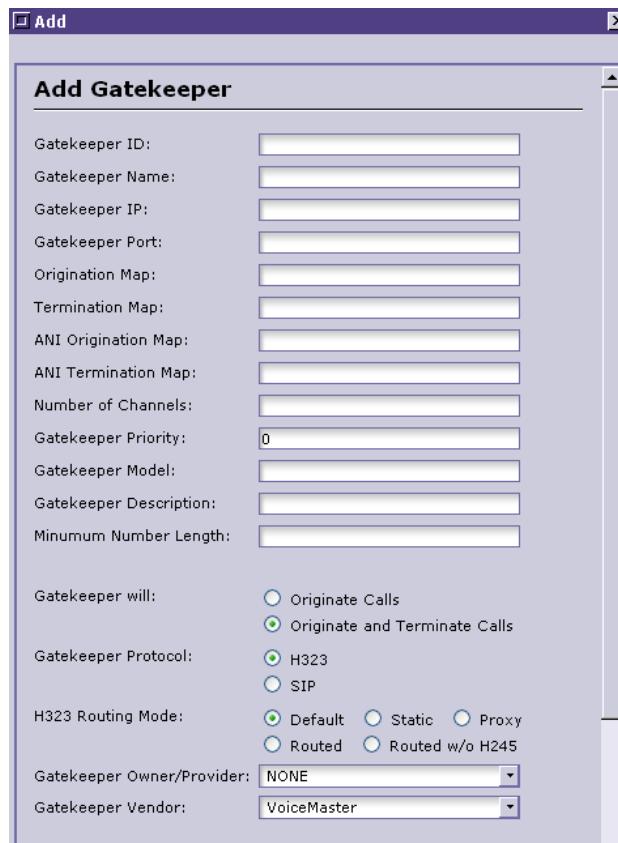
To add a *gatekeeper* as a termination endpoint, follow this procedure:

**Step 1** Select **Route Management>Gatekeepers**. The Navigator reflects your selection:

Eb ID	IP Address	Availability
bC-bC-H353	192.168.1.25	Available

Figure 1-165 Route Management: Gatekeepers List

**Step 2** Choose **Edit>Add Gatekeeper**. The associated dialog is displayed:



**Figure 1-166Add Gatekeeper Dialog (Partial View)**

- Step 3** Enter all relevant field data/parameter settings:
- Gatekeeper ID and name
  - Gatekeeper IP address and VoIP port
  - Origination map definitions, as appropriate
  - Number of channels (“0” is default)
  - Gatekeeper priority (“0”), model and description
  - Minimum number length
  - Gatekeeper role definition:
    - Originates calls; or
    - Originates and terminates calls
  - Gatekeeper protocol (H.323 or SIP)
  - Gatekeeper owner/provider and vendor descriptions (**defining the owner is essential to enable Prefix Routing, the next step in the process.**)
  - Call time adjustments (as desired)
  - Per call adjustments (as desired)
- Step 4** Select **Apply** to save changes and add the provider gatekeeper to the Gatekeepers list.

## Uniswitch

The Unitswitch is the platform that provides H323 Gatekeeper, SIP proxy, and routing related functionalities.

These functionalities can exist as modules on the Voicemaster or they can be a part of a standalone unit (Uniswitch) using the Voicemaster as a Remote Database.

To configure the Uniswitch to use the Database of the Voicemaster, see chapter 2.

The Uniswitch related functionalities and their configuration can be found in chapter 7.

## Special Routing Topics

This section includes some unique VoiceMaster routing topics. They include important functionality that deserves more elaboration and particular configurations/scenarios that an Administrator may encounter.

The set of topics includes:

- **Route Failover.** We expand the discussion of this important fault-tolerant function. Describes the mechanisms and rules for failover activation.
- **Two-Stage Routing.** This feature gets the most of system resources while implementing routing configuration changes in real time.
- **Internal Routing.** Explains how to configure routing when the destination device is registered to VoiceMaster.
- **Virtual IP Addressing.** Assigns proxy IP addresses to a single endpoint as a means of sending multiple prefixes to that endpoint. Overcomes IP addressing restrictions.

### Route Failover

Route Failover functionality provides flexible call routing, activating alternate routes if the current route fails. This is a form of routing redundancy. When route failover is implemented, errors on the primary route trigger failover to the backup route.

The function's value is enhanced further because it effectively cycles between routes:

- The system fails over to the alternate route for a designated, user-configured interval
- It then fails back to the primary route when the interval lapses. (If the primary route is still problematic, the secondary route is again called upon).

The administrator can configure a whole series of RADIUS response (error) codes. If a code is enabled and the event it describes (failure type) occurs, failover is activated.

---

**Note** Two or more termination endpoints must be configured for route failover to work.

---

The codes themselves reflect disconnect causes. (Disconnect is what actually happens in the event of the error *when failover is not configured*. Failover overrides the disconnect.) Errors are divided by device type:

- Gateway errors
- Gatekeeper errors

The Administration Console's Route Failover configuration option further differentiates between SysMaster and non-Sysmaster gateways, creating three code categories.

### Conditions for Activation

In order Route Failover to be triggered the following requirements should be fulfilled:

- The Administrator needs to configure multiple endpoints to a single destination.
- When configuring a (custom) route, the Admin must enable automatic failover (a selectable parameter during route creation).

---

**Note** Failover can be turned on and off for any route in the system.

---

- Some or all gateway/gatekeeper error codes must be enabled at the Route Failover Configuration dialog box (part of System Configuration/System Settings). If an error occurs but is disabled (unchecked), the call will disconnect. (We recommend global code activation).
- The Admin must set a Failover Timeout in order for failover to work properly (fails over, fails back). Timeout settings have global, system-wide effect. This is done at System Configuration/System Settings/Gatekeeper Configuration. As mentioned, the system refers to this setting whenever a route fails, then routes to the alternate for the time indicated. 10 seconds is a standard default for this setting.

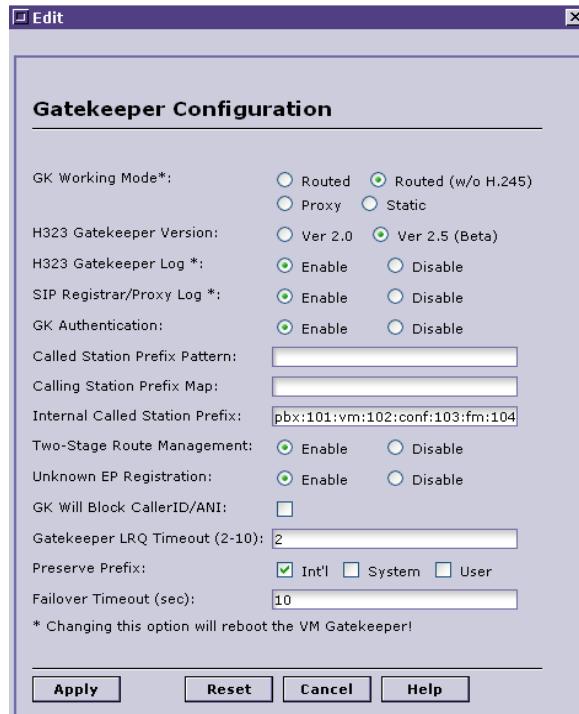
Here is an example of Route Failover in action.

- 1 A customer dials a number in the US. The call is sent to the VoiceMaster gatekeeper for routing and is terminated at Gateway 1.
- 2 Gateway1 fails to terminate the call (unavailable ports, general failure, etc.) and the call is dropped.
- 3 VM detects and logs the failure.
- 4 At the same time additional users dial a number in the US. They are assigned to the VoiceMaster for routing.
- 5 VoiceMaster sees that the route is flagged as 'down' and routes the calls through the alternate termination point used for the same destination area codes. (Alternate endpoints have been configured for the same codes.)
- 6 It employs the alternate route until the timeout expires.
- 7 When the interval ends, VoiceMaster sends the next call again to the primary termination point. According to system rules, it assumes the primary link is again functional. If it is not, failover resumes and calls succeed.

### Route Failover Configuration

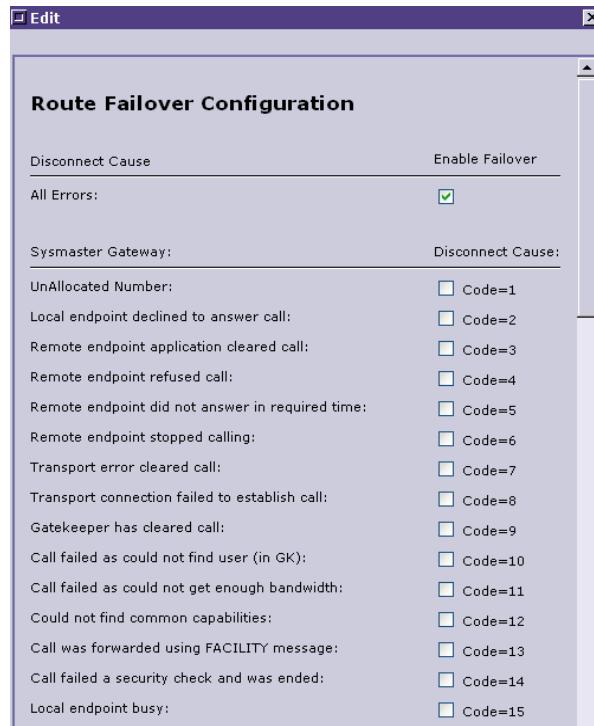
To configure Route Failover:

- Step 1** Log in and open the Navigator.
- Step 2** Select **System Configuration>System Settings**.
- Step 3** Open **Gatekeeper Configuration>Edit Settings**. The dialog appears.



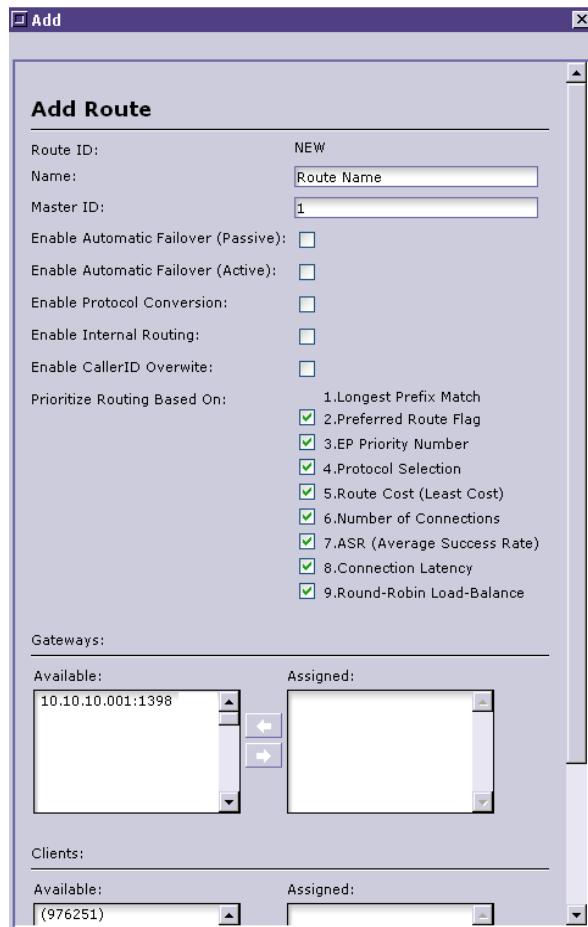
**Figure 1-167Gatekeeper Settings**

- Step 4** In the Failover Timeout edit box enter a failover timeout value. Apply changes.
- Step 5** Still in the System Settings window (no navigation required), select **Route Failover Configuration** and **Edit Settings**. View the Route Failover Configuration dialog:



**Figure 1-168Route Failover Dialog**

- Step 6** Check the “All Errors” box to apply Route Failover to all possible instances of gateway/gatekeeper errors. Alternately, select all errors for a particular category or even individual codes (not recommended).
- Step 7** Select **Apply**.
- Step 8** When creating a new route make sure to enable automatic failover, as shown in this example (the user has checked Enable Automatic Failover). Apply changes.

**Figure 1-169Enabling Automatic Failover for a New Route**

- Step 9** Verify that multiple routes are configured for the specified destination area codes assigned to the route.

We can see how the configuration procedure ties together the conditions for activating Route Failover. Like many other functions, it depends on the implementations of settings both global and specific. The global settings will apply to all instances of a rule; in the case of Route Failover, a rule is enforced on all routes where failover is configured and alternate routes are available.

When error codes are recorded, VoiceMaster activates the first alternate route for the globally configured timeout period. When that period ends, it tries the primary route once again.

## Two-Stage Routing

Two-stage routing is a valuable feature that optimizes system resources while enforcing administrative routing configuration actions. It does this through an update-routing-table mechanism that works in real time, applying the most recent administrator routing changes.

VoiceMaster uses two routing tables by default. These are:

- A production table, analogous to permanent memory in your computer system. This is the table the system calls upon to configure routes. It is a master table.
- A temporary table that saves latest configuration changes while the production table is assisting VoiceMaster in routing calls (remember, call routing is ongoing even as an Admin configures and reconfigures routes and generic routing parameters).

As long as two-stage routing is enabled (we discuss configuring this below), the system will swap the contents of the tables periodically. In effect, a timer is set as a trigger. On activation (this happens automatically), production and temporary tables switch roles. All recent routing ‘edits’ are made permanent, and immediately affect call routing.

---

**Note** If two-stage routing is disabled, the concept of temporary and production tables is discarded. Only one table functions, which means that any configuration changes are made to *it*. This can disrupt call routing, as the routing server within the system is itself called upon to multitask. For this reason, we recommend leaving default two-stage routing as the active mode.

---

In some cases, an Administrator may want to hurry this process along. A new route has been configured or essential changes made to it. At this point, the Admin can ‘sync’ a route, which really means forcing the production-temporary swap on demand. This causes immediate implementation of the latest changes.

---

**Note** The Sync Route option will update the entire routing table, not just the route whose settings you wish to enforce.

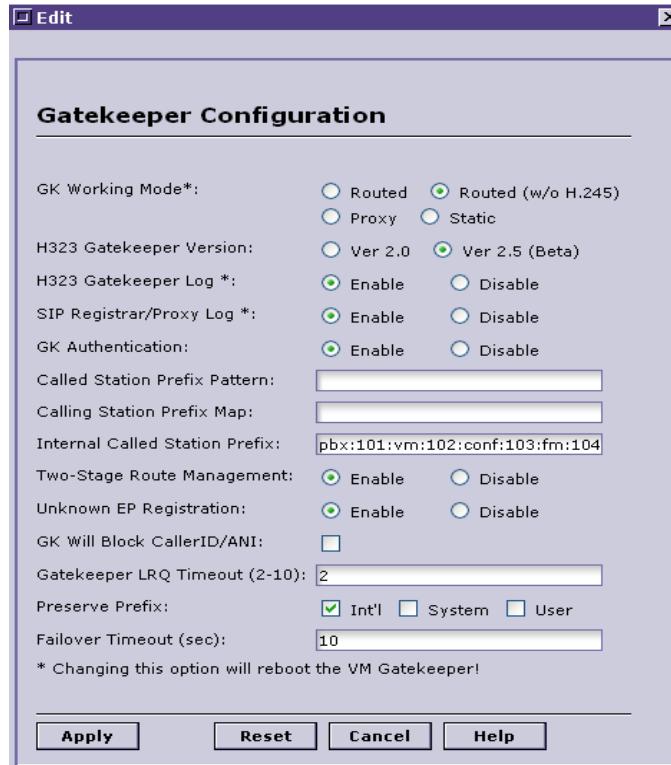
---

### Two-Stage Routing Configuration

To configure two-stage routing:

#### Part 1: Confirming Two-Stage Route Management Activation

- Step 1** Open the Console and Navigator.
- Step 2** Select **System Configuration>System Settings**.
- Step 3** Select **Gatekeeper Configuration** from the **System Settings** window.
- Step 4** Choose **Edit>Edit Settings**. The Gatekeeper Configuration dialog appears:



**Figure 1-170Gatekeeper Settings**

**Step 5** Verify that Two-Stage Route Management ‘Enable’ button is checked. If it is currently disabled, click on the Enable button.

**Step 6** Select the **Apply** button to save this and any other Gatekeeper settings.

## Part II: Table Synchronization

**Step 1** At the Navigator, select Route Management>Routing Tables.

**Step 2** Select the specific table whose routes you wish to edit.

**Step 3** Select a specific route (shown in the following illustration):

Area Code	Endpoint IP	EP Type	Rate (USD/minute)	ProviderID	Preferred	Modified
101		SIP GW	0.0000	1747278	Yes	No
102		SIP GW	0.0000	1747278	Yes	No
103		SIP GW	0.0000	1747278	Yes	No
104		SIP GW	0.0000	1747278	Yes	No

**Figure 1-171Selecting Route for Sync Procedure**

- Step 4** Select Edit>Sync Route.
- Step 5** When the confirmation dialog appears, confirm the synchronization action.
- Step 6** Production and temporary route tables are swapped. All system routing is based on the (new) production table data.

## Internal Routing

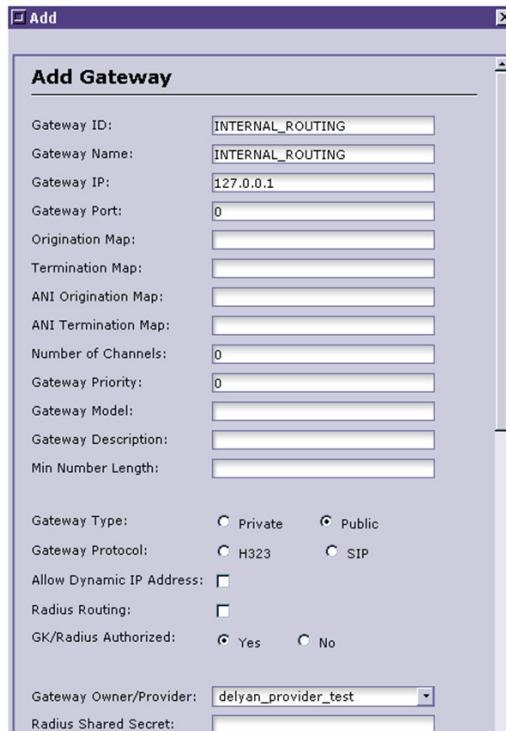
Internal routing is used when you want to route to IP device(s) registered to the VoiceMaster.

Most often users make the mistake of using the VoiceMaster IP address as the terminating endpoint. The correct IP is the loop back address 127.0.0.1

### Creating the Termination Gateway

The first stage in establishing internal routing is to create the termination gateway. We assume that the user has already created provider rates before creating the gateways. To create a termination gateway:

- Step 1** From the Navigator, select **Route Management>Gateways**.
- Step 2** Configure the gateway, using the loopback address (127.0.0.1).
- Step 3** Set the Gateway Type and assign a Gateway/Owner Provider.



**Figure 1-172Gateway Configured for Internal Routing**

### Assign Area Codes

Once the terminating gateway is created, assign area codes:

- Step 1** Select **Route Management > Prefix Routing**.

**Step 2** Locate and select the gateway, as shown:

NIKOTEL	63.214.186.12	Gateway	PRIMUS	0	0	0	-	
GW1T	11.4.3.16	Gateway	GK_Provider	0	0	100	0.00	
Gateway_Term	192.168.0.61	Gateway	DUMMY	0	0	0	-	
gw2	65.113.143.16	Gateway	Primus	0	0	0	-	
OFFICE	67.17.164.16	Gateway	DUMMY	0	0	0	-	
office2	67.17.164.16:1	Gateway	DUMMY	0	0	0	-	
SM2-H323	65.113.143.16:1	Gateway	Local Provider	0	0	0	-	
SM2-SIP	65.113.143.66:1	Gateway	Primus	0	0	0	-	
flush1	22.22.22.22	Gateway	DUMMY	0	0	0	-	
PC_to_PC	127.0.0.1:10	Gateway	DUMMY	0	0	0	-	
PC-PC-H323	127.0.0.1:9	Gateway	DUMMY	0	0	0	-	
111	2.3.4.5	Gateway	DUMMY	0	0	0	-	
dummygw	10.10.10.11	Gateway	DUMMY	0	0	0	-	
testgw423	192.168.0.1:100	Gateway	delyan_provider_test	0	0	0	-	
GW21	65.113.143.66	Gateway	Primus	0	0	0	-	
KUKU	212.50.11.2:1	Gateway	DUMMY	0	0	0	-	
LOLO	1.2.3.4:88	Gateway	DUMMY	0	0	0	-	
WIFI	213.91.247.3	Gateway	DUMMY	0	0	0	-	
Sidespinner	65.112.145.5	Gateway	Sidespinner Inc.	0	0	0	-	
Sandstone	65.112.132.1	Gateway	Sandstone Enterprises	0	0	0	-	
Cargill	212.54.11.34	Gateway	Biff Cargill Enterprises	0	0	0	-	
... INTERNAL_ROUTING	127.0.0.1	Gateway	delyan_provider_test	0	0	0	-	
ciscogk	65.113.143.010	Gatekeeper	Primus	0	0	761350144	0.00	
111222	209.227.165.252	Gatekeeper	DUMMY	0	0	0	-	
HAGK	65.113.143.116	Gatekeeper	DUMMY	0	0	0	-	
HAGKDNW	65.113.143.117	Gatekeeper	DUMMY	n	n	n	-	

**Figure 1-173**Selecting the Gateway at Prefix Routing

**Step 3** Select Edit>Assign Area Codes.

**Step 4** When the Assign Area Codes dialog appears, assign the area codes that the gateway will terminate.

**Step 5** Navigate to **Route Management>Routes** and add the gateway to an existing route or create a new one.

**Note** Customs Routes module is needed to create multiple routing tables in the VoiceMaster.

### My\_test\_Route [10]

▲	Area Code ▼	EndPoint IP	EP Type	Rate (USD/minute)	ProviderID	Preferred
	999	127.0.0.1	SIP GW	0.0000	1123435	No

**Figure 1-174**Internal Routing Configured

**Note** Calls that start with 999 will not be routed from the VoiceMaster. Instead the system will attempt to route such calls to a registered IP device.

### IP Devices

All registered IP devices must have an existing VoiceMaster account in order to be authenticated. The IP devices need to register using a specific number - entered within the user account ANI field. It is this number that will be used to make IP to IP calls and/or to route incoming traffic to a particular IP device.

This illustration of a user account shows an active user whose Caller ID indicates configuration for Internal Routing.

The screenshot shows a Windows-style dialog box titled "Edit Account Information". The form contains numerous fields for account configuration:

Setting	Value
AccountID:	1857356
PIN:	PIN_NUMBER
Username:	UserName
Password:	UserName
User Type:	Active User
Rate Plan:	wholesale 01 [26]
Route Plan:	GK_RouteTable [17]
ISP Rate Plan:	System [0]
Custom Service Plan:	NONE
Signup Plan:	NONE
Caller ID Distribution:	NONE
Content Plan:	NONE
Company:	
Full Name:	
Address:	
City:	
ZIP:	
State:	Non-US/Other
Country:	United States of America
Email:	support@sysmaster.org
Phone:	5328576465
Speed Dial:	
Gateway:	Any Gateway
Caller ID (ANI):	9991234
IP Address:	
Authentication Method:	ANI OR PIN OR USERNAME
Currency:	UNITED STATES OF AMERICA

**Figure 1-175 'Internal Routing' Account**

When another registered IP device dials the specified number located in the ANI field, the VoiceMaster check the routing table associated with the account and routes accordingly.

In this case, it routes the call to the loop back address and makes it an IP to IP call.

## Virtual IP addresses

Virtual IP addresses are used to assign multiple addresses to a single endpoint. This enables the following options:

- Configuration of both H.323 and SIP traffic to a single endpoint. Useful when a single endpoint (gateway) supports both protocols, enabling both kinds of traffic.
- Transmission of multiple prefixes to a single endpoint.

In fact, both functions are related, for a provider may want to ‘read’ multiple prefixes in order to implement multiple-protocol traffic. That is, by receiving multiple prefixes the termination gateway can decipher the *type* of traffic the queuing call represents.

Standard IP address is as follows: 1.2.3.4

A virtual IP would be the same as above, except with the following appended to it at the end: 1.2.3.4:1

---

**Note** The number appended to the end of the IP address can be any number

The VoiceMaster interprets this as a new IP, but will still route to the correct address.

---

EP ID	Gateway Name	Gateway IP
STANDARD_IP	STANDARD_IP	1.2.3.4
VIRTUAL_IP	VIRTUAL_IP	1.2.3.4:1

**Figure 1-176Endpoint Addressing: A Virtual IP Address Configured**

### Routing H.323/SIP to a Single IP

Virtual addressing can be used to route calls in either primary VoIP protocol - H.323 or SIP - to a single termination point (gateway). To do so:

- Step 1** Log in and open the Navigator, as required.
- Step 2** Select **Route Management>Gateways**.
- Step 3** First create an H.323 gateway:
  - (a) Select **Edit>Add Gateway**.
  - (b) When the Add Gateway dialog appears, define gateway settings. Specifically, at the Gateway Protocol option (radio button), enable H323 (it is actually default-enabled).
  - (c) Include a Gateway Owner/Provider.
  - (d) Complete all settings and apply.
- Step 4** Now configure a SIP gateway:
  - (a) Select **Edit>Add Gateway**.
  - (b) Define the gateway parameters.
  - (c) Enable SIP at the Gateway Protocol option
  - (d) At the Gateway Owner/Provider field, **select the same provider as in Step 3 above**.

(e) Apply configuration settings.

The gateways list will show both gateway descriptions as follows, with the same Provider ID for both:

Gateways									
▲	EP ID	Gateway Name	Gateway IP ▾	Type	Priority	Connections	Ports	Master ID	Provider ID
	STANDARD_IP	STANDARD_IP	1.2.3.4	Public H323 GW	0	0	0	-	1123435
	VIRTUAL_IP	VIRTUAL_IP	1.2.3.4:1	Public SIP GW	0	0	0	-	1123435

**Figure 1-177One Termination Point, Two Protocols: Virtual Addressing**

**Step 5** Once the termination gateways are created, select **Route Management>Prefix Routing** and assign all area codes that these gateways will terminate.

**Step 6** Select **Route Management>Routes** and add the newly created gateways to an existing route or create a new one.

---

**Note** Customs Routes module is needed to create multiple routing tables in the VoiceMaster.

---

When the routing table is used, the VoiceMaster will route the H.323 or SIP calls to the same termination end point.

---

**Note** When debugging termination endpoints through the CLI, you see the real IP address in places of the virtual one. By observing the gateway name, you can tell which address is in use.

---

### Configuring Multiple Prefixes to a Single IP Address

Prefixes are used in conjunction with some termination providers. This allows termination providers to identify or authenticate traffic. (Termination mapping in the VoiceMaster does not recognize which protocol is being passed. Using Virtual IP addressing to send multiple prefixes finesse this problem.)

For instance, a termination provider may need H.323 traffic be sent with 1234 appended to the beginning of the number being passed and SIP to be appended with 5678.

You can also use virtual addressing to send multiple prefixes to a single endpoint.

To implement this multiple prefix send functionality:

**Step 1** From the Navigator, select **Route Management>Gateways**.

**Step 2** Select **Edit>Add Gateway**.

**Step 3** Define the gateway. In the Termination Map field, enter a prefix. Apply Changes.

**Step 4** Repeat Step 3 for as many prefixes as you wish to add. Note that the prefix pattern in each new gateway must be unique, reflecting a real pattern.

Here is an illustration of what the Termination Map field should look like during configuration:

**Add**

### Add Gateway

Gateway ID:	<input type="text" value="GATEWAY_ID"/>
Gateway Name:	<input type="text" value="GATEWAY_NAME"/>
Gateway IP:	<input type="text" value="STANDARD_IP"/>
Gateway Port:	<input type="text" value="0"/>
Origination Map:	<input type="text"/>
Termination Map:	<input type="text" value=".=1234;"/>
ANI Origination Map:	<input type="text"/>
ANI Termination Map:	<input type="text"/>
Number of Channels:	<input type="text" value="0"/>
Gateway Priority:	<input type="text" value="0"/>
Gateway Model:	<input type="text"/>
Gateway Description:	<input type="text"/>
Min Number Length:	<input type="text"/>
Gateway Type:	<input type="radio"/> Private <input checked="" type="radio"/> Public
Gateway Protocol:	<input type="radio"/> H323 <input checked="" type="radio"/> SIP
Allow Dynamic IP Address:	<input type="checkbox"/>
Radius Routing:	<input type="checkbox"/>
H323 Routing Mode:	<input checked="" type="radio"/> Default <input type="radio"/> Static <input type="radio"/> Proxy <input type="radio"/> Routed <input type="radio"/> Routed w/o H245
GK/RADIUS Authorized:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Gateway Owner/Provider:	<input type="text" value="NONE"/>
Radius Shared Secret:	<input type="text"/>

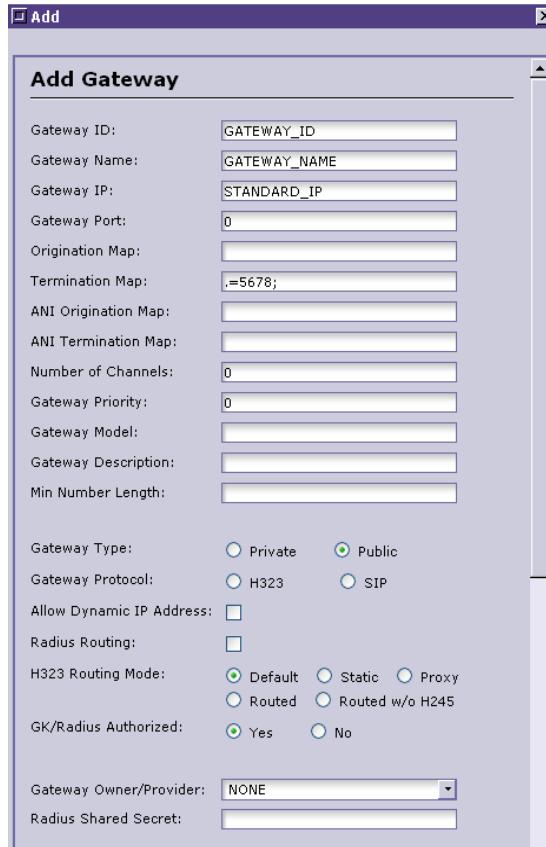
**Figure 1-178Building Prefix Mapping**


---

**Note** The value in “Termination Map” states that all calls will be appended with 1234. So the end result will look like 1234xxxxxxxxxx, where xxxxxxxxxxx is the number being passed. Refer to the “Help” button for more termination mapping values.

---

A second gateway would be defined with a different prefix mapped:



**Figure 1-179 Second Prefix Pattern Mapped**

- Step 5** Once the terminating gateways are created, choose **Route Management>Prefix Routing** and assign all area codes that these gateways will terminate.
- Step 6** Now select **Route Management>Routes** and add the newly created gateways to an existing route or create a new one.

# Chapter 8: Rate Administration

---

## In This Chapter

Rate Administration is split into the following sections and topics:

- Overview
- Rate Administration

## Overview

This chapter covers how VoiceMaster Platform manages rates, how to set-up different types of rates, how to create rate tables and assign rates to them, as well as how to use global rate management and provider billing management functionality.

Rates are the basic unit used by the VoiceMaster Platform for calculating charges imposed on customer calls. A rate reflects charges associated with calls to a termination point within a certain geographical area. It is associated with a specific area code, and defined by expense (provider rates) and charge (billing rate) parameters.

As the previous sentence implies, VoiceMaster Rates divide into two categories:

- Expense Rates
- Revenue Rates

Expense Rates are associated with Providers / ISP Providers. They represent charges/expenses that the Management Company would incur while providing service to its Clients.

---

**Note** The notion of Clients, as used in this documentation, encompasses the following customer entities: Resellers, Wholesalers, and Corporate Clients.

---

Revenue rates refer to the your VoIP call customers. The profit your business earns in a given period can be calculated as:

Aggregate revenue rates minus aggregate expense rates

Rate Management lets you set different rates and use them to populate particular rate plans (tables). The rates then affect assigned customer calls and resulting billing. This of course has a direct impact on your business' revenues and profits, and relates to expenses.

General Rate Management procedures include (though the order may vary):

- 1** Setting Provider Rates
- 2** Creating Billing Rate Plans (Table) and configuring rates for each plan
- 3** Assigning clients/customers to specific plans

The following sections lead you through the procedures that make rate configuration and management (= administration) possible.

## Provider Rates

Provider Rates define a set of parameters describing charges imposed to the Management Company by the Network Provider for the use of its infrastructure.

Provider Rate parameters are:

Call Time Adjustments that include:

- Init Time
- Init Charge
- Sample Interval
- Sample Rate
- Increment Time

Per Call Adjustments that include:

- Call Origination Charge
- Call Termination Charge
- Tech Markup
- Profit
- Other
- Discount

---

**Note** For a complete listing and explanation of Provider Rate parameters please refer to Table 7-1.

---

Provider Rates are a basic type of rates. Even though they contain the basis for calculating charges, VoiceMaster billing system never uses them directly for billing purposes. Instead, it uses the rates defined and contained within a billing rate plan (table).

Provider Rates cost is obtained by the Network Provider itself. Once available provider rates can be added to the billing system:

- Manually
- Via Import

---

**Note** VoiceMaster recommends importing provider rates, when dealing with large amounts of provider rates

---

# Rate Administration

Rate Administration can be seen as any configuration or management action that relates to VoiceMaster rates. Alternatively, you might think of it as the sum of the actions available to manage all aspects of rates (both billing and provider rates).

Adding provider accounts and rates is an essential step in initial VoIP service configuration, as outlined in [Chapter Four: VoIP Service Configuration](#).

Provider Rates will serve as our starting point for discussion of Rate Administration actions because of their centrality in the entire administrative process.

## Provider Rates Administration

In this section, we describe all user actions that relate to Provider Rates administration. We include all the essential procedures required to perform these actions.

---

**Note** Before adding Provider Rates to the system, you must create specific provider accounts, as rates are added per provider. Refer to [Chapter Six: Account Administration](#), for more on creating provider accounts.

---

Provider Rate administration includes these actions:

- Creating the provider account and importing the new provider rates as available. These topics are discussed in [Chapter Six: Account Administration](#) and also in Chapter Four.

---

**Note** We do not specifically discuss creating a Provider Rate Table. Rather, rate table creation is a subset of provider account creation and is explained in context.

---

The remaining actions (described below), include:

- Adding provider pates
- Editing existing rates
- Deleting rates, which may be done per rate or globally
- Copying provider rates
- Binding (clients and customers) to provider Rates (an action that ‘belongs’ to Managed Services scenarios)
- Importing rate tables (from files obtained from the specific provider) and exporting rate tables to a desired target (directory, server, etc.)
- Making rates for specific customers available to view at the (customer-oriented) CRM site or hiding the relevant rates. (CRM Visibility).

---

**Note** Adding and importing Provider Rates are variations of the same basic function. Adding rates is a ‘manual’ procedure by which you define a rate parameter by parameter. Importing provider rates is a global action that imports all rates for a specific provider into his VoiceMaster rate table. Which rate addition path you choose may depend on the number of rates per provider and if they are available in the required spreadsheet format.

---

## Adding Provider Rates

Adding (creating) Provider Rates may be required at different times and in different contexts:

- After creating a new provider account
- Because a specific provider's rates have changed

---

**Note** You may add multiple rates for a single provider. If this is called for, you will need to repeat the following procedure for each individual rate that the provider uses. (Each rate corresponds to a single area code.)

---

Creating a new rate involves setting parameters, mostly different charges (an aspect of your business expenses. Configuration settings include:

**Table 1-4 Provider Rate Parameters**

Provider	The provider name.
Location	The location (geographical region) to which the provider's rates apply.
Area Code	Denotes the location's area code; calls reaching the area code have a base charge equal to the provider's rate. (How much you bill a particular customer is also a reflection of billing rate policies.)
Init Time	Specifies an interval for which the provider rate is calculated per call, starting with call initiation and ending when the number of seconds indicated elapses.
Init Charge	Specifies the base amount (in US cents) charged during the initial time period.
Sample Interval	Sets call billing cycles. Used with Sample Rate, defines a period during which configured rates are charged.
Sample Rate	Specifies the amount (in US cents) that a user would be charged per Sample Interval. (Sample Rate / Sample Interval = per second charge)
Increment Time	The Increment Time value would represent a single time unit that would be used in segmenting the call for billing purposes. For instance: If the Increment Time is specified as 10 sec and a user initiates a call for 31 sec, the call would be segmented into 4 billing time units and charges are calculated as if the call lasted 40 seconds.
Call Origination Charge	Specifies Call Origination Charge, passing on expenses related to call origination.
Call Termination Charge	Defines an expense for call termination for the given rate.

Add provider rates as follows:

- Step 1** With the Navigator view open, select **Rate Management>Provider Rate Tables**. The Rate Management folder is opened, with all current rate tables shown as sub-folders within the Console folder hierarchy:

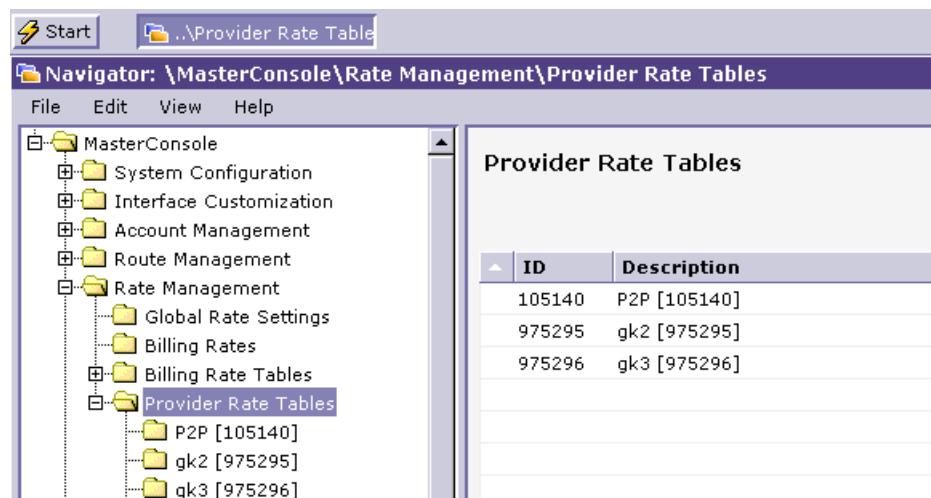


Figure 1-180 Provider Rate Tables Folder Selected

**Note** At this point, the Navigator window still shows all Rate Management options.

- Step 2** Select the folder for the rate table that you wish to manage. The view changes to display that table and its contents:

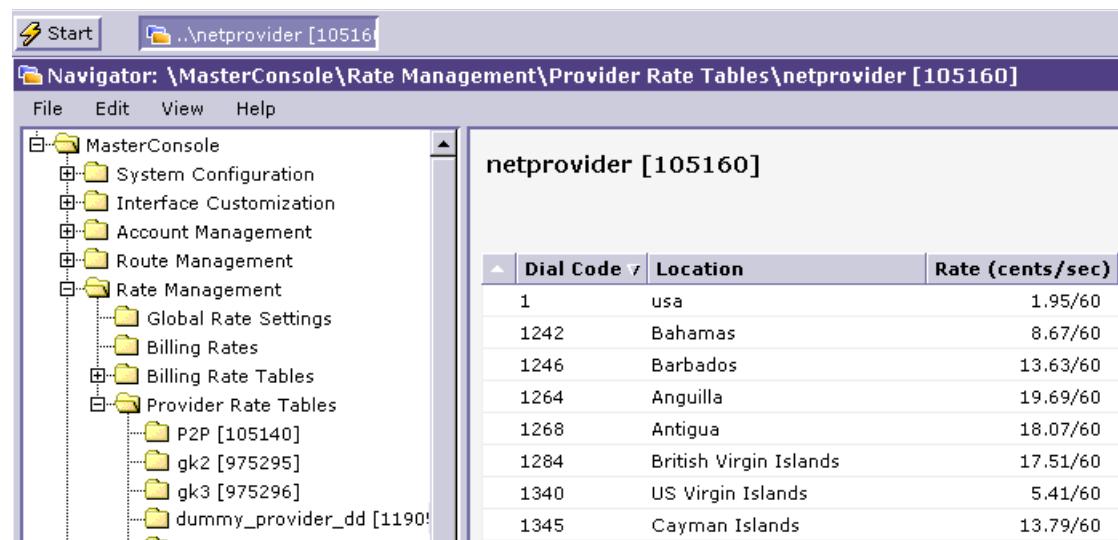
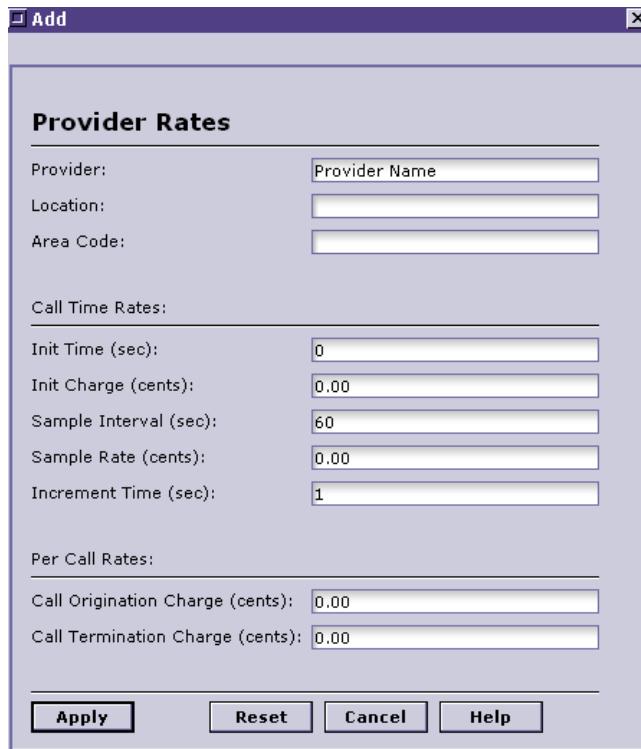


Figure 1-181 Provider Rate Table Ready for Administration

- Step 3** Select **Edit>Add Provider Rate**. The edit dialog is produced:

**Figure 1-182Adding a Rate**

**Step 4** Define each parameter:

- Define the ‘logistical’ fields - provider name, location and area code (to which the rate applies).
- Set Call Time Rates parameters (refer to parameter definitions in Table 8-4).
- Set Per Call Rates parameters (see Table 8-4).

**Step 5** Select **Apply** to save the settings and add the new rate to the Provider Table.

### Importing Provider Rates

Provider rates may also be ‘created’ automatically via the global import of all rates for a given provider. While this method does not involve administrative configuration of any parameters, the end result is the same: a rate (in this multiple rates) is added to the designated provider’s rate table.

The most common scenario for importing rates into the VoiceMaster Platform is when a provider notifies you that he has a list of new rates for route termination (this will be parsed by area code).

The file you receive must correspond to the import format required by the VoiceMaster Platform. The file containing the rates must be in comma delimited Microsoft Excel format.

---

**Note** Should this format not correspond to the Excel format structure, read the section that follows immediately. If the structure **does correspond** to the Excel template, skip to [Import Provider Rates](#).

---

### Creating a Spreadsheet Format for Import

The first step in importing provider rates is to prepare a comma delimited file (CSV). This file format is handled by all popular spreadsheets and is easy to manage.

The following sample is created for MS Excel.

**Step 1** In Excel, open a new spreadsheet.

**Step 2** Enter the following headings in the first row.

Location Code	Init Time	Init Charge	Sample Interval	Charge per interval
Increment Call	Orig Charge	Call Term	Charge	Modified

---

**Note** The imported file can not have any special characters such as periods and commas. That is why the ‘headings’ example is presented as it is.

---

**Step 3** Enter the appropriate values for each column. If no information is available for a particular column leave the rows blank.

**Step 4** Delete the first row containing the heading fields from Step 2.

**Step 5** Select **File>Save As**.

**Step 6** In the **Save as Type**, select **CSV (Comma delimited)**, and click the save button.

**Step 7** Click **Yes** to save the active sheet.

**Step 8** Click **Yes** on the next message screen.

### Import Provider Rates

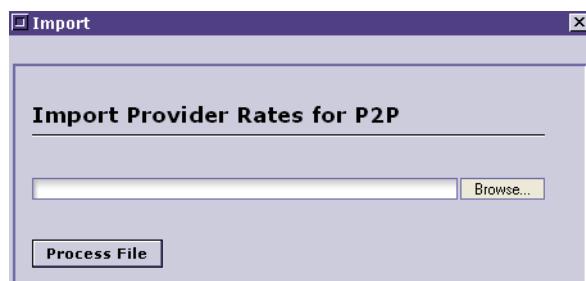
To import provider rates, the ‘automatic’ provider rate configuration option, perform this set of steps:

**Step 1** Locate the spreadsheet sent by the network provider whose account you have now created. Request it now if you have not done so.

**Step 2** Select **Rate Management>Provider Rate Tables**.

**Step 3** Select the folder for the rate table to edit. The window displays the provider rate table (the table will be empty if this is the first time rates are imported, and none have been added manually).

**Step 4** Select **Edit>Import Provider Rates**. The import dialog appears:



**Figure 1-183Import Rates Dialog**

**Step 5** Type in the directory path and file name of the imported provider rate data, if known. Otherwise, select browse and use the Windows Choose File dialog to locate the file.

- Step 6** Find the file to open and load it into the Import Rates dialog.
- Step 7** Select **Process** to import the spreadsheet file into the Provider Rate table. The provider rate entries will populate the provider's rate table.

---

**Note** Provider rates are set *by area code*. If a provider services multiple area codes, then a set of rates for all area codes is imported. (Even in the case that rate parameters are the same for all area codes supported, the system treats each rate individually.)

---

### CLI Import Option

Alternatively, you can import provider rates directly from the command line interface of the VoiceMaster Platform, available over SSH. This is done by executing the `upload_rates.pl` script located in the `/home/manager/scripts` directory.

- Step 1** Start a SSH session and login with username `imanager` and your password.
- Step 2** From the command line type in:  
`cd /home/manager/scripts`
- Step 3** Type in the following command:  
`upload_prov_rates.pl <FNAME> <RATE_ID> <DB_PASSWORD>`

, where

`<FNAME>` is the name of the file that you want to import  
`<RATE_ID>` is the ID of the provider that rates will be imported for  
`<DB_PASSWORD>` is the password for the “manager” DB.

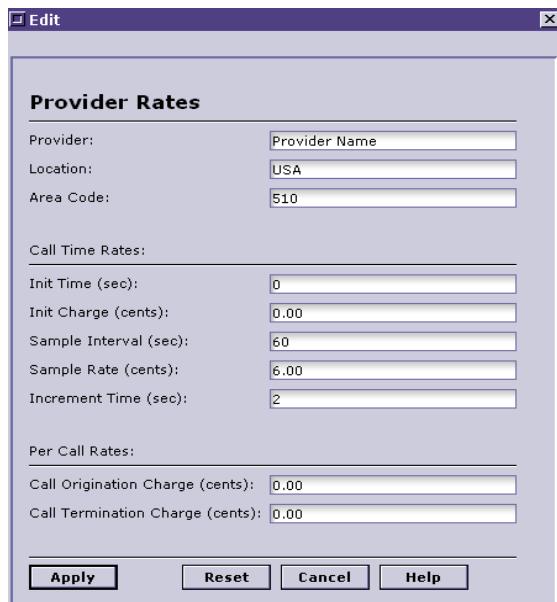
### Editing Provider Rates

Editing provider rates is a matter of selecting the rate table where a ‘target’ rate resides, then selecting the rate and modifying it through the associated dialog box.

The reasons for editing a specific rate or set of rates are fairly clear: a provider has changed specific rates and informed your VoIP service of this modification. Alternatively, you may want to review a set of rates and find errors that call for correction.

To edit existing provider rates.

- Step 1** At the Navigator view, select **Rate Management>Provider Rate Tables**.
- Step 2** Select the folder for the target provider rate table.
- Step 3** Scan the table, and locate and select the rate to modify.
- Step 4** Select **Edit>Edit Provider Rate** to work with the dialog:



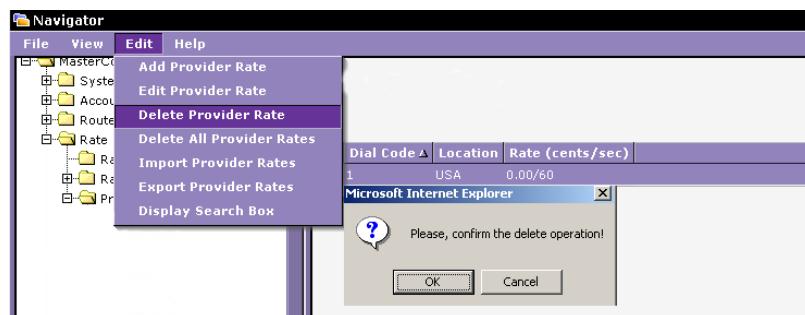
**Figure 1-184**Editing Provider Rates

- Step 5** Change any settings, from provider name and location to rate area code and the two kinds of available charges (expenses).
- Step 6** Select **Apply** to save modifications.

### Deleting Provider Rates

To delete a provider rate:

- Step 1** At the Navigator view, select **Rate Management>Provider Rate Tables**.
- Step 2** Select the folder for the provider whose rate(s) you intend to remove.
- Step 3** Scan the table, and locate and select the rate to delete.
- Step 4** Select **Edit>Delete Provider Rate**.
- Step 5** When the confirmation dialog appears, select **OK** to delete it.



**Figure 1-185Deleting a Provider Rate**

Another delete option deletes *all* rates within a table at once. To do so:

- Step 1** At the Navigator view, select **Rate Management>Provider Rate Tables**.
- Step 2** Select the folder for the provider whose rates you want to remove.
- Step 3** Choose **Edit>Delete All Provider Rates**.
- Step 4** The Windows confirmation prompt is once again displayed. **Before you confirm it, be sure of this choice.**

---

**Note** Deleting all rates within a specific provider rate table is appropriate in cases where a provider has sent a revised set of rates. If this revision is comprehensive, it makes sense to 1) delete all current rates for his table, 2) import the revised rates (see the section on importing rates).

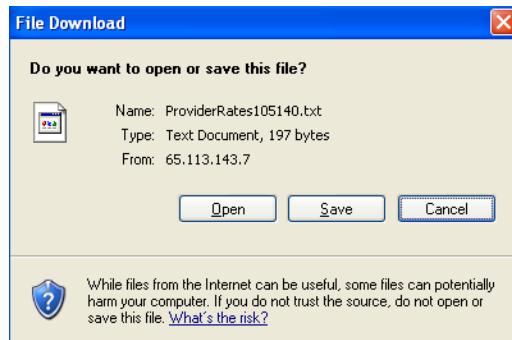
---

## Export Provider Rates

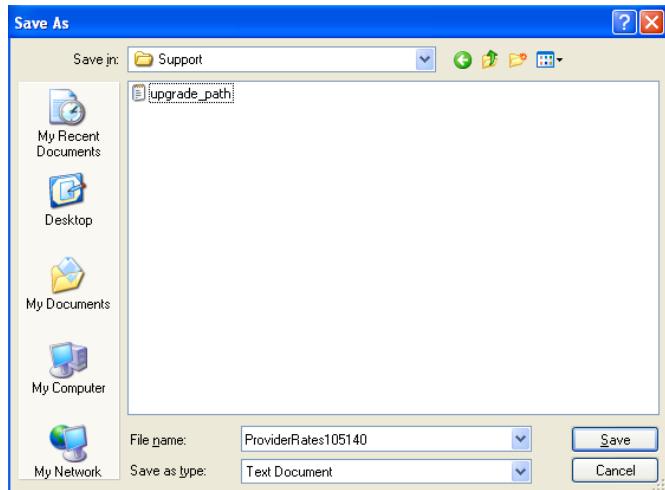
Exporting Provider Rates is a simple process of transferring all rates belonging to a provider to a specified destination. Rates are exported in .txt format with a file name in the form <ProviderRate[ID]> where, [ID] is the identification number of the network provider.

Export provider rates as follows:

- Step 1** From the Navigator, select **Rate Management>Provider Rate Tables**.
- Step 2** Select the desired provider folder.
- Step 3** Select the rate to export.
- Step 4** Open **Edit>Export Provider Rates**. The File Download dialog box will appear:

**Figure 1-186Exporting Rates (Windows File Download)**

- Step 5** Click Save and choose the location the file to be saved to:



**Figure 1-187Export Target Directory**

**Step 6** Save the download/export.

## Billing Rates Administration

Billing rates are the mechanism used to impose actual charges on customers for placing calls over the VoIP network managed by VoiceMaster and the human administrator. While provider rates are the basis for calculating system expense and a guide to setting billing rates (a sort of revenue calculation platform), billing rates are the actual determinants of customer rate plans.

Provider rates are a base for figuring customer rate charges, but VoiceMaster's flexibility gives the Administrator full control of these end user rates. They are set according to billing policies, and can be configured with variety in accordance with customer types, calling habits and preferences.

Moreover, billing rate plans should reflect your overall business model and strategy. Think of them as the most practical, tangible tools for enhancing revenue strategically. The idea is to create consistent revenue and profit while satisfying and expanding the customer base.

---

**Note** Customizing rates and rate plans is facilitated by the implementation of VoiceMaster Custom Modules.

---

Note that the rates customers are charged are typically a combination of (base) provider rates to a particular destination and the adjustments for customers set using procedures in this section.

Building customer rate plans involves

- Creating a Rate Plan. This involves two steps:
  - Creating a Rate Table that will house the individual rates that will apply to the plan (together, all rates to different area codes are the plan's contents)
  - Assigning client/customers to this plan
- Defining the individual rates that form the plan, i.e., building the rate table contents.

Typically, configuring a plan means adjusting provider rates by adding charges to each customer. This is what builds profits from the Revenue-minus-expense calculus. You can do this manually, by adding a rate plan (see next section).

Apply specific provider rates to particular customers by copying provider rates to a billing rate table. You may also bind specific clients to specific providers, which fits a Managed Services scenario in which an agent uses the VoiceMaster infrastructure to service his own customers. (In this scenario, binding or copying rates to an agent's passes on network provider costs to the agent.)

---

**Note** VoiceMaster provides a default Rate Plan – System[0] and the ability to create unlimited number of rate plans. VoiceMaster recommends that the default System[0] rate plan contains only rates that the end users would be charged.

Rates imposed on all customers are called Fixed Rates. Fixed Rates are “dummy” charges and they are associated with “dummy” providers, used mostly in Managed Services scenarios.

---

The following sections lead you through the critical steps within Rate Administration.

## Create Rate Plans (Tables)

Before you can create (add) a Rate Plan, you must do the following:

- Create Client (Reseller, Wholesaler, Corporate Client) accounts
- Establish which clients will be assigned to the rate plan created here.

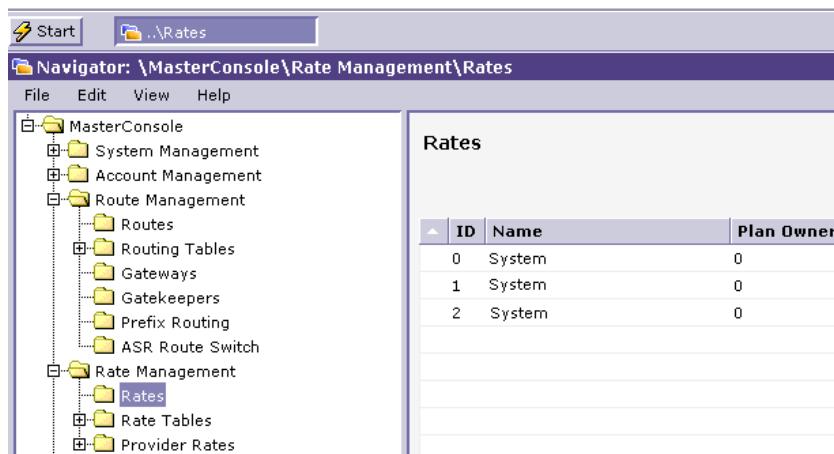
When you create new rate plans, you define or configure just a few parameters:

**Table 1-5      Rate Plan Parameters**

Name	Specifies the name of the rate table to be created
Master ID	The Master ID of a rate table is relevant to the Managed Services Module. Sets up limited agent access to the Administration Console (while you ‘master’ administer the system). Apply a Master ID that is identical to the reseller/agent’s account ID. If the plan is not relevant to Managed Services, no Master ID is entered. Leave the default value of 0.
Clients: Available / Assigned	Assigns clients to a rate table. Only one rate table is associated with any client, so that assigning a client to a table deletes it from any previous rate tables to which it ‘belonged.’

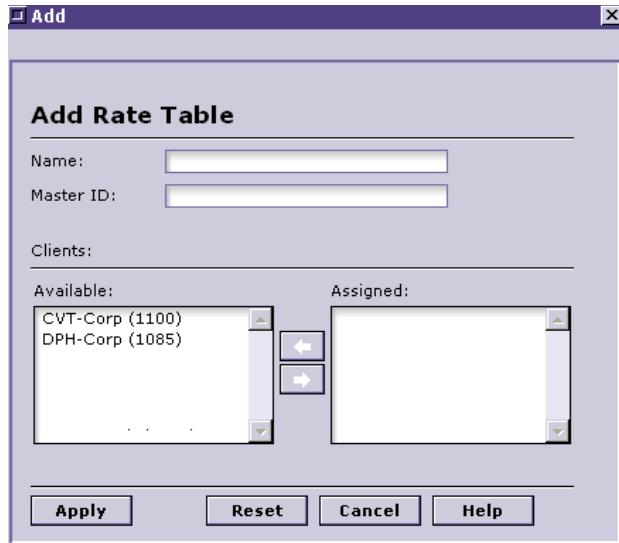
To add a rate plan:

**Step 1** At the Navigator, Select **Rate Management>Billing Rates**. The view changes to:



**Figure 1-188 Billing Rates**

**Step 2** Select **Edit>Add Rate Table**:



**Figure 1-189Add Rate Table Dialog**

- Step 3** Name the table, preferably choosing a name that you can associate with the provider and/or assigned clients.
- Step 4** If the implementation is Managed Services, assign a Master ID that is identical to that of the agent (reseller/wholesaler) who will manage the plan's rates. Otherwise, enter '0'.
- Step 5** Assign clients to the rate table (plan) by moving them, one by one, from the Available to Assigned boxes.
- Step 6** Select **Apply** to save changes and create the new rate table.

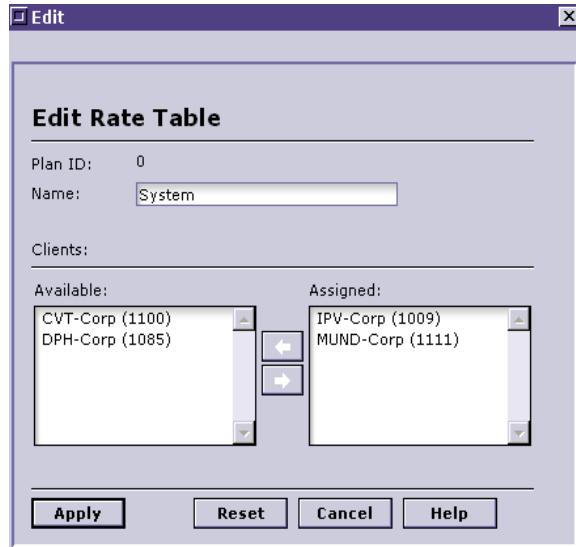
### Editing Rate Plans

Modifying a rate plan involves changing any parameter within the plan. Most likely, this will involve the assignment and removal of clients to and from the plan.

To edit an existing plan:

Edit rate plans as follows:

- Step 1** At the Navigator, Select **Rate Management>Billing Rates**.
- Step 2** From the Billing Rates window, select a plan to edit (highlight it).
- Step 3** Select **Edit>Edit Rate Table** and view this dialog:



**Figure 1-190Edit a Rate Table**

**Step 4** Modify the data fields. Assign or remove clients.

**Step 5** Click **Apply** when finished. Changes are saved.

### Deleting Rate Plans

To delete a rate plan:

**Step 1** At the Navigator, Select **Rate Management>Billing Rates**.

**Step 1** From the Billing Rates window, select a plan to delete (highlight it).

**Step 2** Open the Edit menu and select **Delete Rate Table**.

**Step 3** The confirmation prompt appears. Click **OK** to delete rate plan

## Configuring Billing Rates

A billing rate plan is not complete until individual rates are created that will apply to assigned clients and customers. That is, individual rates are set for different area codes based on different charges.

This section includes procedures not just for creating new rates per plan/table, but also modifying and deleting rates.

### Add (Individual) Rates

The first and natural step in administering the rates themselves that make up a plan is to add individual rates to the selected rate table. To do so, just follow these easy instructions:

**Step 1** At the Navigator view, select **Rate Management>Billing Rate Tables**.

**Step 2** Select the folder for the rate table you will create rates for (if the plan does not exist, return to the previous section and add it). The window changes to the Rate Table view:

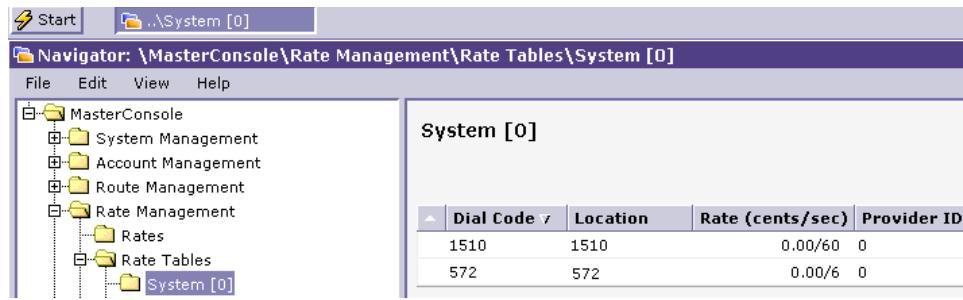


Figure 1-191A Billing Rate Table Selected

**Step 3** Choose **Edit>Add Rate** and the rate creation pops into view:

The 'Add' dialog box is titled 'Rate Definition'. It contains several sections:

- Area Code:** [Text Box]
- Location:** [Text Box]
- Call Time Adjustments:**
  - Init Time (sec): [Text Box] 0
  - Init Charge (cents): [Text Box] 0.00  %
  - Sample Interval (sec): [Text Box] 60
  - Sample Rate (cents): [Text Box] 0.00  %
  - Increment Time (sec): [Text Box] 1
- Per Call Adjustments:**
  - Call Origination Charge (cents): [Text Box] 0.00
  - Call Termination Charge (cents): [Text Box] 0.00
  - Tech Markup (cents): [Text Box] 0.00
  - Profit (cents): [Text Box] 0.00
  - Other (cents): [Text Box] 0.00
  - Discount (cents): [Text Box] 0.00
- CRM Visible:**  Yes  No

At the bottom are buttons: **Apply**, **Reset**, **Cancel**, and **Help**.

Figure 1-192Adding a Rate

- Step 4** Set the area code for the rate. This is the key identifier/factor around which a rate is built.
- Step 5** Set the location.
- Step 6** Set Call Time Adjustments.
- Step 7** Define Per Call Adjustments.
- Step 8** Enable CRM visibility as desired.
- Step 9** Set **Apply** to save the new rate and add it to the table list.

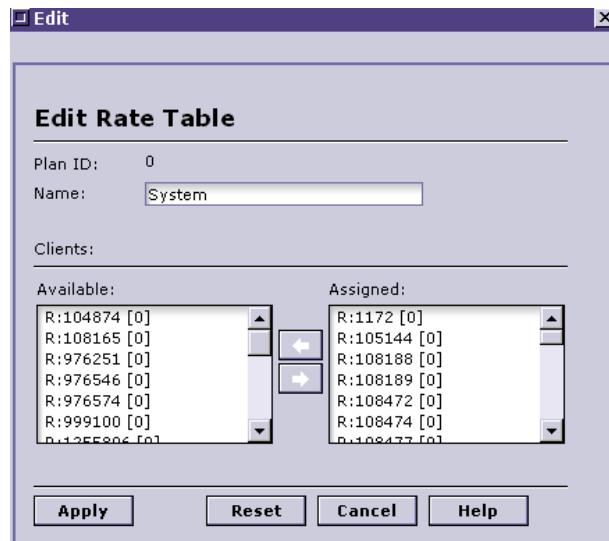
### Edit Rates

To edit an existing rate:

- Step 1** At the Navigator view, select **Rate Management>Billing Rate Tables**.

**Step 2** Select the plan/table whose rate(s) you intend to edit.

**Step 3** Select a rate from the Billing Table to edit, and the Edit dialog appears:



**Figure 1-193**Editing a Rate Definitions

**Step 4** Change any desired parameter, editing entry boxes or buttons. **Selecting a specific provider applies that provider's rates as the basis for billing rates.**

**Step 5** Select **Apply** to save changes.

### Delete Rates

Deleting rates from a plan is simple enough:

**Step 1** At the Navigator view, select **Rate Management>Billing Rate Tables**.

**Step 2** Select the plan/table whose rate(s) you intend to delete.

**Step 3** Select a rate from the Billing Table to delete.

**Step 4** Now choose **Edit>Delete Rate**.

**Step 5** The confirmation prompt appears. Click **OK** to confirm; the rate is deleted.

### Copy Rates from Provider

This is the first of a set of generic or ‘global’ actions that affect the entire selected billing rate table.

When you copy rates from a provider, in effect you are overwriting existing rates within the table and replacing them with the selected provider rates (that you import here). The reasons for this include special scenarios like Managed Services.

System Administrators can copy rates from one or more providers to a single rate table. This is only possible when no provider binding has been previously performed. (see the next section, guys)...

---

**Note** We recommend that rates from different providers are not contained within a single rate table. Instead system administrators should create separate tables for each provider rates that need be accommodated.

---

Binding is dynamic. You can copy from multiple providers but only area codes and rates that are not present will be copied. Duplicate rates never appear.

To copy a provider’s rates into a plan (table) and use them to apply to plan-associated customers:

- Step 1** At the Navigator view, select **Rate Management>Billing Rate Tables**.
- Step 2** Select the table (plan) whose current rates you wish to replace with the select provider.
- Step 3** Open the Edit menu and choose **Copy Rates from Provider**. The needed dialog displays:



**Figure 1-194Copy Rates Dialog**

- Step 4** Select the pulldown menu and choose a provider as an import source.
- Step 5** Select **Apply** to enforce the change.

---

**Note** All imported files must be formatted according to the Excel standards, as discussed earlier.

---

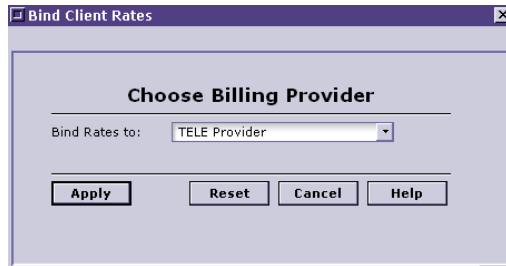
### Bind to Provider Rates

This option, specifically for a Managed Services scenario, hard-codes rates for a plan’s customers to a specific provider. This is a quick and easy means of passing on the provider costs (to you) to the agent (reseller, etc.) who makes use of your infrastructure - including the provider’s network - to facilitate service to his customers.

Once bound, all rates for the customer will change if and when the provider rates do.

To bind all clients tied to a plan to a provider's rates:

- Step 1** At the Navigator view, select **Rate Management>Billing Rate Tables**.
- Step 2** Select the table (plan) whose current rates you wish to bind to the provider.
- Step 3** Select **Edit>Bind to Provider Rates**. The 'bind' dialog appears:



**Figure 1-195Binding Plan Clients to a Provider**

- Step 4** Select the pulldown menu and choose a provider from the list.
- Step 5** Choose **Apply** to finish and create the binding.

### Export Rate Table

Exporting a rate table to a specific destination may be useful to store it (save it), or send it to another VoiceMaster Administrator for use (etc.).

To export a rate table, follow these steps:

- Step 1** At the Navigator view, select **Rate Management>Billing Rate Tables**.
- Step 2** Select the table to export.
- Step 3** Select **Edit>Export Rate Table**. The Windows export dialog is shown:



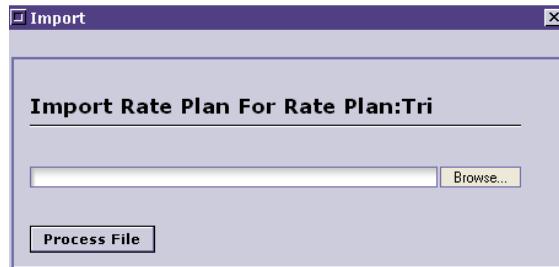
**Figure 1-196File Download Dialog: Exporting a Table**

- Step 4** Select **Save** to export it to a directory.
- Step 5** Choose a 'Save As' location at the next window. The rate table is exported

### Import Rate Table

To import a table from a specified source, thus applying its individual rates to the selected table:

- Step 1** At the Navigator view, select **Rate Management>Billing Rate Tables**.
- Step 2** Select the table whose current contents (rates) you want to override with the desired table.
- Step 3** Select **Edit>Import Rate Table**.
- Step 4** A special dialog is displayed:



**Figure 1-197 Importing a Rate Plan**

- Step 5** Enter the directory and file name, if known. Otherwise, select Browse and locate the Import Rate file in your directories.
- Step 6** Select **Process File**.
- Step 7** The file and rate plan are imported.

# Chapter 9: Batch Administration

---

## In This Chapter

Batch Administration is divided into these sections, or topics:

- Overview
- Global Batch Administration
- Reseller Batch Administration
- Corporate Client Batch Administration

## Overview

VoiceMaster provides flexible and robust support for VoIP service providers who generate and distribute calling cards for international and long-distance call access. To simplify the process of creating and distributing these calling cards, VoiceMaster organizes them into batches.

Each batch is associated with a single pre-established reseller or corporate client account. The Administrator identifies each batch, which then generates a group of PINs (personal identification numbers).

---

**Note** Batches are really custom subscription plan assignments, or the configuration of such custom plans to selected users.

---

Each card has a unique PIN that the reseller or corporate client distributes according to his own administrative needs. In addition to the PIN, cards are distinguished by the face value (call amount limit) and account numbers.

Reseller and corporate administrators can distribute the cards by a selected delivery system. They can sell cards to retail customers (in person) or through web sites. Corporate clients might hand out cards to employees.

VoiceMaster's batch administration functions are designed to facilitate the configuration and management of batches of different types. Complete control of the various defining parameters is in the Administrator's capable hands.

---

**Note** There are different batch types in VoiceMaster. For instance, VoIP Booth is used for call shops, or Internet kiosk arrangements.

---

# Configuring Global Batch Settings

Global Batch Management facilitates custom parameter configuration for target batches. SysMaster assumes that certain batches require unique handling, and so offers the administrator the chance to define them uniquely. Many of the parameters will have been configured previously, while some are unique to batch management.

**Note** The ‘global’ parameters are thus applicable to the batches for which they are defined, and will not affect settings for the parent client account itself. Those global settings will remain.

Global Batch Settings are visible when you open the edit dialog. We will describe individual parameters per procedural step.

To configure Global Batch settings, follow this procedure:

- Step 1** At the Navigator view, select **Batch Management** from the folder hierarchy.
- Step 2** Select **Global Batch Settings**.
- Step 3** From the Edit menu, select **Edit Settings**. The Global Batch Management dialog is displayed:

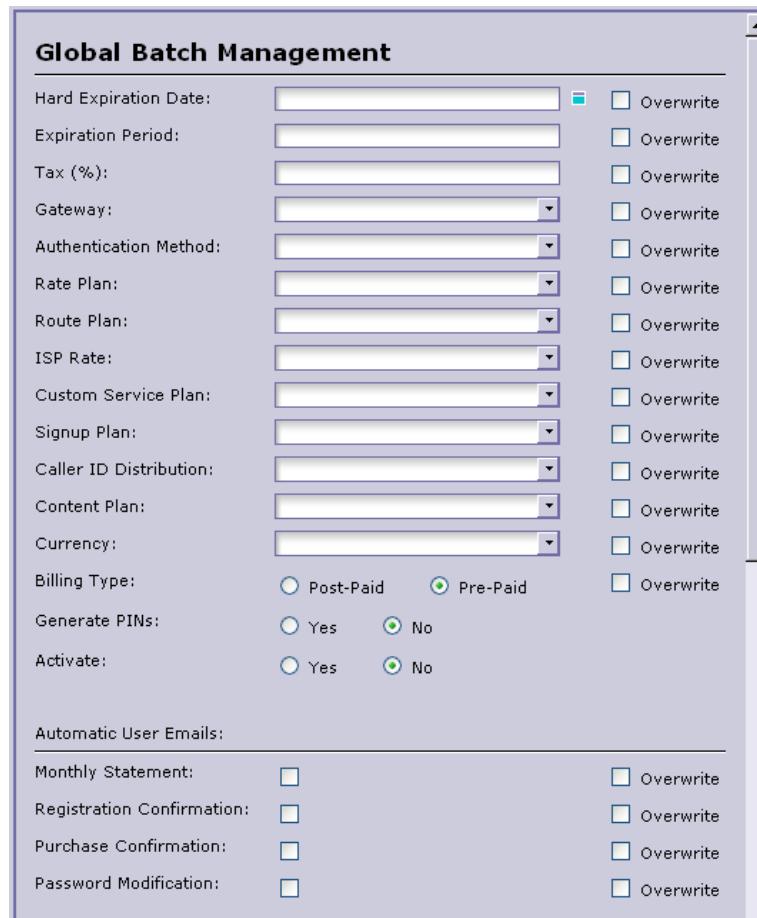


Figure 1-198Configuring Global (Custom) Batch Settings

- Step 4** Configure each setting required, and those optional settings you wish to enforce for the batches selected:
- (a) Hard Expiration Date sets an end date at which batch accounts will expire.
  - (b) Expiration period sets a number of days to trigger account disabling for affected accounts.
  - (c) Tax percentage sets a flat tax on accounts within the selected batches.
  - (d) ISP rate. This is relevant if you are working with an ISP Billing implementation and want to set global rates for batches of ISP customers.
  - (e) Generate PINs activates PIN generation for the relevant batches.
  - (f) Activate PINs gives account holders permission to start calling using their assigned PINs.
  - (g) Rate Plan lets you assign a specific rate plan for the affected batches.
  - (h) Route Plan does the same thing vis-a-vis routes.
  - (i) Custom Service Plan assigns a custom plan (modifies the rate plan).
  - (j) Authentication Type controls what authentication method is used to authorize calls from the batches' associated customers.
  - (k) Currency configures the currency to be associated with the associated accounts.
  - (l) Gateway is used to assign a specific gateway (or all gateways) to be used for calls from the batch accounts.
  - (m) Account Type sets the type as pre-paid or post-paid.
  - (n) Automatic user email fields set passing of the selected message types to the account holders.
  - (o) Options management lets you permit (or deny) multiple calls per customer, enable short (account) statements, and set up credit card payments (as desired).
  - (p) The two DID Management options configure direct dialing parameters.
  - (q) Finally, Apply to Batches is the means by which you assign specified batches to be governed by the preceding global settings.
- Step 5** Select **Apply** to apply the settings configured and save them.

---

**Note** The Overwrite check box must be selected for any parameter configured to have it overwrite the previous setting. So, each parameter must be applied individually, then again collectively in Step 5.

---

## Reseller Batch Administration

The purpose of Reseller Batch functionality is to facilitate a mechanism for authenticating reseller customers when placing calls. The PIN numbers created to define these customers serve an additional function of facilitating CRM web site access (by the customer).

Available Reseller administrative actions include:

- Add Batch
- Edit Batch

- Delete Batch
- Enhanced Batch Deletion
- Export Batch
- Import Batch
- Replicate Batch
- Selective PIN Activation/Deactivation

Each of these functions and required procedures for their execution is described in the sections that follow:

### Creating (Add) Reseller Batches

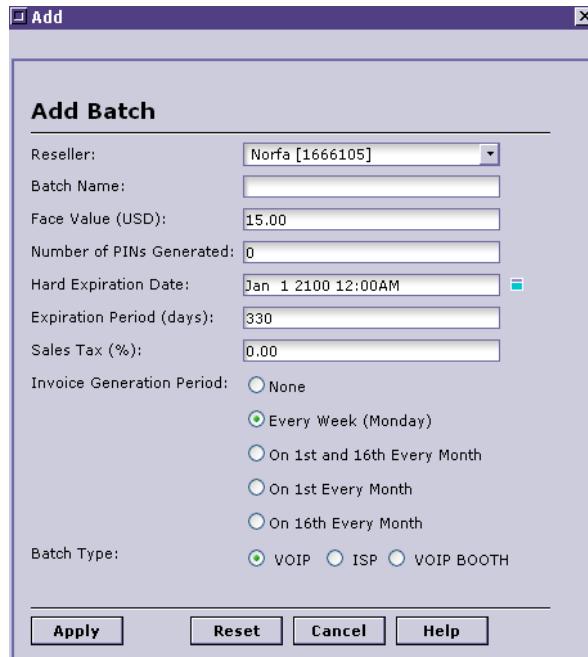
This is the first step in Batch Administration, and is based on batch definitions comprised of user-set parameters:

**Table 1-6      Batch Parameters**

Reseller	Specifies the reseller for which this batch is created.
Batch Name	Identifies the batch.
Face Value (\$)	Specifies the value of every calling card for this batch.
Number of PINs Generated	Configures total PIN generation count
Hard Expiration Date	Specifies a firm end date after which all accounts (respectively PINs and calling cards) will be considered invalid and void.
Expiration Period (days)	Specifies the expiration period for the account (PIN and calling card) after making the first call.
Delta Sample Rate (\$/100)	Specifies the delta rate in US cents for the Sample Rate in US cents. The Sample Rate specifies the rate that the user will be charged for each Sample Interval for which he/she used the service.
Tax (%)	Absolute tax imposed on the batch.
Invoice Generation Period	When and how often to generate an invoice for batch accounts.
Batch Type	VoIP: for typical Voice over IP customers ISP: for Internet Service Provider customers VoIP Booth: for VoIP customers who use a kiosk or call booth to make VoIP calls

To create a reseller batch:

- Step 1** Create a Reseller account, if you have not done so.
- Step 2** At the Navigator view, select **Batch Management**.
- Step 3** Select **Reseller Batches**, then select the client folder for the client who is the ‘target’ of the batch creation.
- Step 4** Select **Edit>Add Batch**. The Add Batch dialog is produced:



**Figure 1-199Adding a Batch**

- Step 5** Define the batch by setting parameters (described above).
- Step 6** Select Apply when finished.

---

**Note** Once a batch has been created it generates Personal Identification Numbers (PINs). Such generation does **not** ensure that PINs are active. Batch activation is done through the Edit Reseller Batches dialog, through the Generate Pins option.

An administrator can also selectively deactivate specific PINs within a batch by using the Selective PIN Activation/Deactivation Edit menu option.

---

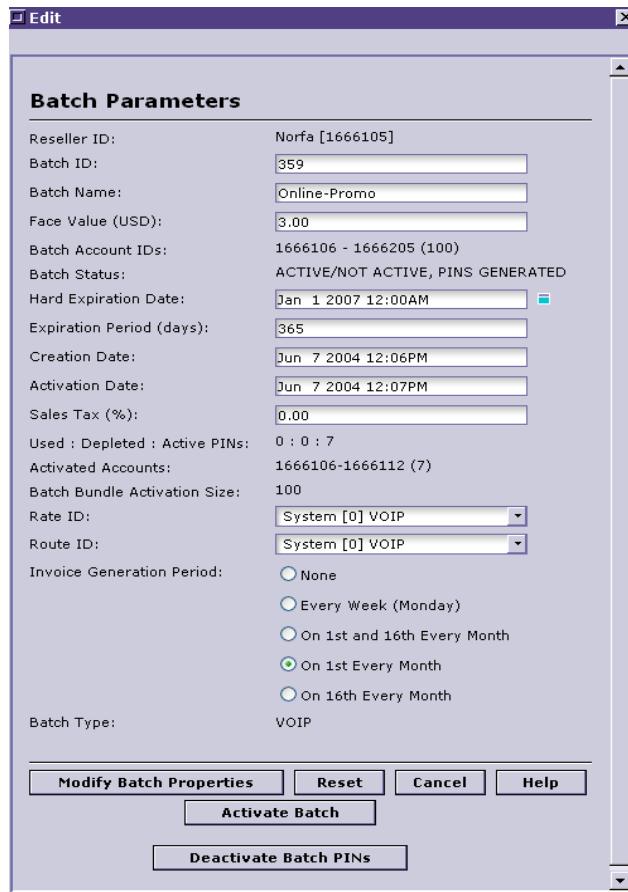
To activate batches for which automatic (Global Batch Management setting) activation is not configured, see the next section.

## Edit Reseller Batches

(Note that when viewing the Edit dialog for Reseller Batches, the appearance may be slightly different than the Add Batch dialog. Do not be deterred; the same parameters are included.)

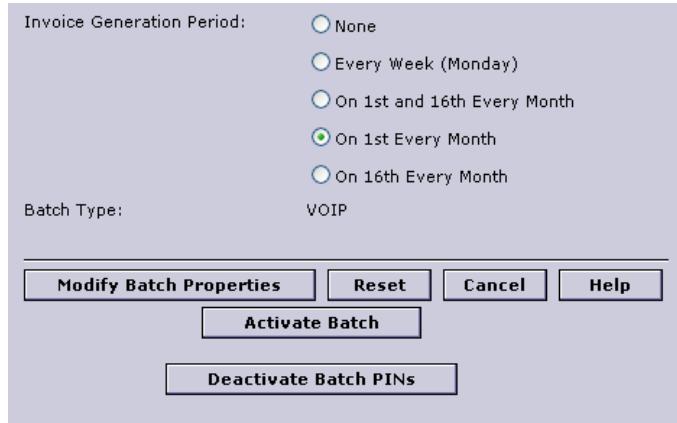
To edit a Reseller PIN batch:

- Step 1** From the Navigator, select **Batch Management>Reseller Batches**.
- Step 2** Select a reseller batches folder or entry from the Reseller window.
- Step 3** Select the specific batch to edit.
- Step 4** Select **Edit>Edit Batch**. The Edit dialog appears:



**Figure 1-200**Editing a Reseller Batch

- Step 5** In the dialog enter the necessary changes.
- Step 6** *If you have just created a batch and would like to activate its PINs, select Activate Batch.*  
This view shows the same dialog with the bottom portion visible:



**Figure 1-201 Editing a Batch: Selection Buttons Available**

**Step 7** Select **Apply** to enforce any and all changes.

#### Delete a Reseller PIN Batch

- Step 1** From the Navigator, select **Batch Management>Reseller Batches**.
- Step 2** Select a reseller batches folder or entry from the Reseller window.
- Step 3** Select the specific batch to delete.
- Step 4** From the Navigator menu select **Edit>Delete Batch** command.
- Step 5** Confirm the deletion at the prompt.

---

**Note** All related Reseller accounts belonging to the batch are also deleted. Please do not delete batches unless you are prepared to accept this consequence as well. //**checking to see if this is so//**

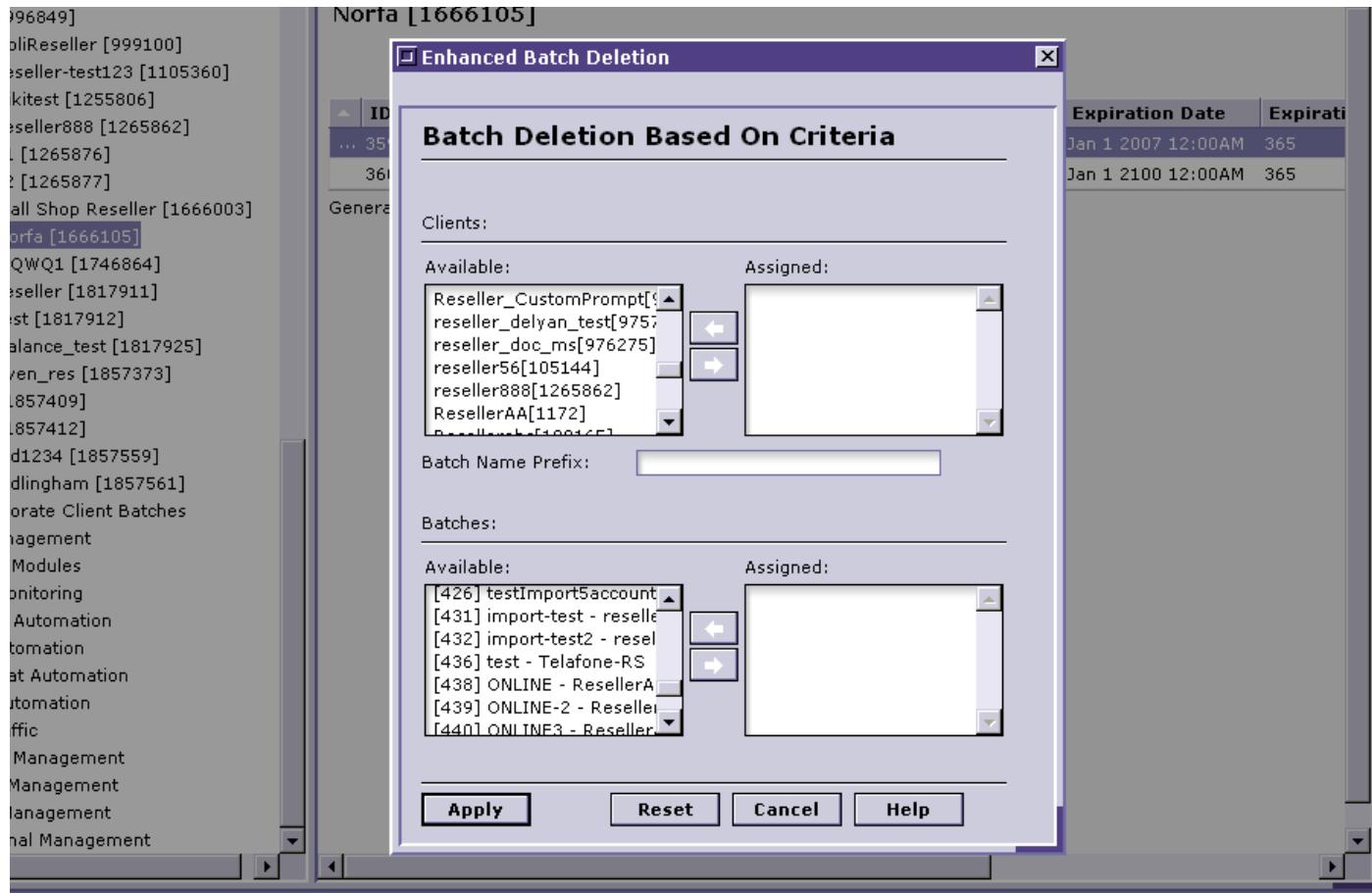
---

#### Enhanced Batch Deletion

Enhanced Batch Deletion is a special, ‘global’ implementation of the delete function applied to batches. It lets an Administrator delete individual clients associated with batches, groups of such clients, or selected batches assigned to clients.

To perform Enhanced Batch Deletion:

- Step 1** From the Navigator, select **Batch Management>Reseller Batches**.
- Step 2** Select a reseller batches folder or its entry from the Reseller window.
- Step 3** Choose **Edit>Enhanced Batch Deletion**. The corresponding dialog is presented:



**Figure 1-202Batch Deletion Based on Criteria (Enhanced Deletion)**

**Step 4** Select clients or batches to delete:

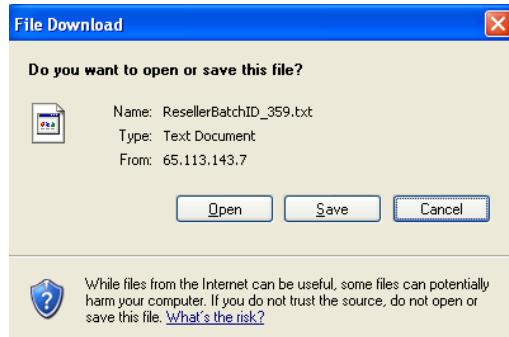
- Select one or more batch-associated clients by moving them from the Available to the Assigned box.
- Alternately, enter a client prefix in the special text entry field below the Client assignment interface.
- Assign individual batches by selecting them and moving them to the Assigned box (this refers to the lower of the two sets of Available/Assigned boxes in the dialog).

**Step 5** Select **Apply** to confirm the custom ‘batched’ batch deletion.

To export a Reseller PIN batch

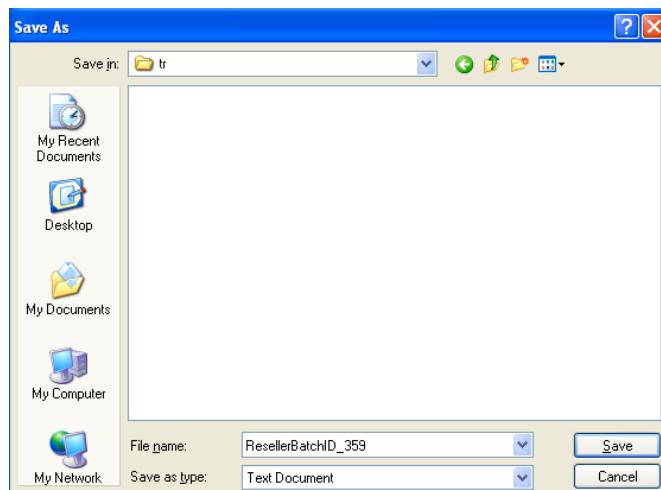
It's also possible to export a Reseller Batch:

- From the Navigator, select **Batch Management>Reseller Batches**.
- Select a reseller batches folder or entry from the Reseller window.
- Select the specific batch to export.
- Choose the **Export Batch** edit option.
- Use the File Download dialog to confirm that you wish to export (Save) the selected batch:



**Figure 1-203** Exporting a PIN Batch

**Step 6** Confirm the export (save) when this window appears:



**Figure 1-204** Finishing Batch Export

**Step 7** Locate a target directory, then save the batch file.

### Replicate Batches

You can also replicate (copy) a batch, creating multiple instances of it. This may be useful to create a stock of PINs for a batch to activate upon expiration, or for some other reason (**please supply**).

To replicate batches in VoiceMaster:

**Step 1** From the Navigator, select **Batch Management>Reseller Batches**.

**Step 2** Select a Reseller Batches folder.

**Step 3** Select a source batch from that reseller's listed batches in the Navigator window.

**Step 4** Select **Edit>Replicate Batch**. The necessary dialog is shown:



**Figure 1-205(Live) Batch Replication**

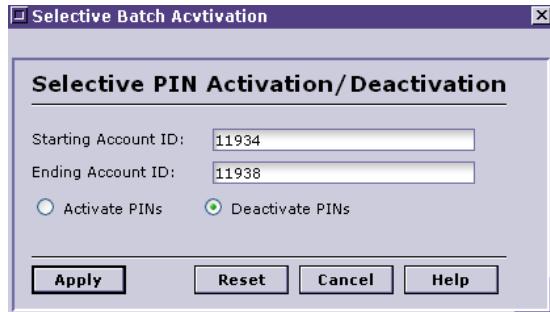
- Step 5** Select the batch to replicate from the pull-down.
- Step 6** Enter a number of copies to create.
- Step 7** Select **Apply**.

### Selective PIN Activation/Deactivation

PIN activation can also be controlled on a pin-by-pin basis. This granularity lets the Administrator specially activate a desired PIN/account. Inversely, it permits the deactivation of any batch-associated account that for which payment is not made or some other event occurs that may trigger an 'account close' response.

To activate any PIN tied to a batch:

- Step 1** From the Navigator, select **Batch Management>Reseller Batches**.
- Step 2** Select a Reseller Batches folder.
- Step 3** Select a batch from the Navigator window.
- Step 4** From the Edit menu, choose **Selective PIN Activation/Deactivation**. The activation dialog appears:



**Figure 1-206PIN Activation in Progress**

- Step 5** Set starting and ending Account IDs for activation.
- Step 6** Enable the **Activate PINs** setting.
- Step 7** Select **Apply** to confirm and enforce the step.

---

**Note** To deactivate a PIN or group of PINs, perform Steps 1-5. At Step 6, select **Deactivate PINs**.

---

## View Batch-Created Customer Accounts

PIN batches can also be a vehicle to viewing and editing customer accounts created as batches:

- Step 1** At the Navigator, select Account Management.
- Step 2** Choose the specific account management type folder.
- Step 3** Use the Reseller Batch ID filter to list all accounts belonging to a particular batch. (The Batch ID sits in the Batch definition dialog.)
- Step 4** Click the Search button to list the accounts, then open any you like (Edit Account Info).

# A Sample Batch Administration Workflow

## Step One: Create a Batch

- Step 1** Go to **Batch Management>Reseller Batches**
- Step 2** From the menus select: **Edit>Add Batch**.
- Step 3** In the Add Batch window:
  - choose Reseller;
  - add Batch name;
  - add Face Value of each card;
  - add size of batch in number of PINS/accounts to be generated;
  - modify expiration period;
  - press the Apply button.

The batch is created but NO PINs are generated yet. Batch status is NOT ACTIVE.

## Step Two: Generate PINs

- Step 1** Go to **Batch Management>Reseller Batches**.
- Step 2** Highlight the desired batch.
- Step 3** From the menus select: **Edit>Edit Batch**.
- Step 4** Press the Generate PINS button at the bottom of the dialog:
  - this starts PIN generation: approximately 1000 PINs per minute;
  - a counter appears on the screen incrementing by 100 PINs;
  - once the PINs are generated the Edit Batch screen pops up.

Batch Status is ACTIVE; PINs are disabled.

### Step Three: Export PINs

- Step 1** Go to **Batch Management>Reseller Batches**.
- Step 2** Highlight the desired batch.
- Step 3** From the menus select: **Edit>Export Batch**.
- Step 4** Save the file in comma separated format.
- Step 5** Print Cards.

### Step Four: PIN Activation

- Step 1** Select **Batch Management>Reseller Batches**.
- Step 2** Highlight the target batch.
- Step 3** From menus select: **Edit>Edit Batch**.
- Step 4** Hit the Activate Batch PINs button to activate the accounts.

### Importing Versus Exporting Batches

It is important to note that differences exist between batch import and export.

Selecting a batch to import produces a Search (Browse) window from which the desired file is located, then processed (entered into the system).

Exporting a batch is effectively saving the batch to file (duplicating it).

---

**Note** This will be discussed in more detail in the printed version of this Guide.

---

## Corporate Client Batch Management

Corporate Clients are assigned batches of PIN (Personal Identification Number) numbers. These clients then distribute the PINs to employees.

The difference between Resellers and Corporate Clients is that the customers accessing the system through a Corporate Client account share an aggregated amount of money. When the set limit for a Corporate Client is exceeded, further calls are suspended. Once the client account is empty, no individuals may make calls until more PINs are distributed (new batch created).

**Table 1-7      Corporate Batch Settings:**

Client Batch ID	Specifies the client the batch belongs to.
Corporate Batch Name	Specifies the name.
Hard Expiration Date	Firm end date after which all accounts will be considered invalid and void.
Expiration Period	The expiration period for the account after making the first call through its PIN.
Monthly Cap Per PIN	Specifies a monthly limit of calls per corporate batch.
Call Cap Per PIN	Specifies the maximum call time per single call belonging to the corporate batch created.
Creation Date	Moment of Batch Creation (including Day/Month)

## Configuring Corporate PIN Batches

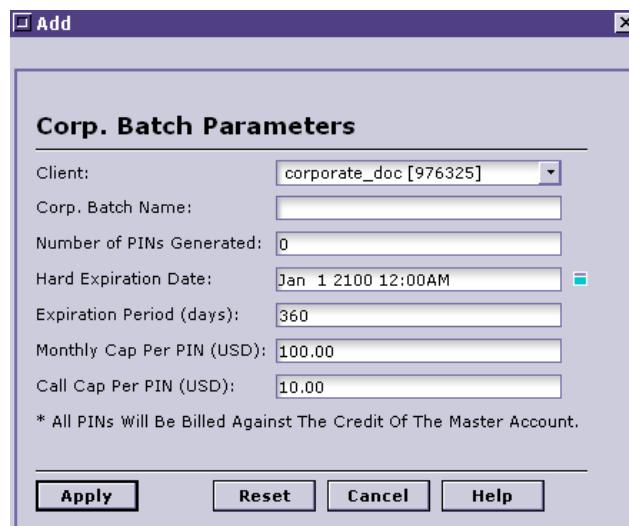
This section describes the configuration of Corporate PIN Batches.

To create a Corporate Client PIN batch

**Step 1** From the Navigator, select **Batch Management>Corporate Client Batches**.

**Step 2** Select a specific client folder.

**Step 3** Choose **Edit>Add Batch**. The edit dialog is now displayed:



**Figure 1-207Adding Corporate Client Batch**

**Step 4** In the dialog box, configure each parameter or setting

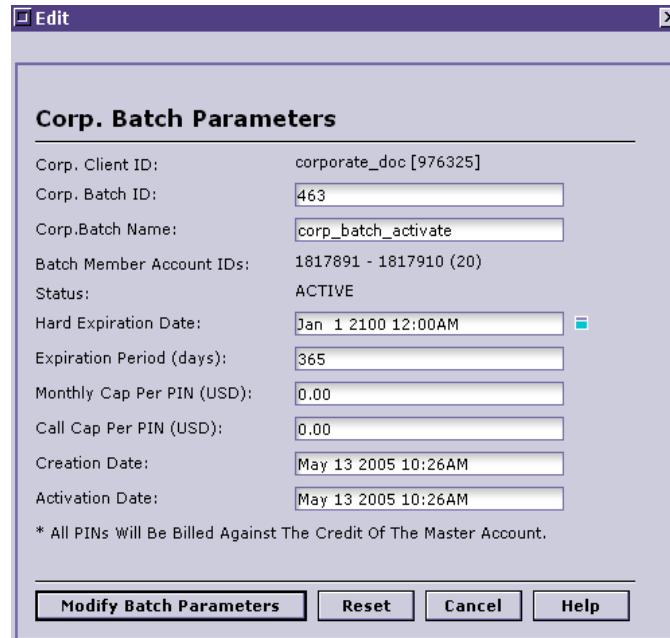
**Step 5** Click on the Apply button to create the new batch.

To activate a Corporate Client PIN batch

**Step 1** From the Navigator tree select **Batch Management>Corporate Client Batches**.

**Step 2** Select the specific client folder, then select a batch from the window at right.

**Step 3** Select **Edit>Edit Batch** command.



**Figure 1-208Editing Corporate Batches**

**Step 4** Click on the Activate button to activate the batch. The new batch is created but is still not active.

To edit a Corporate Client PIN batch

- Step 1** From the Navigator tree select **Batch Management>Corporate Client Batches**.
- Step 2** Select the client folder, then the specific batch from the list (window).
- Step 3** Again, choose **Edit Batch**.
- Step 4** In the dialog enter changes per setting as desired.
- Step 5** Select **Apply** to enforce changes.

### To delete a Corporate Client PIN batch

- Step 1** Select **Batch Management>Corporate Client Batches**.
- Step 2** Select the client folder, then the specific batch from the list (window).
- Step 3** Select **Delete Batch** from the Edit options.
- Step 4** Confirm the deletion at the confirmation prompt to delete it.

### To export a Reseller PIN batch

- Step 1** Select **Batch Management>Corporate Client Batches**.
- Step 2** Select the client folder, then the specific batch from the list (window).
- Step 3** Choose the **Export Batch** edit option.
- Step 4** Use the File Download dialog to confirm that you wish to export (Save) the selected batch:
- Step 5** Confirm the destination directory and save the download (export).

### View Customer Accounts Created Via Corporate Client PIN Batches

PIN batch numbers are also a search reference for retrieving customer accounts:

- Step 1** At the Navigator, select Account Management.
- Step 2** Choose the specific account management type folder.
- Step 3** Use the Corp Batch ID filter to list all accounts belonging to a particular batch.
- Step 4** Click the Search button to list the accounts, then open any account desired.



# Chapter 10: Special Implementations

---

## In This Chapter

This chapter presents the Special Implementations that differ from ‘typical’ VoiceMaster implementations.

Though no ‘stock’ implementation truly exists, there is a typical system use architecture in which the VoiceMaster is used by a VoIP service provider/owner to directly service customers. In this scenario - the basis for most of the Guide - the VoIP service provider and the VoiceMaster owner are one and the same. An Administrator configures and manages the entire system (gatekeeper, routing, billing) for the business.

In the case of Managed Services, the basic product (VoIP service) is the same, but additional entities play a role in the basic structure. This is an agent who is also the business owner, and contracts with the VoiceMaster owner for infrastructure and administration needs - bandwidth, termination devices, gatekeeper and routing functionality. The agent manages his own customer’s billing needs, based on his own expenses charged by the VoiceMaster owner.

---

**Note** This relationship is actually similar to that of the VoiceMaster owner and the network provider in ‘standard’ implementations. In these configurations, the VoiceMaster owner is dependant on the network providers for infrastructure. Without this relationship, only part of the infrastructure is in place. In Managed Services, the agent/business owner has no physical infrastructure, and relates to the VoiceMaster owner as his infrastructure provider.

---

In the case of ISP billing, the general structure is unchanged, but the product itself changes from “VoIP Service” to “Internet Access.” The subscription is now for ISP service and not VoIP calls.

Basic chapter topics are:

- Managed Services
- ISP Billing

## Managed Services Configuration

Managed Services configuration is the means by which an Administrator implements the VoiceMaster Managed Services business model. In this model, VoIP administrative duties are divided between the VoiceMaster owner and an agent (reseller/wholesaler) who “leases” core VoiceMaster functionality to set up his own service.

**Note** We refer to a ‘VoiceMaster owner’ when describing Managed Services because the agent, rather than the owner, is the VoIP service provider to the customers (subscribers). The VoiceMaster owner provides infrastructure and administrative services only.

---

The VoiceMaster owner provides administrative support functions for the agent’s subscribers but does not interact with them. The ‘box’ owner’s revenues derives from the infrastructure charges billed to the agent. The agent requires the gatekeeper, routing and billing power of VoiceMaster to run his network and enable customer calls. His profits derives from customer subscriptions and call. Agent expenses are the sum of the infrastructure functionality provided by the owner.

The customers see the agent’s company as the VoIP service supplier, while behind the scenes the infrastructure and essential management services are provided by the actual VoiceMaster owner. This should all be invisible to the customer.

The final component in this implementation architecture is the network provider bandwidth and termination points that the VoiceMaster owner uses.

It goes something like this:

VoiceMaster Infrastructure (including network provider data links and gateways)  
**plus**  
VM owner-agent relationship  
**plus**  
agent billing administration  
**plus**  
agent-customer relationship  
**plus**  
customer account subscription/usage  
**equals**  
Managed Services implementation design.

This unique architecture finds expression most clearly in the mechanics of billing. Instead of the standard two billing interactions:

- Network provider to VoIP service
- VoIP service to customer

Another layer is added:

- (Network provider to VoIP service) - Expense charged to VoiceMaster owner
- VoIP service (here: VM owner) to agent - expense to agent, revenue for VM owner
- Agent to customer - Expense (charge) to customer, revenue for agent.

## An Agent’s Perspective

The agent (reseller or wholesaler) may be thought of as substituting for the VoIP service in the typical VoiceMaster implementations. The agent’s business is the focus. Just as in standard scenarios, the agent provides VoIP calling privileges to subscribers, and (from the customer point of view) facilitates the technical process of placing VoIP calls.

The difference is that the agent will not administer more than the billing components of the business. All gatekeeper and routing administration is provided by the VoiceMaster owner, while IP links and termination devices are supplied by the network provider. Though the agent interacts with the VoiceMaster owner, he has no contact with network providers.

Typically, the agent manages revenues received from customers, provided he has the necessary administrative privileges. (These are defined by the VoiceMaster owner, and are settled in the agreement between these two parties.) The agent's expenses are really the sum of:

- The network provider expenses (rates) already charged to the VoiceMaster owner
- Additional expenses (VM owner profit) added to these basic infrastructure costs.

The VoiceMaster owner passes on provider expenses to the agent by binding the agent and his customer to the VoiceMaster owner's own provider rates. It is the configuration of customer billing rates that enables the agent to create enough overall revenue to create profit, after his expenses are deducted.

Setting up Managed Services involves two basic steps:

- Creating a Managed Services model. This means defining/configuring the basic roles and elements that exist within the Managed Services VoIP business model.
- Configure Managed Services accounts. This implements the model by configuring real agent (reseller/wholesale) accounts that will employ the Managed Services model created in the previous step.

## Create a Managed Services Model

In order to create such a three-layered structure you need to do the following:

**Step 1** Create a Reseller Account for your Reseller (Agent). Do this through the Account Management folder:

- (a) Log in and open the Navigator.
- (b) Select **Account Management** from the Navigator view.
- (c) Select the desired account type folder: reseller or wholesaler.
- (d) Choose Edit>Add Account. View the Add Account dialog:

**Figure 1-209Add Agent (Reseller/Wholesaler) Account**

- (e) Assign the parameters that define the wholesaler or reseller whose account you are creating. **Refer to the following chapter on Account Management for relevant field definitions and configuration options.**

---

**Note** Be sure to define the User Type correctly at the User Type field (pulldown menu).

---

- (f) **Apply** the changes, and the new agent (reseller/wholesaler) account is saved and recognized by the system as an existing account. (You can modify it at any time.)

**Step 2** Create a ‘dummy’ provider account (Billing Provider) in order to charge the new agent provider/termination expenses. Do the following:

- (a) At the Navigator view, select **Account Management**.
- (b) Select the **Provider Accounts** folder.
- (c) Select **Edit>Add Account** and view the Add Account dialog (identical to that shown in Figure 5-13).
- (d) Configure the provider account information, making sure that you select *Network Provider* at the User Type field. Call this account *Dummy Provider*.

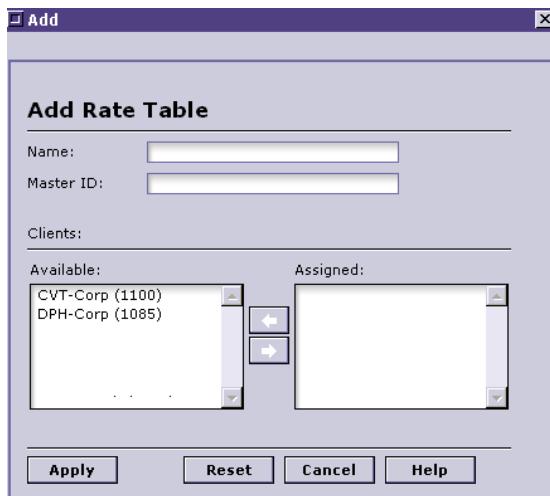
- (e) Select **Apply** to configure the ‘dummy’ provider account.

**Step 3** Import the Billing Provider rates (to apply to your Agent):

- (a) From the Navigator, select **Rate Management**.
- (b) Select **Provider Rate Tables**.
- (c) Now locate and select the folder called **Dummy Provider** (the system created this folder at the end of Step 2 above).
- (d) Select **Edit>Import Provider Rates**. The Windows browse dialog appears. Browse the files and import the provider rates that will apply to this agent (that apply to the routes/termination gateways that the agent’s customers will ‘borrow’ when making calls).

**Step 4** Create a blank Billing Rate Table and set the owner of the billing rate table to the reseller account ID. This billing rate table will be used by the managed services account to manage the billing rates for their end users. Example: **Reseller A Rates**. To do so:

- (a) Select **Rate Management>Billing Rates**.
- (b) Select **Edit>Add Rate Table**. View the dialog box that is displayed:

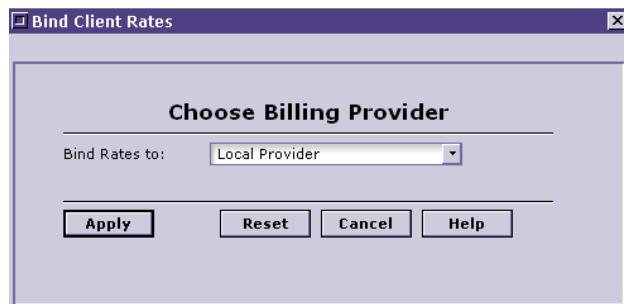


**Figure 1-210Adding a Rate Table**

- (c) Name it (Reseller A Rates) and assign a Master ID.
- (d) Add the reseller batch.
- (e) Select **Apply** to create the table.

**Step 5** Bind the Billing Provider rates to the Agent, following these steps:

- (a) Select **Rate Management>Provider Rate Tables**.
- (b) Select the agent rate folder (Dummy Provider) from the Provider Rate Tables folder.
- (c) Select **Edit> Bind to Provider Rates**. The Bind Client Rates dialog appears:



**Figure 1-211Binding Client Rates to a Provider**

- (d) Choose “Dummy Provider” as the billing provider.
- (e) Select **Apply**.

**Step 6** Create a System User account (refer to **System Users Configuration** earlier in this chapter). Make the user’s *role Reseller/Corporate—MS*. Assign the Reseller A account ID as the Master ID, as shown here (while not forgetting to configure all the System User Management parameters in the dialog):



**Figure 1-212‘Reseller’ A Master ID**

---

**Note** If you want the MS reseller to manage his own provider and routes, set the Provider ID to a real provider account ID. This lets the agent add charges to his customers. Failing to do so strips the agent of administrative rights.

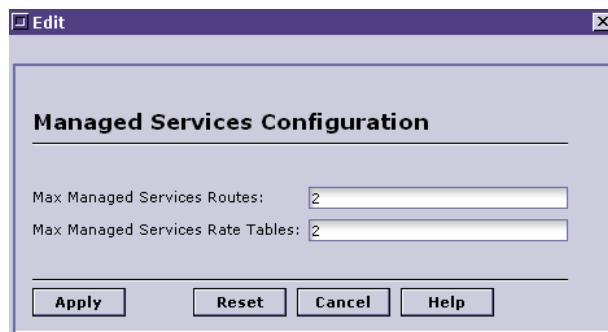
---

With this setup, **Reseller A** Rates will represent Reseller A’s charges to customers - his revenue. **Agent Rate (Dummy Provider)** rates will represent Reseller A termination charges, or your Revenue from Reseller A.

## Configuring Managed Services Accounts

Follow these steps to create actual Managed Services accounts that will use the structure just created:

- Step 1** Create a Reseller/Corporate client account (refer to the previous section or the Account Management chapter for a reminder on how to do this).
- Step 2** Create a System User account and use the Reseller Account ID as its Master ID.
- Step 3** Create the billing rate plan for that reseller as described in the previous section, again applying the Master Reseller ID to the plan.
- Step 4** Select **System Configuration>System Settings**.
- Step 5** Select **Managed Services Configuration** from the System Settings window.
- Step 6** Select **Edit>Edit Settings** to display the Managed Services dialog:



**Figure 1-213** Managed Services Route/Rate Settings

- Step 7** Enter the maximum number of routes and rate tables that you want Managed Services agents to be able to manage. Assuming that the agent has billing management rights (contingent upon a real provider account ID being assigned in the previous procedure), the agent can create as many rate tables as desired - up to the number specified here.

The maximum number (each) of routes and rate tables that an agent can administer is 100.

---

**Note** If the reseller is to possess the ability to modify routes and add gateways to route, you must enter his ID when defining routes to which his administrative privileges will apply. (This is done when creating routes, as described in Chapter Four and again in [Chapter Seven: Route Management](#).)

---

## ISP Billing

ISP Billing is a special implementation of VoiceMaster functionality that creates an ISP billing service. In both the typical VoiceMaster scenario and in the Managed Services model just discussed, the ‘subject’ or service provided to the end customer is VoIP service. In the ISP Billing model (and implementation), the underlying rate functionality is still used, just directed towards ISP providers.

You can find additional descriptions of ISP Billing at the SysMaster home page on the Web, specifically at [/brochures/isp\\_billing.pdf](/brochures/isp_billing.pdf).

## Network Configuration Requirements

ISP Billing requires a network configuration that includes the following:

- The VoiceMaster's primary Ethernet port (eth0) should have a public IP assigned to it. This port is used to access the Internet via the ISP Gateway.
- The second Ethernet port(eth1) is connected to a private network.
- The client uses the VoiceMaster's private IP address as the default gateway. This means that all traffic destined for the Internet passes through the Voicemaster.

These are settings that reflect the ISP provider's use of the VoiceMaster as the physical access point to the Internet for all Internet connections made by his own customers.

## ISP Billing Configuration

This procedure sets for the entire ISP billing configuration process. It all starts with account creation.

### Create an ISP Provider Account

Configuring an ISP provider account is the first phase of the process:

**Step 1** Select Account Management>ISP Provider Account

**Step 2** Select Edit>Add Account. The Add Account dialog appears:

**Figure 1-214Add (ISP Provider) Account**

**Step 3** Specify the username, password, and company name (the username and password will not be used, but are required fields in the dialog).

- Step 4** Under User Type select ISP Provider./  
**Step 5** Click **Apply** to save the new account.

### Create an ISP User Account

Creating the accounts of the ISP service subscribers is next:

- Step 1** Select **Account Management>ISP Users**.  
**Step 2** Select **Edit>Add Account**. The dialog in Figure 10-7 is again displayed.  
**Step 3** Specify the username and password (to be entered to obtain access to the Internet).  
**Step 4** At the User Type field, select ISP User.  
**Step 5** Click **Apply**.

### Create ISP Provider Rate

The next phases of the ISP Billing implementation scenario involve the application of billing policy. ISP provider rate parameters are similar to provider rate parameters, the major difference between the two being the addition of ISP Provider Rate bandwidth management functionality.

System administrators must specify an initial bandwidth usage, which is effectively a form of time management. Rate plan parameters include:

**Table 1-8 ISP Rate Parameters**

Name	Specifies the name.
Bind to Provider	Specifies the initial bandwidth to be applied to the account. Init Bandwidth is necessary for proper billing to be conducted.
Session Timeout	Specifies the flat charge to be imposed based on initial bandwidth usage
Init Bandwidth	Charge to be levied on the user during the initial time interval
Init Bandwidth Charge (USD)	Specifies the flat charge that will be imposed for the initial Init Bandwidth used.
Sample Bandwidth	Specifies the sample bandwidth that will be used to calculate the charges that will be imposed on users that exceeded the Init Bandwidth. E.g. if Sample Bandwidth = 1MB and Sample Bandwidth Charge = \$1 then the user will pay effectively \$1 per 1MB bandwidth on surpassing the cap.
Init Time	Specifies the initial time interval used in calculating billing charges. In most instances, the value of the Init Time parameter is supplied to the VoiceMaster owner by the respective network provider.
Init Time Charge (USD)	Specifies the charge to be imposed on the client for communication usage during the initial time (Init Time) interval.
Sample Time (sec)	Specifies the period of time after the end of the initial time (Init Time) interval. Sample Time is used in calculating billing charges imposed on users/clients when the initial time (Init Time) period has been exceeded.
Sample Time Charge (USD)	Specifies the charge to be imposed on the client for communication usage during the Sample Time interval.
Time Unit	Specifies the unit in which Init Time and Sample Time intervals would be measured in. Available options are: Hour/Day/Week/Month/Year Year

Billing Period	Specifies the time frequency for statement / billing generation Available options are: Hour/Day/Week/Month/Year Year
Billing Period Base	Specifies when the statement / billing period should start. Available options are:  Calendar Period - refers to a particular instance in time (e.g., the first day of the week (Monday), the first day of the month (01), the first day in the year (01 Jan))  Billing Base Date - refers to a particular date specified by the user in the "Base Billing Date" field
Base Billing Date dd mmm yyyy (e.g., 01 Jan 2003)	Specifies the base billing date from which the statement / billing cycle would begin.
Billing Type	Specifies the rules according to which billing would be imposed. Available options are:  Time - billing would be based on time rules Bandwidth - billing would be based on bandwidth rules Bandwidth and Time - billing would be based on both bandwidth and time rules  Lower From Both -billing would be based on both bandwidth and time rules. However, final billing calculation would be performed based on the lowest billing rule price  Higher From Both -billing would be based on both bandwidth and time rules. However, final billing calculation would be performed based on the higher billing rule price.

To create the ISP rate plan:

- Step 1** Select **Rate Management>Internet Rates**.
- Step 2** Choose **ISP Providers**.
- Step 3** Select **Edit>Add ISP Provider Rate**.
- Step 4** Select the provider at the Bind to Provider field.
- Step 5** Configure the Rate Plan to coincide with what the ISP charges for access. Confirm.

### Create ISP Billing Plan

This is where the Administrator configures the charges to apply to ISP service provider customers.

Billing plan parameters include:

**Table 1-9 ISP Billing Parameters**

Name	Plan Name
Init Bandwidth	Specifies the initial bandwidth to be applied to the account.
Init Bandwidth Charge (USD)	Specifies the flat charge on accounts based on the initial bandwidth usage.
Sample Bandwidth	Specifies the charge to be levied on the user during the initial time interval.

Bandwidth Unit	Specifies the bandwidth unit in which Init Bandwidth and Sample Bandwidth are measured.
Init Time	Specifies the initial time interval used in calculating billing charges.
Init Time Charge (USD)	Specifies the charge to be imposed on the client for communication usage during the initial time (Init Time) interval.
Sample Time (sec)	Sample Time is used in calculating billing charges imposed on users / clients when the initial time (Init Time) period has been exceeded.
Sample Time Charge (USD)	Specifies the charge to be imposed on the client for communication usage during the Sample Time interval.
Time Unit	Specifies the unit in which Init Time and Sample Time intervals would be measured in. Available options are: Hour/Day/Week/Month/Year
Billing Period	Specifies the time frequency for statement / billing generation Available options are: Hour/Day/Week/Month/Year
Billing Period Base	Specifies when the statement / billing period should start. Available options are:  Calendar Period - refers to a particular instance in time (e.g., the first day of the week (Monday), the first day of the month (01), the first day in the year (01 Jan))  Billing Base Date - refers to a particular date specified by the user in the “Base Billing Date” field
Base Billing Date dd mmm yyyy (e.g., 01 Jan 2003)	Specifies the base billing date from which the statement / billing cycle would begin provided that the “Billing Base Date” option has been selected
Billing Type	Specifies the rules according to which billing would be imposed. Available options are:  Time - billing would be based on time rules Bandwidth - billing would be based on bandwidth rules Bandwidth and Time - billing would be based on both bandwidth and time rules Lower From Both - billing would be based on both bandwidth and time rules. However, final billing calculation would be performed based on the lowest billing rule price. Higher From Both - billing would be based on both bandwidth and time rules. However, final billing calculation is done based on the highest billing rule price.

The procedure is:

- Step 1** Select **Rate Management>Internet Rate >ISP Plans**.
- Step 2** Select **Edit>Add ISP Plan**.
- Step 3** Select the provider under Bind to Provider.
- Step 4** Configure the Plan with the charges to apply to End User's ISP sessions.
- Step 5** Select **Apply** to confirm.

## Assign the Billing Plan to the End User

To assign the configured billing plan to ISP service customers.

- Step 1** Select **Account Management>ISP Users**.
- Step 2** Find the account to assign to the ISP Billing plan.
- Step 3** Select **Edit>Edit Account**.
- Step 4** Assign the ISP Rate Plan from the available options.

## Setup Network Configuration

Specific network configuration is needed at this point. Follow these steps to configure these settings:

- Step 1** From the Navigator, select **System Configuration>Network Configuration**.
- Step 2** Select **IP Address Configuration**.
- Step 3** Select **Edit>Add Server IP Configuration**.
- Step 4** At the Add Network IP address dialog box, configure a public IP address (if not already assigned) to eth0 (in the Devices field). *Typically, this will already be assigned.* Apply the settings.
- Step 5** Open the same dialog box (step 3) and create a Private address, then select *eth1* at the Devices field. It should be in the same subnet as your clients. Apply settings.
- Step 6** Select the Server Configuration function.
- Step 7** Select the VoiceMaster server, then select **Edit Server Configuration**.
- Step 8** Set the Gateway to be the ISP gateway.
- Step 9** Set the DNS server. Apply.
- Step 10** Once again, select the IP Address Configuration function, then select the entry for device name *eth1*. Open the Edit Server IP Configuration option.
- Step 11** In the dialog, enable “NAT on the *eth1:0* port. This allows the VM to pass traffic from the Private Network to the Internet.
- Step 12** Click Apply.

## Setup Login Page

If you have a custom login page, upload it to the VoiceMaster Web Server root directory and change the setting “ISP Login File” to the name of your login file (ex: login.htm)

# Chapter 11: Custom Modules

---

## In This Chapter

The purpose of this chapter is to review the contents of the Administration Console's Custom Modules folder. This folder is the administrative link to the configuration and management of VoiceMaster custom modules, each of which has its unique value and attributes. (Each module must be obtained independently from SysMaster.)

Each module is described in its own section. Each has an overview that presents the role and benefits of the specific module, followed by procedural instructions that enable module administration.

---

**Note** Read the sections that pertain to the modules installed in your system first. There may also be benefit in reading other sections, especially if your business may derive value from including *those* modules in a system upgrade.

---

## Overview

Custom modules are specially purchased VoiceMaster add-on modules that expand overall system capability and functionality. Each custom module typically expands either 1) system billing capabilities and flexibility or 2) routing and call service functionality. Others have unique functionality such as fraud detection.

Using modules means configuring 'rules' that effectively create policies regarding some aspect of VoiceMaster function. For instance, the Custom Tax plan lets the administrator create rules that apply special taxes to desired customers.

The majority of custom modules address the desire of VoIP service providers to customize billing options and plans, enhancing billing configuration and management. While certain modules (Provider Time Interval) relate to system expenses, most rates-focused modules are directed towards customer billing. For instance, the Calling Plan module lets the Administrator assign custom calling plans for calls to designated area codes. Specialized rates are enabled, enhancing the flexibility of service options and offerings.

Other modules such as Custom Maps enhance call rate efficiency by enabling mapping (pattern translation) between numbers that may not fit the international telephony standard (E.164).

Another valuable module, Exception Numbers, enables the configuration of specific, varied responses to call attempts involving particular numbers. When fraudulent activity is suspected from these numbers, this may trigger aggressive fraud detection actions set in Exception Number's 'sister' module, Fraud Detection.

An Administrator basically works through several configuration phases when creating a policy for any module:

- Defining the rule, including the individual parameters that shape its functions, limitations and exclusions.

---

**Note** Some custom modules include Active and Inactive statuses that the user must select when defining a module rule. Others do not have this ‘on/off’ rule status option. *In the case of modules where configuration does not include setting the new rule status, you must assume that applying the rule makes it immediately active.*

---

- Assigning an object or ‘target’ for a particular module rule, whether that object be a customer, a number, a call pattern, etc. (here it is a customer)
- Applying area codes to the configured rule. This ties the rule’s contents (parameters) and target (a customer) to actual calls.

---

**Note** Administration is more efficient if modifications are made to a rule at one time, if possible. Organizing and executing management actions in this way will reduce overhead and make it easier to track system performance and behaviors.

---

## Calling Plans Module

The Calling Plan Module permits the assignment of flat-rate charges to specified users regardless of the time of day or day of the week. On active plan days (days of the week on which the plan pertain), callers are given allotments of free time (calculated in seconds). Throughout the month, clients and users assigned to a plan can use these minutes.

Once the client reaches this bulk time limit, calls continue, but billing now defaults to previous rate settings. Customers keep calling until they reach a monthly time cap (if set), at which point the system revokes their calling privileges.

A Calling Plan rule can also be configured so that each call governed by the rule can be limited to a specified number of seconds. If this call time cap is set, then calls are terminated when the cap is reached.

In addition, an Administrator can define the Calling Type as a standard or rollover plan. In the former case, plan-assigned clients have ‘x’ bulk time seconds for a monthly period. If they fail to exhaust this sum, the remaining time is lost to them. However, if the plan is defined as a *rollover* plan, unused minutes are assigned to the next monthly period.

The Calling Time module thus assigns the Administrator great configuration flexibility:

- Limit free minutes to a given month or let assigned clients take advantage of unused time
- Customize time interval and daily settings to have a plan reflect customer preferences - and, inversely, ensure that the specified customers are charged default billing rates at other times
- Increase or decrease free calling time (monthly bulk time), and use cap time limits to control caller behavior once bulk time is exceeded (allowing calls at ‘charged’ rates or refusing call permission).

---

**Note** Configuring a custom Calling Plan can be done in conjunction additional custom modules. (The implementation of multiple custom modules depends on your business needs and strategy.)

---



Figure 1-215 Calling Plans List

## Calling Plans Configuration

The Calling Plan module enables the configuration of special calling plans for particular customers dialing numbers within assigned area codes. The Administrator can configure multiple calling plans for various groups of clients.

As with other Custom Modules, creating a rule that applies to real-world calls involves three steps:

- Step 1** Define the core parameters that set billing rates per rule-defined calls.
- Step 2** Assign clients/users to the configured plan.
- Step 3** Apply area codes. This ties the plan definition and user assignment with real calls to specified destinations.

### Configuration Procedures

The contents of the VoiceMaster Edit menu will change to reflect the individual module selected. In the case of Calling Plans, the Edit menu contains these options:

- Add Calling Plan
- Edit Calling Plan
- Delete Calling Plan
- (Refresh)

Each Edit menu option (with the exception of Refresh) has a specific Administrative purpose. Note that Add and Edit (Calling Plan) are similar in purpose, the first serving to create new plans, the second to modify existing plans. The combined configured parameters create the calling plan rule.

Delete Calling Plan does just that, removes a Calling Plan and erases its application.

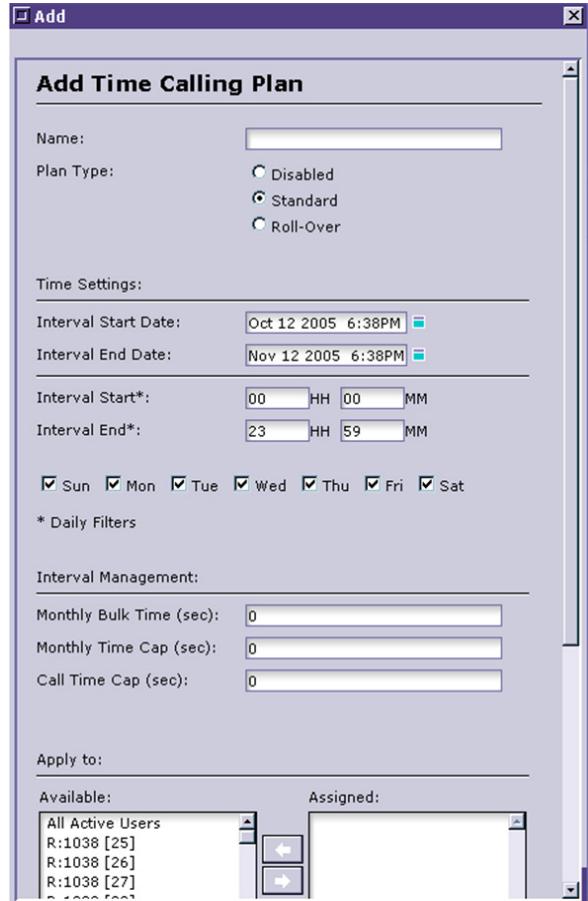
Refresh refreshes the Calling Plans.

### Add Calling Plan

To add a calling plan to the list of plans, follow these steps

**Step 1** Select Custom Modules>Calling Plans.

**Step 2** Select Edit>Add Calling Plan and view the Add Time Calling Plan dialog:



**Figure 1-216Add Time Calling Plan**

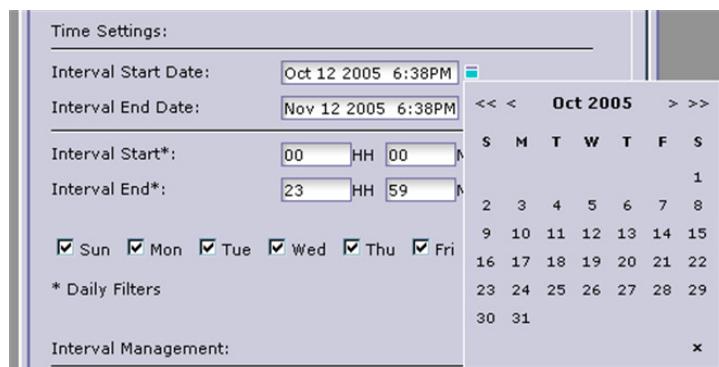
**Step 3** Assign a name to the plan. Choose a name that you can easily associate with the plan, one that relates to its time settings, time (interval) management, assigned clients, etc.

**Step 4** Set the plan type. The options are:

- **Disabled.** Disables the new plan so it won't be activated until you edit the plan and change its type to Standard or Rollover.
- **Standard.** Assigned users must use all allotted call time within each time period or lose it once the plan expires.
- **Rollover.** Unused time is added to the customer accounts after an assigned interval elapses.

**Step 5** Fix the time settings for the new plan:

- (a) Set Interval Start Date. Use the Calendar, the small, square turquoise box to the right of the preset date. When the dialog appears, as shown in Figure 3, click the desired date. It populates the Interval Start Date entry box.

**Figure 1-217** Interval Start Date PopUp Calendar

- (b) Repeat this for the Interval End Date (open the calendar popup, select a date).

---

**Note** The standard Calling Plan time is one month. Time interval management parameters are based on this period. If you set a plan to terminate in less than a month, two things happen: 1) all calls after the End Date are billed at default rates and 2) the plan terminates and the Administrator has to create a new Calling Plan to apply to the next month. (The plan is renewed only if the start and end points are one month apart.)

---

- (c) Choose interval start and end times. The Interval Start and End field entries determine the time of day that a calling plan takes effect. Typically, plans are set for the entire day.
- (d) Select days of the week to which to apply the new plan. All days are default-selected; uncheck any days on which you want the call plan **not** to apply.

---

**Note** Selecting specific days filters the plan's definition further. It lets the Administrator tailor the plan to 1) meet customer expectations and desires, 2) enhance revenues and 3) mesh with rules and rates set in other modules.

---

**Step 6** Set the Interval Management parameters:

- (a) **Monthly Bulk Time:** Total number of free calling hours, per month, assigned to plan-included customers. Once bulk time is exceeded, the user can continue to make calls according to default billing rates assuming a monthly time cap is configured (where the amount exceeds monthly bulk time).
- (b) **Monthly Time Cap:** Used to set a limit, beyond the bulk time, during which a rule-assigned customer may make calls but is billed per default rates. Further calls are terminated once the customer reaches the time cap (calling privileges resume at the start of the next plan month).

- (c) **Call Time Cap.** Sets a limit for the assigned call customers per call. Once this limit is reached, calls are disconnected. It is billed according to the customer's place in the bulk time-time cap progression.

**Step 7** Assign clients (and their customers/users) to the plan:

- (a) Select the available client or clients you wish to move (Shift + Click can select multiple clients simultaneously);
- (b) Click the right arrow key. The client moves to Assigned status.
- (c) Repeat these steps for additional clients/users as desired.

---

**Note** Most clients assigned belong to various batches that are pre-assigned to the Available window/box. You can assign batches of resellers, wholesalers and corporate clients, as well as end users not associated with a pre-defined batch.

---

**Step 8** Apply to area codes. Using the selection process outlined in Step 7, move the area codes that you wish to apply to the plan from the Available to Assigned box.

**Step 9** Select **Apply** to save changes and complete the plan's creation.

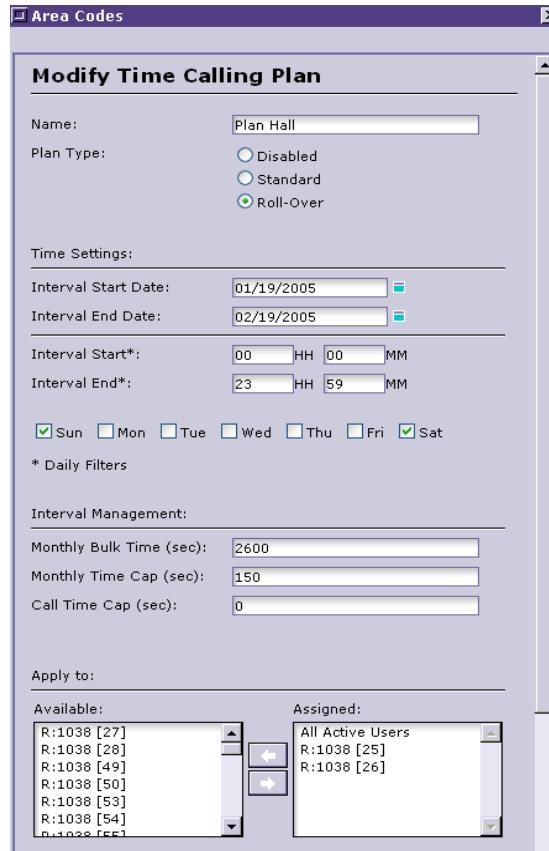
### Edit (Modify) Calling Plan

An Administrator may want to modify aspects of a configured Calling Plan. Editing a plan may be appropriate for a number of reasons:

- Change the plan type. For example, if you find that customers are not approaching monthly bulk time limits, redefining a standard plan to 'rollover' may make it more attractive to clients.
- Filter time settings, particularly days of the week. Adding or subtracting days on which a specific calling plan applies may reflect patterns of use or draw more clients/customers to your VoIP service.
- Redefine interval management settings. Increase or decrease monthly bulk time to respond to customers, or change policies activated when bulk time is reached (monthly and call time caps).
- Assign and remove new clients/users.
- Apply and remove specific area codes.

To edit an existing Calling Plan:

- Step 1** From the Navigator view, select **Custom Modules>Calling Plans**.
- Step 2** Select an existing plan from the Calling Plan list.
- Step 3** Open **Edit Calling Plan**. The Modify Time Calling Plan dialog (Figure11-4) is displayed.
- Step 4** Change any desired parameters.
- Step 5** Make as many changes as required to modify the plan policies. Actions are often related. For example, a change in monthly bulk time is often (though not necessarily) tied to changes in time cap settings.
- Step 6** When you have modified the calling plan to your satisfaction, select **Apply** to save and enforce the changes.



**Figure 1-218**Modify Calling Plans (Dialog)

### Delete Calling Plan

To delete a calling plan that is no longer relevant, do the following:

- Step 1** From the Navigator view, select **Custom Modules>Calling Plans**.
- Step 2** Select an existing plan from the Calling Plan list.
- Step 3** Select **Delete Calling Plan**.
- Step 4** A special message requests confirmation of the deletion. Click **OK** to delete the selected plan or **Cancel** to abort.

## CDR Collection Module

The CDR Collection Module contains essential functionality for those Administrators who wish to maintain coherent billing methodology when some configured gateways in the network lack AAA RADIUS (and when calls are not routed through the VoiceMaster gatekeeper). Call Detail Records are collected for systematic billing.

The CDR Collection module has two applications.

- The first is for importing batches of CDR records for delayed billing. To configure this, the target gateway must be added through the CDR collection module. Then, CDR records are imported via the Import CDR records functions. This is useful where an existing platform - switch, gateway, channel bank - collects such records but does not support Radius.
- The second application is configuring specific gateways as collection gateways. (Some gateways can send Radius accounting messages but lack the authentication/authorization facilities that typically trigger real-time billing.) In this case, the Administrator configures the gateway as a collection gateway, so that it will send billing records to the VoiceMaster.

Though an Administrator typically collects CDR records to facilitate his own billing mechanism, another purpose may be to provide billing service to additional VoIP service providers.

---

**Note** CDRs are kept for a period of up to 6 months in database but are stored in the accessible from the `/home/manager/cdr` temp directory for up to 2 months. Afterwards such ‘dump’ files are deleted. We recommend that the Administrator periodically back up CDR files back-up to avoid periodic automatic deletion.

---

## CDR Import

Instructions in this section are for CDR *import*.

For the collection role to function properly, the following conditions must be met:

- the collection gateway must be on a specified list of CDR gateways
- the file format must be correct.

---

**Note** Most VoIP service providers/Administrators experience problems with CDR collection because one of these two conditions are not met. They have either 1) not added the gateway to the list or 2) failed to specify the correct file format. (Procedures for using the module correctly follow).

---

### Add CDR Gateways

To add CDR gateways to those configured for importing records, follow these instructions:

- Step 1** From the Navigator view, select **Custom Modules > CDR Collection**. View the current CDR collection list, shown in Figure 5.
- Step 2** Select **Edit>Add CDR Gateway**. The CDR Collection Gateway dialog is displayed:



**Figure 1-219CDR Collection Gateway Dialog**

- Step 3** Open the Gateway ID list by selecting the down arrow to the right of the entry box. All available (managed) gateways are shown.
- Step 4** Select the Gateway that you want to add.
- Step 5** Select **Apply**. The gateway, complete with name, ID and IP address, joins the Current Gateway list.

You can now bill for customer calls through this gateway, assuming that such users have billing rates configured.

The other method of adding gateways to the Collection Gateway list is global. Instead of adding individual gateways, you add all available gateways in one fell swoop:

- Step 1** From the Navigator view, select **Custom Modules > CDR Collection** (if you have not already done so).
- Step 2** Choose **Edit>Add All Gateways**.
- Step 3** A confirmation dialog is displayed. Select **OK** to confirm that you wish to add all gateways. All gateways currently incorporated into the system's route management are added to the CDR Collection list.

### Delete CDR Gateways

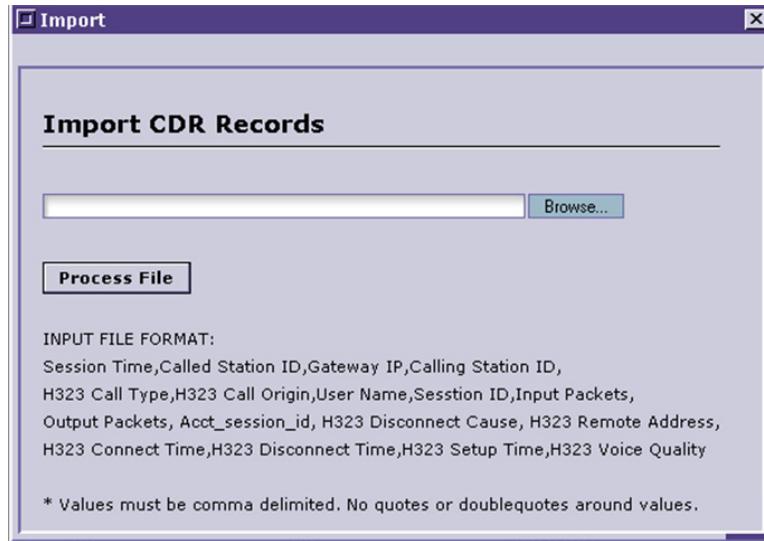
To delete a CDR gateway:

- Step 1** From the Navigator view, select **Custom Modules > CDR Collection** (if you have not already done so).
- Step 2** Select the gateway from the CDR Collection list that you intend to delete.
- Step 3** Select **Edit>Delete CDR Gateway**.
- Step 4** At the Confirmation prompt, select **OK** to delete or **Cancel** to abort the action and leave the target gateway as a CDR collection gateway.

### Import CDR Records

To import CDR records for post-call billing, do the following:

- Step 1** From the Navigator view, select **Custom Modules>CDR Collection** (if you have not already done so).
- Step 2** Select **Edit>Import CDR Records**. View the following dialog/window.



**Figure 1-220CDR Import Dialog**

- Step 3** If you know the target directory and file name, type it in the text entry box. If not, select **Browse** and browse Explorer directories to locate the CDR file to import.
- Step 4** Once the file is located and selected (it must appear in the text entry box), select the **Process File** button. The (correctly formatted) file is imported. The Administrator can bill customers associated with the calls that the file records.
- Step 5** Be sure that imported CDR files match the format specified on the Import CDR Records dialog.

## CDR Collection

To collect CDR records, the following must be established:

- The gateway must be notified that the VoiceMaster needs to collect its billing records periodically. In other words, the VoiceMaster administrator must communicate with the gateway owner (if the gateway belongs to a network provider).
- An external CDR collection facility, such as a softswitch, must be configured to collect the records.
- This device's administrator must send the files to the VoiceMaster in proper format.

The VoiceMaster administrator must:

- 1 Receive the file in the correct file format, using the import facility described above.
- 2 Add the data to billing configuration records.

## Custom Maps Module

The Custom Maps modules lets the Administrator standardize origination and termination number strings to conform to the international E.164 standard. Using Custom Maps functionality, the Administrator defines mapping rules that apply to called and calling number patterns from and to

designated endpoints. When calls are made to and from endpoints that fit within a Custom Map's definition, mapping is performed, the patterns are translated and conformity to the E.164 standard is established.

---

**Note** The E.164 standard includes country code, area code and calling/called number. Mapping translates patterns that deviate from this expected sequence into its format. E. 164 is discussed in detail at this HTTP (web site):

<http://www.en.wikipedia.org/wiki/E.164>

---

As this functionality description shows, the Custom Maps module has a very important role to play in a network where this standard is expected but certain endpoints' calling patterns do not conform to it. This can be an invaluable tool in enhancing call success ratios and satisfying customer demands.

Mapping is used to accomplish the following specific purposes:

- destination number normalization, in accordance with the E.164 standard.
- prefix stripping (system default)
- prefix appending

In each mapping type, actions are configured to 'clean up' some aspect of a call to match the country/area code/number standard.

Mapping can be applied to:

- origination endpoint
- termination endpoint
- both (in the same rule)

Custom maps help to address gateway functionality. Mapping can apply to special situations 'targets' such as IP phones. If a set of origination endpoints possess a non-conforming pattern, a custom maps can standardize them and guarantee that incoming and outgoing calls will work.

## Mapping By Endpoint Type

Let's look at the two basic types of mapping, origination and termination (whether or not both are mapped in a particular rule):

- **Origination Mapping.** Origination mapping is performed on DNIS/ANI after authentication and before routing in order for routing to be enabled. For instance, it will remove the international code dialed to reach international destinations.

Origination mapping will strip out a prefix on a default basis. The VoiceMaster then does the following:

Searches for a map (rule) to translate the number.

Locates country, billing rate, route and termination endpoint

Practically, a custom map modifies the patterns, replacing the first pattern identified by the rule with its assigned replacement string. Here is an example:

123 = 789.

The rule is created and applied to the origination number in the knowledge that ‘123’ does not conform to the standard. Each time the system sees ‘123’ in the originating call, it replaces that string with ‘789’, meeting the E.164 standard and triggering call routing.

- **Termination Mapping.** Specifies sets of rules that the VoIP Platform gatekeeper uses for phone number transformations when the gatekeeper is acting as a termination gatekeeper. Termination providers expect that the VoIP service provider will supply the append/default translation (prefix stripping).

## Custom Maps Configuration

As with most VoiceMaster modules, the primary Administrator activities are creating (adding) and editing rules and policies. Custom Maps Edit menu options are:

- Add Custom Map. Create a new map with translation rules. Filter by call authentication type, and map type (origination, termination, both).
- Modify Custom Map. Change the individual settings for any of the rule-defining parameters.
- Delete Custom Map. Remove a map from the Custom Maps stock.
- Display Search Box. (search for a particular map)

### Add Custom Map

To add (create) a Custom Map, do the following:

- Step 1** At the Navigator view, select **Custom Modules>Custom Maps**.
- Step 2** Select **Edit>Add Custom Map**. The following dialog is displayed:



**Figure 1-221Add Custom Map Dialog**

- Step 3** Assign a name to the new rule by typing an appropriate name in the ‘Name’ text box. This name should identify the map’s purpose in some way so you can associate it easily with its role for future modifications.

- Step 4** Assign an IP address. Sets the IP address for the map (this becomes relevant if ‘IP Address’ is the filter type selected in Step 9 below).
- Step 5** Set ZIP code. If assigned, can be used as rule filter.
- Step 6** Set the Called Number Pattern. Enter the target DNIS prefix for the call destination number
- Step 7** Assign the Calling Number Pattern. Enter the ANI number pattern for the calling station for this rule.
- Step 8** Define the Origination Map. Here you establish the rules for translating the originating call string. For instance, entering:
- 00=;0=52  
(where ‘00’ is the default)
- tells the system to strip “00” from numbers with that starting pattern, and replace any number starting with 0 with the number 52.
- Step 9** Define the Termination Map. Set rules for replacing termination strings to conform to the standard. For instance, a pattern can be created to automatically add a prefix before a pound sign, such as:
- =789#;  
(adds the prefix 789 at the termination endpoint)(all rules end with the ;)

---

**Note** The actions specified in the Origination and Termination map fields are not enabled unless its type is selected in the Map Type field (see below).

You can also select existing Gateways and open the Edit dialog to view entries in the Origination and Termination map fields. These will give you an idea of formats used.

---

- Step 10** Add a filter to the rule. The filter chosen specifies the type of authentication. Some filters are ‘single parameter only’ while other assign multiple authentication methods to a rule. (Naturally, authentication combinations filter a specific Custom Map (rule) more thoroughly than a single method.)
- Assign a filter:
- Select the Down Arrow next to the Filter by text box
  - Select one filter (whether single or multiple authentication method)
  - The filter list closes automatically on selection and the choice is displayed in the Filter By text box.
- Available Custom Map filters are:
- IP Address only. Sets the map to apply to the IP address specified in Step 4 above. Failure to perform Step 4 will render this filter inactive.
  - ANI only. When selected, only Calling Number Pattern need be defined (Step 7 above) for map rule to take effect. (Calling number pattern is checked and translated when this filter is set.)

- DNIS Only. Filters the rule by the Called Number Pattern established in the associated field above (Step 6). If this filter is chosen, the rule checks this pattern and performs translation before routing.
  - DNIS and IP Address. Filters the rule by these two parameters; they must be configured above (IP Address and Called Number Pattern fields) for the filter to work.
  - ANI and IP address. Filters by previously defined ANI (Calling Number Pattern) and assigned IP address.
  - ANI and DNIS. Filters by both called and calling number patterns, DNIS and ANI respectively. If both have been specified, rule performs mapping accordingly.
  - ANI and DNIS and IP Address. All three fields must be defined when this filter is selected in order for rule to be applied.
  - ZIP only. Filters only by defined ZIP code.
  - DNIS and ZIP. Filters by called number pattern and ZIP code.
  - ANI and ZIP. Filters by calling pattern and ZIP.
- Map Type: Sets the mapping that will be performed by the rule's application:
    - Origination Map. Select this to 'tell' the Custom Map to translate only the Origination Map pattern (this field must be defined for the rule to work when Origination is the map type selected).
    - Termination Map – Instructs the rule to act on the termination map, which must be defined above if this type is selected (or rule will not be enforced).
    - Both. Patterns in both Origination and Termination Map fields are translated when the rule is applied; therefore, both kinds of maps must be defined prior to selecting 'Both as the Custom Map (map) type.

### Modify Custom Maps

To modify an existing custom map (and change any of its parameters, map definitions, filters, etc.), take these actions:

- Step 1** At the Navigator view, select **Custom Modules>Custom Maps**. View Custom Maps rules.
- Step 2** Select the specific map from the list that you wish to modify.
- Step 3** Choose **Edit>Modify Custom Map** to open the edit dialog:



**Figure 1-222Custom Map Modification**

**Step 4** Change any of the following:

- (a) Called and/or called number patterns
- (b) Origination and/or termination map definitions
- (c) Filter type
- (d) Map type

**Step 5** Select **Apply**. The modified contents are saved and enforced whenever the rule is applied.

#### Delete Custom Map

To delete a custom map:

- Step 1** At the Navigator view, select **Custom Modules>Custom Maps**. The Custom Maps list is opened.
- Step 2** Select the specific map that you wish to delete.
- Step 3** Select **Edit>Delete Custom Map**.
- Step 4** Confirm **OK** at the prompt to execute the deletion, or select **Cancel** to nullify it and leave the selected map and its associated rules intact.

## Custom Prompts Module

The Custom Prompts modules facilitates customization of reseller prompt language rules. By adding new language rules the Administrator can specify the language prompt type to apply to a given reseller batch.

There are four prompt types:

- Default
- Welcome Message

- Enter Card Number
- Enter Destination Number

The Custom Prompts module lets the Administrator change the default prompt for particular customers at will. When the new rule is created and assigned to a reseller batch (for instance), VoiceMaster generates and assigns the custom prompt to the specified customers (associated with the new rule).

After a custom prompt ID has been created, gateway(s) must be configured to recognize the newly generated and assigned custom prompt ID.

The next time a rule-associated end user calls in the system greets with the new prompt specified.

## Uploading Audio Files

Because of the special character and purpose of this module, an additional step is needed beyond configuring the rule. This involved recording the new message (in the desired language), saving it as a file and uploading it to the IVR server so that the origination gateway can play it when customers tied to a Custom Prompts rule initiate calls.

Here is the overall Administrator task when creating Custom Prompts rules:

- Record a new 8 khz .au/.wav file containing the message in the desired language.

---

**Note** File formats depend on the gateway vendor used. Cisco gateways use .au, Quintum employs .wav files, while SysMaster gateways can accommodate both.

---

- Upload the new .au/.wav file to the IVR Server.

---

**Note** VoiceMaster supports audio customization for virtually all languages. An Administrator can record and upload messages the IVR servers. They are stored as .au/.wav files.

---

- Create a Reseller Prompt Language Rule and apply it.

Part of configuring the new rule is assigning it an ID. The uploaded audio file should include this ID as its extension. The file should be in the form of **fr/filename\_10.au** where **fr** is the name of the directory containing audio file in French and **10** is the ID assigned to the rule at the Add Language Rule dialog used to configure it.

---

**Note** If you have already created the audio file to apply to the newly created rule, make sure its extension matches the rule ID.

---

Procedural instructions on creating and uploading audio files is described in [Replacing or Adding Audio Files](#) in the configuration section that follows. Refer to SysMaster technical support for more details on audio files and their formats.

## Custom Prompts Configuration

Custom Prompts Edit menu options are:

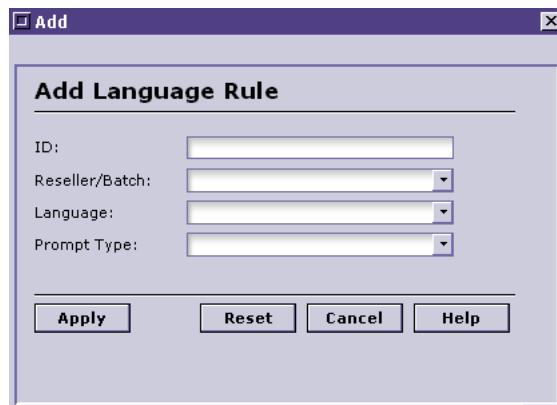
- Add Reseller Prompt. The option selected to configure a new Custom Prompts rule.

- Edit Reseller Prompt. Select to modify an existing rule.
- Delete Reseller Prompt. Delete a rule that is no longer relevant.

### Add Reseller Prompt

To configure a new Custom Prompt, follow these instructions:

- Step 1** At the Navigator view, select **Custom Modules>Custom Prompts**.
- Step 2** Select **Edit>Add Reseller Prompt**. View the Add Language Rule dialog:



**Figure 1-223Add Reseller Prompt Dialog**

- Step 3** Assign the ID for the new custom prompt (this ID should match that of the voice file uploaded to the IVR server). This ID for the rule is automatically generated.
- Step 4** Choose a Reseller/Batch to associate with the rule. Open the Reseller/Batch pull-down menu and choose the specific Reseller Batch.
- Step 5** Select a language for the new prompt. Again, open the pulldown menu next to ‘Language’ and select the desired language from the list of available languages.
- Step 6** Choose a Prompt Type. Open the menu and select from:
- Default
  - Welcome Message
  - Enter Card Number
  - Enter Destination Number
  - Custom Ring-Tone

---

**Note** Selecting a Prompt Type triggers the desired message type when users associated with the rule call in to a gateway to attempt a call.

---

- Step 7** Select Apply. The new Custom Prompt is added to the Custom Prompts list.

### Replacing or Adding Audio Files

To implement a new Custom Prompts rule, you must also record and upload the associated audio file containing the desired message in the new language. To do this:

- Step 1** Record new voice prompt files. (Audio files must be recorded and saved in mLAW 8000 Hz mono Nex / Sun format with wav or au headers)
- Step 2** Connect to VoiceMaster via an SSH client.
- Step 3** Login as :  
Username: manager  
Password: managerXXXXXX (where XXXXX is the Serial Number of the unit)
- Step 4** Navigate to the **upload/ivr** directory. (See Appendix \_\_ [Common VoiceMaster OS Commands]**check this**)
- Step 5** Upload the voice prompt file to the desired directory.

### Edit Reseller Prompt

To edit an existing Custom Prompts rule, follow these instructions:

- Step 1** At the Navigator view, select **Custom Modules>Custom Prompts**.
- Step 2** Select the Custom Prompts rule you wish to modify.
- Step 3** Open **Edit>Edit Reseller Prompt**. View the associated dialog:



**Figure 1-224Edit Reseller Prompt Dialog**

- Step 4** Change any of rule parameters - ID, Reseller/Batch, Language or Prompt Type.
- Step 5** **Apply** to confirm and save the settings.

### Delete Reseller Prompt

To remove any currently active Reseller Prompts:

- Step 1** At the Navigator view, select **Custom Modules>Custom Prompts**.
- Step 2** Select the Custom Prompts rule you wish to delete.
- Step 3** Select **Edit>Delete Reseller Prompt**.
- Step 4** Confirm **OK** or cancel the deletion.

- Step 5** The confirmed deletion removes the specified Custom Prompt rule from the Custom Prompts list.

**Note** Whenever a Custom Prompt is deleted from the database, the language its assigned customers hear will be the gateway's default message, defined when IVR is first configured for that gateway.

## Custom Service Plans Module

The Custom Service Plans module lets an Administrator assign special billing charges to clients and their associated VoIP calling plan users. Flexible Custom Service plans can be configured for groups of users to meet particular calling needs and expectations.

The module functionality depends on assignment of different kinds of *flat charges* to customers. The various flat charges can be defined by different time slices - monthly, weekly, daily and hourly charges. The Administrator can fix as many as desired to apply to the specified customer batches.

In addition, charges can be fixed by percentage. A one-time charge may also be applied to all customers governed by a Custom Plan, so they are charged a defined amount upon call connection. The more flat charges assigned to a particular rule, the greater the costs for customers.

**Note** Custom Service Plans can be employed in conjunction with the Calling Plans module. If you have implemented the Calling Plan module and assigned free time to specific clients/users, they will not be billed for calls during specified Call Plan Intervals (applied to those same clients/users).

## Custom Service Plans Configuration

Configuring Custom Service Plans is facilitated by the Custom Service Plans edit options, which include:

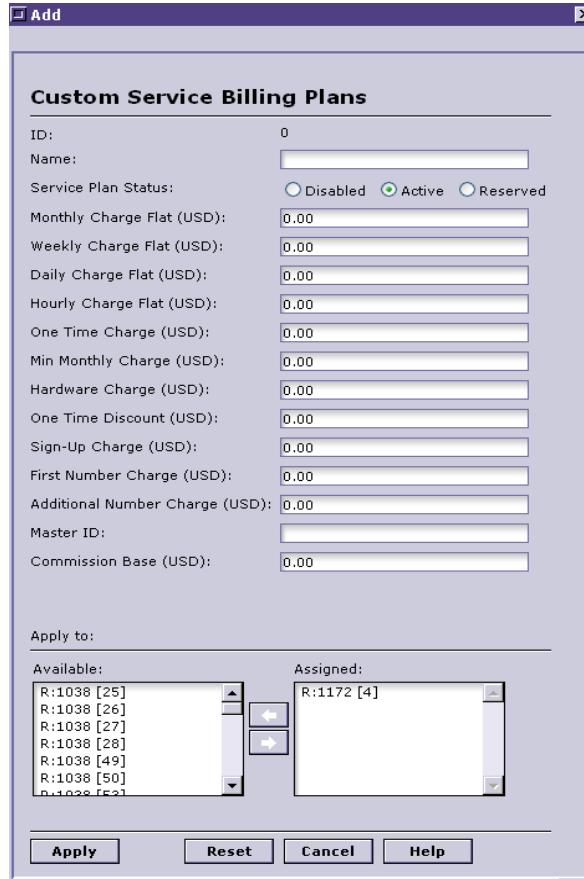
- Add Plan
- Modify Plan
- Delete Plan

Each of these basic Administrative actions is explained in its own section, starting with creating (adding) a new Custom Service Plan.

### Add Custom Service Plan

To add a new Custom Service Plan, do the following:

- Step 1** At the Navigator view, select **Custom Modules>Custom Service Plans**.
- Step 2** Select **Edit>Add Plan**. View the Custom Service Billing Plans dialog:

**Figure 1-225Adding a Custom Service Billing Plan**

- Step 3** Choose a plan name that you can associate with the plan's contents, purpose, etc.
- Step 4** Set Service Plan status. Choose one of these options:
- Disabled. Disables the new plan (the plan is still saved and available for future use).
  - Active. Immediately activates the configured plan and applies it to designated Reseller/Corporate batches.
  - Reserved. This status is applied to pre-paid users to place an absolute limit on the dollar amount of calls per month. When selected, applies the monthly charge against his account balance. (If a calling card customer has a monthly limit of \$20 and a Custom Plan assigns him \$10 per month, he is permitted \$10 for the month.)
- Step 5** Assign any/all available charges:
- Monthly Charge Flat. Flat monthly charge to apply to the plan (if assigned).
  - Weekly Charge Flat. Flat weekly charge.
  - Daily Charge Flat. Daily charge to apply to applied batches.
  - Hourly Charge Flat. (Flat hourly charge)
  - One time charge. Assigns a one-time charge to each call, on connection.

- Min Monthly Charge. Minimum amount to be charged to batches regardless of usage.
- Hardware Charge. Fee assigned affected customers for use of network hardware.
- One Time Discount. A ‘one-off’ discount assigned to batches, mitigating other charges.
- Sign-up Charge. Fee levied for batch-defined users when joining the VoIP service.
- First Number Charge
- Additional Number Charge

Then assign these additional parameters:

- Master ID. This is the Account Id of a Reseller or Corporate account.
- Commission Base. Assigns a commission percentage for the monthly revenue from the plan to an agent who has referred customers assigned to it.

- Step 6** Assign any desired Reseller Batches to the rule.
- Step 7** Repeat this for any Corporate Batches you wish to assign to the new plan.
- Step 8** Select **Apply** to save the plan. (If you set its status to Active in Step 4 above it takes effect immediately for the assigned batches.)

### Modify Custom Service Plan

It may be appropriate to modify an existing Customer Service Plan for any number of reasons. You may want to change a plan’s status, change its cost structure by editing individual charges, or change the current assignment of client (Reseller/Corporate) batches to the plan.

To modify an existing Custom Service Plan, perform these actions:

- Step 1** At the Navigator view, select **Custom Modules>Custom Service Plans**.
- Step 2** Select the Custom Plan that you wish to modify from the Custom Service Plans List.
- Step 3** Select **Edit>Modify Plan**. The following dialog appears:



**Figure 1-226**Modifying a Custom Service Plan

**Step 4** Edit any aspect of the Custom Service plan:

- Plan Status
- Charges (flat or percentage)
- Master ID
- Commission Base
- Assign or remove reseller or corporate batches.

**Step 5** Select **Apply** to enforce the edits (modifications).

#### Delete Custom Service Plan

To delete a custom service plan (and reconfigure default billing rates for those Reseller/Corporate batches assigned to it), do the following:

- Step 1** At the Navigator view, select **Custom Modules>Custom Service Plans**.
- Step 2** Select the Custom Plan that you wish to delete from the Custom Service Plans List.
- Step 3** Select **Edit>Delete Plan**.
- Step 4** Confirm to delete or cancel to abort the plan deletion.

# Custom Tax Module

The Custom Tax module enables the configuration, or levying, of additional taxes on selected clients. These can include all available resellers, wholesalers and active individual users (customers) of your VoIP service.

One of the main uses of the Custom Tax module is to satisfy the legal tax requirements on a local, national or international basis. Taxes may be required for particular clients on different bases, depending on their locations and the applicable laws (which can be, again, local, national or international [tariffs, for instance]).

The geography of custom tax configuration can be as specific as you want to make it. It's possible to set a specific zip code for the individual tax rule to govern.

---

**Note** It is helpful to research tax rules and regulations governing service areas. This will aid in tracking billing expenses and covering these additional fees that may be applied to calls.

---

You can configure these tax types:

- Sales Tax
- Service Tax
- Outstanding Balance Tax
- Special Tax
- Value Added Tax

A Custom Tax rule is specified either as US dollar amount or as a percentage number. It is calculated only after a call is complete and is applied once per billing assigned period.

Two types of billing periods exist:

- Every Week
- Every Month

## Custom Tax Configuration

Configuring Custom Tax rules relies on the standard Edit menu options and the dialog functions that their selection spawns:

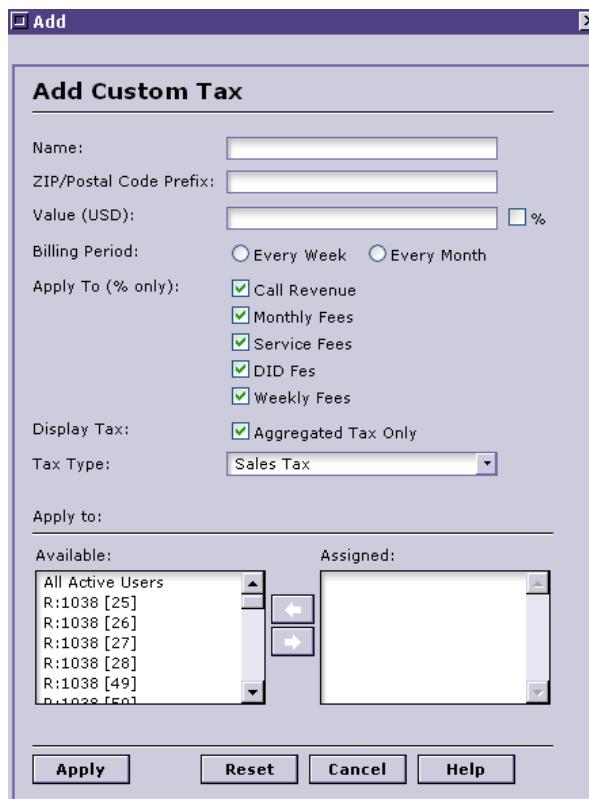
- Add Custom Tax. Lets you configure a new Custom Tax rule and apply it to a selected user set.
- Edit Custom Tax. For modifying existing Custom Tax rules.
- Delete Custom Tax. Used to delete existing rules that are no longer relevant.

### Add Custom Tax

To create a new Custom Tax policy:

**Step 1** From the Navigator view, select **Custom Modules>Custom Tax**.

**Step 2** Select **Edit>Add Custom Tax**. The Add Custom Tax dialog is displayed:



**Figure 1-227Adding a Custom Tax**

**Step 3** Name the new Custom Tax rule.

**Step 4** Define a ZIP/postal code.

**Step 5** Set a value (amount) for the tax or set a percentage of overall call cost).

---

**Note** This is a base value, a generic amount that only gains relevance once you assign to different revenues and/or fees (see Step 7).

---

**Step 6** Set the billing period (weekly or monthly).

**Step 7** Apply the tax to one ore more of the revenue/fee options:

- Call Revenue
- Monthly Fees
- Service Fees
- DID Fees
- Weekly Fees

---

**Note** The preceding options are default-selected. Uncheck any parameter to disable for this particular rule.

---

**Step 8** Choose to display the (aggregated) tax (Display Tax is default-selected). Uncheck the box to hide the tax during billing.

**Step 9** Select a Tax Type from the pulldown in the next field. Options are: Sales Tax, Service Tax, Outstanding Balance Tax, Special Tax and Value Added Tax.

---

**Note** Tax type reflects legal requirements for call areas governed by the rule.

---

**Step 10** Assign the client batches (or individual users) whose calls will be taxed according to the rule's assigned parameters.

**Step 11** Select **Apply**. The new rule is added to the Custom Tax list.

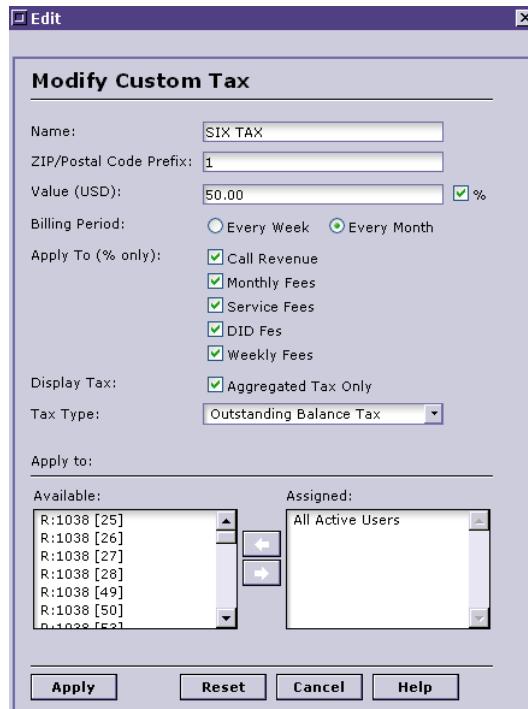
### Edit Custom Tax

You can configure any existing Custom Tax rule by doing the following:

**Step 1** From the Navigator, select **Custom Modules>Custom Tax**.

**Step 2** Select the Custom Tax rule from the Custom Tax list that you intend to edit.

**Step 3** Select **Edit>Edit Custom Tax**, and the edit dialog is displayed:



**Figure 1-228**Modifying a Custom Tax Rule

**Step 4** Modify any aspect of the rule.

**Step 5** Select **Apply**; the modified rule is saved.

### Delete Custom Tax

To delete a Custom Tax rule:

**Step 1** From the Navigator, select **Custom Modules>Custom Tax**.

**Step 2** Select the Custom Tax rule to delete from the Custom Tax list displayed.

**Step 3** Select **Edit>Delete Custom Tax**. Confirm **OK** to delete or Cancel to abort the action. Deleted rules are removed from the list.

## Discount Credit Time Module

When users call in to a gateway to establish a VoIP connection, they are typically informed of available call time. The system authenticates the customer, then informs him of available call time remaining.

**Note** The Discount Credit Time module can be used for calling card customers who are allotted ‘global’ calling time amounts. Every time such a customer originates a call, the system calculates call time based on remaining dollar amount and rates per minute to the intended destination.

Using the functionality of the Discount Credit Time module, this ‘time remaining’ message can be changed. Additionally, the module permits an Administrator to reduce or increase actual call time by configuring ‘time remaining until disconnect’ (in effect).

The Administrator can divide announced and actual call time one of two ways:

- increase the IVR message announcement time
- decrease the disconnect time (shorten the time before affected calls are disconnected).

By separating announced and functional time so the latter is less than the former, customers increase call initiation frequency. This boosts initial connection charges and offsets revenue lost through technology and other costs.

### Official Time and Manager Time

The Discount Credit Time Module operates against the background of basic system time definitions.

- **Official Calling Time.** This is the default calling time reported to the user through the IVR (it assumes that IVR is implemented on relevant origination gateways). Official time is calculated based on card dollar amount remaining and base call costs. Note that this Official Calling Time can include taxes and other fixed charges. Calls that exceed the official calling time are typically capped when billing is first configured.
- **Manager Time.** An arbitrary block of time added or subtracted to the official time. When configured, it is reflected in the time announced to the user by the IVR. See the online Help for more information.
- **DISC Time (Disconnect Calling Time).** Actual calling time that the system permits. Once a specific disconnect time is set, this overrides official time.
- **IVR Time.** The reported available calling time announced to the user through the IVR. Official time plus manager time = IVR time.

## Discount Credit Time Configuration

Configuring Discount Credit Time is facilitated by the module-associated Edit menu options:

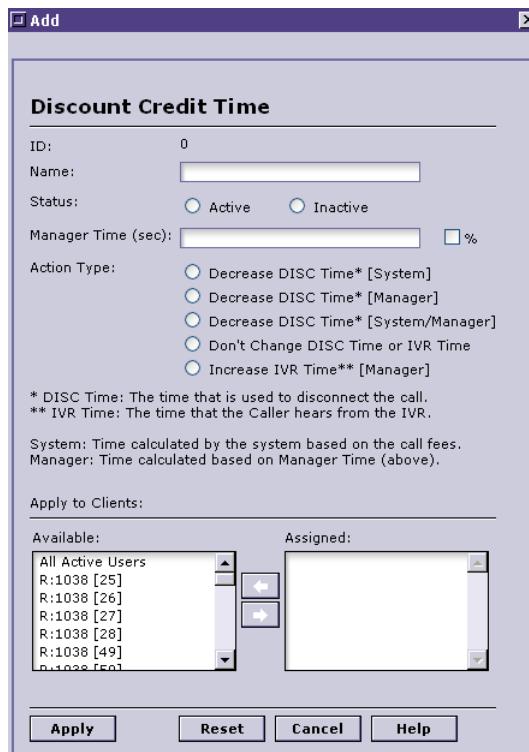
- Add Discount Credit Time Rule. Create a new policy for designated clients/users.
- Edit Discount Credit Time Rule. Modify an existing rule.
- Assign Area Codes. Assign the area codes to apply to the rule.

- Delete Discount Credit Time Rule. Delete an existing Discount Credit Time rule.

### Add Discount Credit Time Rule

To add a new Discount Credit Time rule, carry out these steps:

- Step 1** Select **Custom Modules>Discount Credit Time** at the Navigator view. The Discount Credit Time list with existing rules is displayed.
- Step 2** Select **Edit>Add Discount Credit Time Rule**. The Discount Credit Time dialog appears.



**Figure 1-229Adding a Discount Credit Time Rule**

- Step 3** Assign a rule name, preferably one that you can associate with its parameters or assigned clients (or both).
- Step 4** Set the status to Active or Inactive to trigger rule activation or reserve it for later use.
- Step 5** Set the manager time, if any, to decrease the official time.

Manager time can be set in one of two measures:

- In seconds (fixed value)
- In percentage (of official time)

---

**Note** To apply manager time settings made here, choose either Decrease DISC Time [Manager] or Increase IVR Time [Manager] as the designated *Action Type*.

---

- Step 6** Select an Action Type:

- **Decrease DISC Time [System]**. Configures a decrease in ‘talk time’ by setting a disconnect time to override official system time settings.
- **Decrease DISC Time [Manager]**. Decreases calling time based on the value or percentage entered in the Manager Time field above.
- **Decrease DISC Time [System/Manager]**. Calculates the disconnect time by choosing the smaller of the two values – system (official) or manager (if set above).
- **Don’t Change DISC Time or IVR Time**. System time announced to the caller is the default when this is the selected action type. (Announced time is accurate.)
- **Increase IVR Time [Manager]**. Increases IVR time based on the value or percentage of the Manager time entry in Step 5.

---

**Note** Administrators can check all call parameters using the Call Calculator report.

---

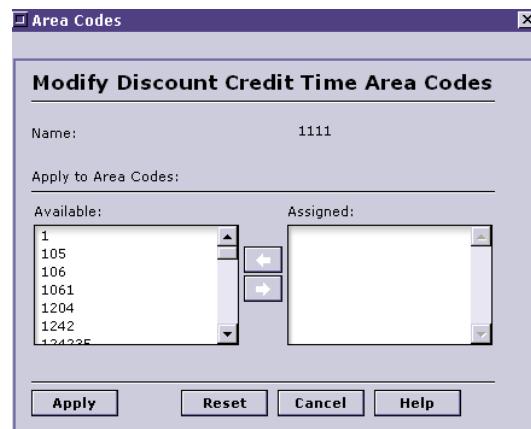
- Step 7** Apply the rule to specified clients by selecting and moving them from the Available to the Assigned window.
- Step 8** Select **Apply** to confirm the settings and save the rule. It is added to the Discount Credit Time list.

---

**Note** One more step must be performed to apply the new Discount Credit Time rule: applying area codes.

---

- Step 9** To apply area codes to pertain to the rule:
- (a) Select the rule just created from the list.
  - (b) Select **Edit>Assign Area Codes**. View the dialog:



**Figure 1-230**Assigning Area Codes

- (c) Select Area Codes from the Available window and move them to Assigned to apply them to the rule.
- (d) Select **Apply**.

Congratulations! The new rule is now configured. If set to active status, it takes affect, applying to designated clients and users for the assigned area codes.

### Edit Discount Credit Time Rule

To edit an existing Discount Credit Time Rule, perform these actions:

- Step 1** At the Navigator view, select **Custom Modules>Discount Credit Time**.
- Step 2** From the Discount Credit Time list, select the rule that you wish to modify.
- Step 3** Select **Edit>Edit Discount Credit Time Rule**.
- Step 4** Change entries for any parameters or fields within parameters:
  - Rule name
  - Rule status
  - Manager Time
  - Action Type
  - Assigned Clients
- Step 5** Select **Apply** to enforce the changes. The dialog closes.
- Step 6** To change any area code assignments:
  - (a) select the same rule from the Discount Credit Time list.
  - (b) Select **Edit>Assign Area Codes**. When the dialog appears, assign available area codes or remove currently assigned codes.
  - (c) **Apply** confirms the area code edits and completes the rule modification changes.

---

**Note** Step 6 is optional when modifying Discount Credit Time rules. Applying rule modifications in Step 5 above enforces parameter changes made in Step 4.

---

### Delete Discount Credit Time Rule

To delete any existing Discount Credit Time rule:

- Step 1** At the Navigator view, select **Custom Modules>Discount Credit Time**.
- Step 2** From the Discount Credit Time list, select the rule that you wish to delete.
- Step 3** Select **Edit>Delete Discount Credit Time Rule**.
- Step 4** Confirm the deletion at the prompt (OK), or cancel to abort.

---

**Note** Rules whose deletion you confirm are removed from the list. Previous configuration settings for the affected clients/users are reinforced.

---

## Exception Numbers Module

The Exception Numbers module lets the Administrator define specific numbers - ‘exception numbers’ - for special treatment. Specific and responsive policy actions are triggered when calls are attempted from such numbers.

**Note** Exception Numbers functionality also works in conjunction with the Fraud Detection module. Although VoIP service providers do not need the Fraud Detection module to implement the Exception Numbers module, the Fraud Detection functionality does depend on the presence of Exception Numbers.

---

Some Exception Numbers functions (like Special Services options) may also be used by customers who have implemented SysMaster's Norfa package. These options are thus relevant in both a standard VoiceMaster context *and* for Norfa.

Exception Numbers module acts on a specified Exception Number type (DNIS, ANI, destination number or customer service number) or prefix type, setting actions for calls to or from the number.

Action types can include:

- **Drop Call.** Specifies that the system will drop calls that match the exception number.
- **Accept Call & Bill.** Accepts calls for the number designated, then bills normally.
- **Toll-Free Call.** Allows the call but does not charge the user.
- **Detect Fraud w/o Block.** Configures the system to record fraud attempts originating from the specified number. Records the fraud attempt in report form (**Event Monitoring>Reports>System Reports>Fraud Detection**). Does not take any policy action in response to the observed attempt.
- **Detect Fraud with Block** Blocks fraud from the number, and logs the attempt under **Event Monitoring>Reports > Administrative > Messages > Fraud Detection**.

**Note** See the section on Security in [Chapter Four: VoiceMaster Administration](#), for more on the related Fraud Detection functionality.

---

- **Record Line Access.** Selecting this action type records any call attempts that match the configured rule. All recorded (rule-matching) instances are logged. This and related action types are useful for law enforcement to track potential violations of the law that might be associated with VoIP activity.

## Exception Numbers Configuration

Configurations of Exception Numbers module rules involves the standard Edit menu options:

- Add Exception Number. Build a new Exception Numbers rule.
- Edit Exception Number. Modify an existing Exception Numbers rule.
- Delete Exception Number. Delete an existing rule.
- Display List. Reorder Exception Numbers list alphabetically by action type.

### Add Exception Numbers Rule

To create a new Exception Numbers rule, follow these steps:

**Step 1** From the Navigator View, select **Custom Modules>Exception Numbers**:

**Step 2** Select **Edit>Add Exception Number** and view the dialog:

The screenshot shows a software interface titled 'Add' at the top. Below it is a section titled 'Exception Number Management'. There is a text input field labeled 'Exception Number:' followed by a dropdown menu. Below this are several groups of labels and checkboxes:

- DNIS (Gateway Station ID) Number:
- ANI (Caller ID) Number:
- DESTINATION (Called Station ID) Number:
- Customer Service Number:
- Group Prefix:
- Local Prefix:
- Toll Free (800,888,877,866) Prefix:
- Toll Local Prefix:
- International Prefix:
- Operator Assisted Prefix:
- Directory Assistance Prefix:
- Special Services I (700 Number) Prefix:
- Special Services II (776 Number) Prefix:
- Premium Services I (900 Number) Prefix:
- Premium Services II (976 Number) Prefix:
- Casual 1010XXX Prefix:
- Internet Dialing Prefix:

**Figure 1-231 Add Exception Number Rule**

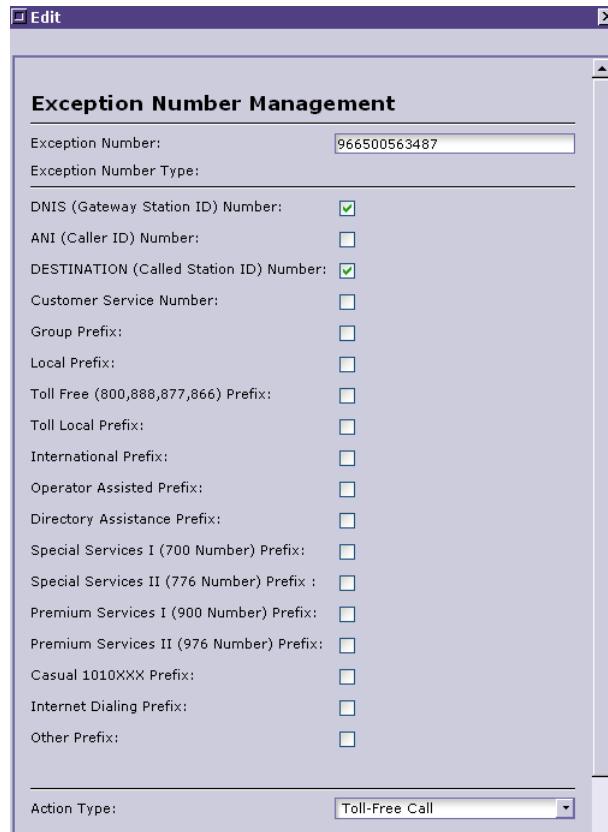
- Step 3** In the Exception Number text box, enter the number to which the rule will apply.
- Step 4** Check the box corresponding to the correct number or prefix type.
- Step 5** Select the Action Type to apply to the number. Select the pull-down menu arrow and view the available options:
  - (a) Drop call. Tells the system to drop calls to or from the defined number.
  - (b) Accept Call & Bill. Accept calls that reference the Exception Number, but bill them.
  - (c) Toll-Free Call. Accept the calls and do not bill.
  - (d) Detect Fraud w/o Block. Trigger detection and reporting, as explained in the Module overview section above.
  - (e) Detect Fraud with Block. Detect fraud pertaining to the number, log it and take the action specified in Fraud Detection module settings, if any. Will also trigger Administrator Email notification if this option is set in the System Alerts dialog.
  - (f) Record Line Access. Records all access attempts for the number; logs them. Takes no further action.
- Step 6** Apply the rule to designated clients that you move from Available to Assigned status.
- Step 7** Select **Apply** to save the rule and enforce it. The rule is added to the list.

### Edit Exception Numbers Rule

To edit an existing Exception Number rule, follow this procedure:

- Step 1** From the Navigator View, select **Custom Modules>Exception Numbers**.
- Step 2** View the Exception Numbers list (Figure 22) and select the rule you wish to edit.

**Step 3** Select **Edit>Edit Exception Number** and open its Edit dialog:



**Figure 1-232** By the (Exception) Numbers

**Step 4** Change any parameter desired: number/prefix type, action type or assigned clients.

**Step 5** Select **Apply** to save changes.

### Delete Exception Numbers Rule

To delete an existing rule:

**Step 1** From the Navigator View, select **Custom Modules>Exception Numbers**.

**Step 2** Select the rule to delete from the list.

**Step 3** Select **Edit>Delete Exception Number**.

**Step 4** Confirm the deletion or cancel to abort. On confirmation the rule is deleted and its instance removed from the Exception Numbers list.

### Display List

Display List is a selection state that alternates ('toggles') with Display Search Box. It allows the Administrator to filter a search for exception numbers by typing in a string. All numbers that start with this string are then displayed (and *only* these numbers).

# Flag Fall Billing Module

The Flag Fall Billing module facilitates the configuration of additional charges for calls associated with specific, selected clients. The Administrator exploits module functionality to specify a flag fall rule to apply for a specified time interval, referred to as Call Progress Time.

The Administrator can then apply additional charges to that interval. An example is a Sample Flag Fall charge that recurs during the Call Progress Time interval. When the call exceeds interval time, Flag Fall charges no longer apply to the assigned users.

---

**Note** Any part of a call before or after the interval itself is not charged recurring charges (such as Sample Flag Fall) that are tied to the interval itself.

---

By setting Call Time and Per Call adjustments, you assign additional editable charges. Alternately, apply an additional initial charge, then use the Per Call adjustment fields to apply arbitrary markup and profit charges - or apply a discount when it fits the situation.

Here is an example of a Flag Fall billing configuration:

Example:

A user is to be charged a recurring flagfall of 10 (ten) US cents for every two (2) minutes of the call until the user reaches a talking time of 10 minutes. The FlagFall rule is to be applied after the third (3) minute of the call.

FlagFall Rule Configuration:

**Call Progress Time:**

From: 180 sec To: 600 sec

Initial FlagFall Charge = 0

Sample FlagFall Charge = 10

Sample FlagFall Interval = 120

To properly configure a flagfall rule a number of adjustments must be specified. FlagFall adjustments could be grouped into two categories:

- Call Time Adjustments
- Per Call Adjustments

## Call Time Adjustments

Call Time Adjustments represent the main component of the flagfall module. Call Time Adjustments determine when and how the flagfall rule and associated charges are applied to calls. FlagFall call time adjustments are broken down into three distinct parameters:

- Initial FlagFall Charge. Specifies the initial flagfall billing amount applied at the moment when the receiving party answers the call (calculated in US cents).
- Sample FlagFall Charge. Specifies the amount of the recurring charge applied to the flagfall rule. Sample FlagFall frequency is set by the value entered in the Sample FlagFall Interval field.
- Sample FlagFall Interval. Decides how frequently the Sample FlagFall Charge will occur during the rule interval (Call Progress Time).

## Per Call Adjustments

Per Call Adjustments are one time charges that can be specified in addition to standard charges:

- **Tech Markup (cents)** Specifies additional technology charge(s) (in US cents) added to compensate for infrastructure costs.
- **Profit (cents)** Sets an arbitrary profit amount per call. If billing configuration produces a profit amount less than this, profit is default-applied.
- **Other (cents)** Miscellaneous additional charges.
- **Discount (cents)** Specifies a discount, typically used in dealing with Reseller clients.

## Flag Fall Billing Configuration

Flag Fall billing has these Edit menu options:

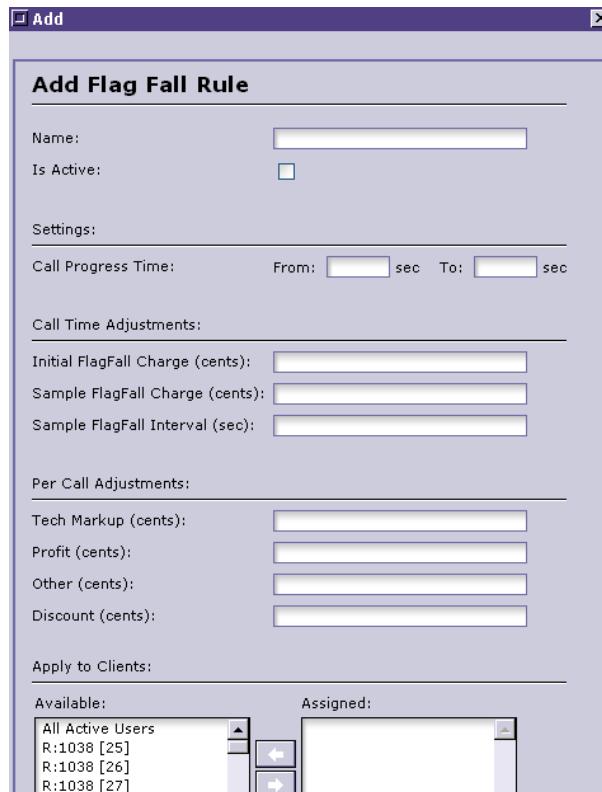
- Add Flag Fall Rule. Create a new Flag Fall rule.
- Edit Flag Fall Rule. Modify an existing rule.
- Delete Flag Fall Rule. Delete a rule.
- Assign Area Codes.

### Add Flag Fall Rule

To add a new Flag Fall rule, just execute these actions:

**Step 1** Select Custom Modules>Flag Fall Billing.

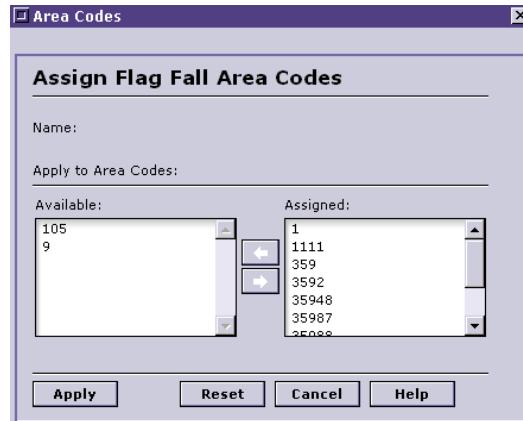
**Step 2** Select Edit>Add Flag Fall Rule. View the Add Flag Fall Rule dialog:



**Figure 1-233Add Flag Fall Rule**

**Step 3** Assign the rule a name.

- Step 4** Set the rule to active status or leave unchecked to activate at a later time.
- Step 5** Define the Call Progress Time by entering values in the ‘From’ and ‘To’ fields. This sets the total interval, in seconds, during which Sample Flag Fall Charge apply.
- Step 6** Set Call Time adjustments:
- Initial FlagFall charge. Specifies the one-time initial charge.
  - Sample FlagFall Charge. Specifies the recurring charge (in US cents) applied to calls during the call progress time.
  - Sample FlagFall Interval. Interval at which the Sample FlagFall charges is applied during Call Progress Time.
- Step 7** Set per call adjustments as desired - Tech Markup, Profit, Other or Discount.
- Step 8** Select clients as objects of the rule by moving them to the Assigned window.
- Step 9** Select **Apply** and changes made to this point are saved. The dialog is closed.
- Step 10** Assign Area Codes (final step):
  - (a) Select the new rule from the Flag Fall Billing list.
  - (b) Select **Edit>Assign Area Codes**.
  - (c) At the Assign Area Codes dialog, assign available codes.
  - (d) Select **Apply** to save and close the dialog.



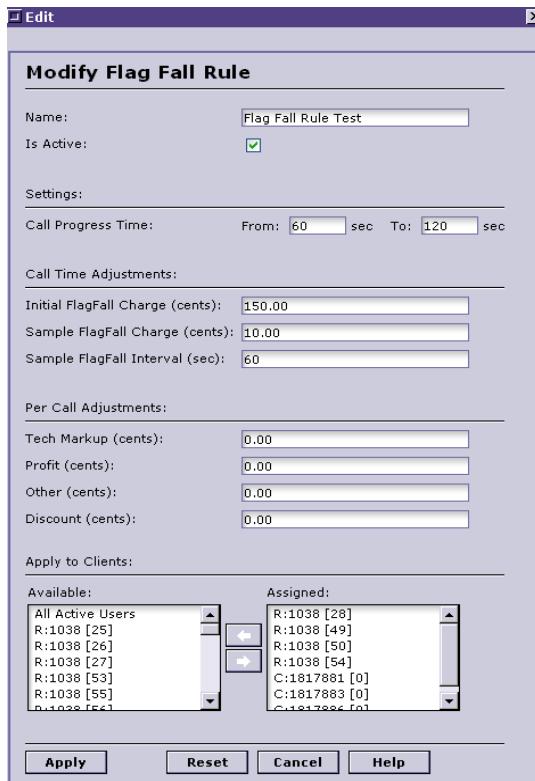
**Figure 1-234Assign Flag Fall Area Codes**

The new rule is now configured and ready to work if its status is *active*.

### Edit Flag Fall Rule

To edit an existing Flag Fall rule, follow this procedure:

- Step 1** Select **Custom Modules>Flag Fall Billing**.
- Step 2** Select the Flag Fall rule that you wish to edit.
- Step 3** Select **Edit>Edit Flag Fall Rule**, and the rule modification dialog appears:



**Figure 1-235 Modify Flag Fall Rule**

- Step 4** Change any parameters, from name and status to Call Progress Time and any desired Call Time or Per Call Adjustments.
- Step 5** Change any assigned clients by adding available clients to the Assigned box or removing currently assigned clients and returning them to the Available stock.
- Step 6** Select **Apply** to save changes.
- Step 7** If you want to change area code assignments:
  - (a) Reselect the rule from the Flag Fall Billing list.
  - (b) Select **Edit>Assign Area Codes**.
  - (c) At the Assign Area Codes dialog, select and move area codes from the Available to the Assigned window (or do the reverse for area codes no longer relevant to the rule).
  - (d) Select **Apply** to save and close the dialog.

The rule is now modified. Its configuration will reflect the last modifications made.

### Delete Flag Fall Rule

To delete a rule:

- Step 1** Select **Custom Modules>Flag Fall Billing**.
- Step 2** Select the Flag Fall rule that you wish to delete.
- Step 3** Choose **Edit>Delete Flag Fall Rule**.

**Step 4** Confirm the deletion, or cancel to leave it standing.

## Multi-Level Marketing Plans Module

The Multi-Level Marketing Plans module facilitates configuration of a fee/commission structure for VoIP customers and sales agents. ‘MLM’ is a unique marketing method for increasing customer subscriptions of users who can also profit by marketing the service to others. The pay-out structure provides an incentive to recruit, for as customers/agents ‘climb’ the levels of the plan.

---

**Note** MLM plans are tied to individual user accounts, so that specified amounts of the profit generated by such accounts are distributed among MLM agents, according to level.

---

The Multi-Level Marketing Plans module lets an Administrator set the fee/commission structures to attract customers and agents and encourage them to actively promote the VoIP service.

Module configuration functions let the Administrator configure each plan level individually, setting both fixed and commission rates for each level:

- Fixed rate payment. This can be set by the minute or per call.
  - Fixed per minute. Specifies a fixed commission rate in cents based on per-minute usage of the account the MLM management plan has been created for.
  - Fixed per call. Defines per call amount to be paid an agent when a user he has recruited uses the VoIP service.
- Commission payments. These can be tied to profit, revenue or set as a base amount:
  - None. No commission is paid out when this MLM-recruited account is used.
  - Profit. The commission paid to agents (by level) is a cut of the total profit per user account.
  - Revenue. The commission is paid, by level, according to the total revenue produced by VoIP accounts recruited through MLM.

A coherent MLM plan is designed around a sensible increase in fixed and commission payments to agents as they advance. Typically successful MLM plans are those that 1) provide an incentive to join and 2) remain a member (subscriber-agent). To achieve this, payouts should be boosted systematically from level to level.

The Administrator then refers to this pay structure when making periodic payments to plan participants by level. The ‘math’ becomes a function of level and individual productivity.

## MultiLevel Marketing Configuration

Multi-level Marketing Edit menu options are:

- Add MLM Plan
- Modify MLM Plan
- Delete MLM Plan

### Add MLM Plan

To create a new Multi-Level Marketing plan, take these actions:

**Step 1** At the Navigator View, select **Custom Modules>Multi-Level Marketing Plans**:

**Step 2** Select **Edit>Add MLM Plan** and view the MLM Management dialog:

The screenshot shows the 'Multi-Level Marketing (MLM) Management' dialog box. It includes four main sections: Level (MASTER), Level (RESELLER), Level 1, and Level 2. Each section has fields for Fixed Per Minute (cents), Fixed Per Call (cents), Commission (%), and Commission Base (radio buttons for None, Profit, Revenue, or Base). The 'None' option is selected for all levels.

**Figure 1-236Adding MLM Rule**

**Step 3** Assign a Master ID to the rule. Agent commissions are paid by association with the Master ID.

**Step 4** Assign a payout basis for Master level agents:

- (a) Assign Income per minute and per call
- (b) Assign a commission%, then choose a commission base type - Profit, Revenue or Base.

---

**Note** One of these must be set if the commission percentage is to apply. Setting the Base to 'None' disables the Commission payment.

---

**Step 5** Repeat Step 4 for the Reseller level, and for each of the levels beneath it. The Multi-Level Marketing model works best when agents on lower levels have real incentive to recruit new subscribers to the VoIP service.

- Step 6** Once you have assigned rates and commission bases for all plan levels, select **Apply** to save changes. The dialog box closes and the new plan is added to the list.

---

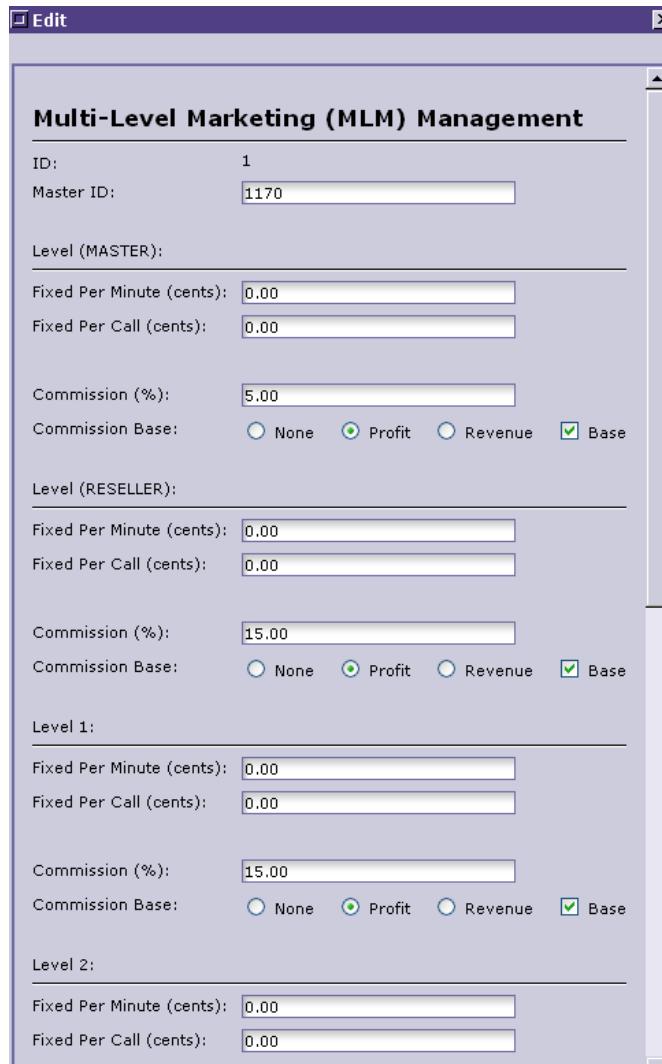
**Note** Plans apply to all subscriber accounts recruited by plan agents.

---

## Modify MLM Plan

To modify an existing MLM plan:

- Step 1** At the Navigator view, select **Custom Modules>Multi-Level Marketing Plans**.
- Step 2** Select the plan for the Multi-Level Marketing Plan list that you wish to edit.
- Step 3** Select **Edit>Modify MLM Plan** and the edit dialog appears:



**Figure 1-237**Editing an MLM Plan

- Step 4** Edit any existing levels, changing fixed or commission rates as desired.
- Step 5** Select **Apply** to save modifications and close the dialog.

## Delete MLM Plan

Do the following to delete any configured MLM plan:

- Step 1** At the Navigator View, select **Custom Modules>Multi-Level Marketing Plans**.
- Step 2** From the Multi-Level Marketing Plans list, select the plan you want to delete.
- Step 3** Select **Edit>Delete MLM Plan**.
- Step 4** Confirm **OK** at the prompt to delete, or cancel to abort the deletion.

---

**Note** All deleted MLM plans are removed from the Multi-Level Marketing Plans list, and their provisions are nullified.

---

# Progressive Billing Module

The Progressive Billing option lets an Administrator configure additional charges or discounts on calls associated with specific clients.

Specified progressive billing charges/discounts are based on a *per session time* value set at the Call Progress Time field. Charges set at the Call Time Adjustment and Per Call Adjustment fields apply to designated calls within the time interval. The rule's rates override any default rates for the interval set within the Call Progress Time field.

The Progressive Billing module adds impressive flexibility to an Administrator's ability to custom-configure rates for clients and users who fit certain profiles and use patterns.

Progressive Billing charges fit one of two categories:

- **Call Time Adjustments:**
  - **Delta Init Charge.** Assigns a one-time additional charge when clients assigned to the rule initiate a call to assigned area codes.
  - **Delta Sample Rate.** Specifies an additional (delta) charge during the Call Progress Time portion of calls. The Delta Sample Rate charge, like the Delta Init Charge, can be calculated as a percentage of the pre-defined Sample Rate
- **Per Call Adjustments (optional):**
  - **Tech Markup.** One-time charge to offset technology infrastructure and related costs.
  - **Profit.** Minimum profit applied to any calls that fall within a rule.
  - **Other.** Miscellaneous charges.
  - **Discount.** Special discount, mostly for Reseller clients.

---

**Note** In the case of overlapping progressive billing policies, the policy with the smallest call progress time interval has precedence over all other progressive billing rules.

---

Here is an example of a Progressive Billing rule.

Example:

The following progressive billing rules could be applied in order users to be encouraged to talk more at lower rates.

Base Sample Rate = 10 cents per 60 secs (1 minute)

Progress Billing Rule 1

Call Progress Time: 0-5 (min)

Delta Sample Rate: 10 (cents)

Progress Billing Rule 2

Call Progress Time: 0-10 (min)

Delta Sample Rate: 8 (cents)

Progress Billing Rule 3

Call Progress Time: 0-20 (min)

Delta Sample Rate: 5 (cents)

This rule has the following practical effects:

- If a user talks up to 5 minutes the effective billing rate will be 20 cents per minute (base rate + delta rate).
- Talking more than 5 minutes but less than 10 minutes makes the effective billing rate is  $10 + 8 = 18$  cents per minute.
- A conversation longer than 10 but less than 20 minutes results in a combined, applied billing rate of 15 cents per minute.
- If a user talks more than 20 minutes the effective billing rate is 10 cents per minute. (The progressive billing rule will not apply after 20 minutes).

## Progressive Billing Configuration

Progressive Billing configuration relies on the functionality contained within the associated Edit menu options:

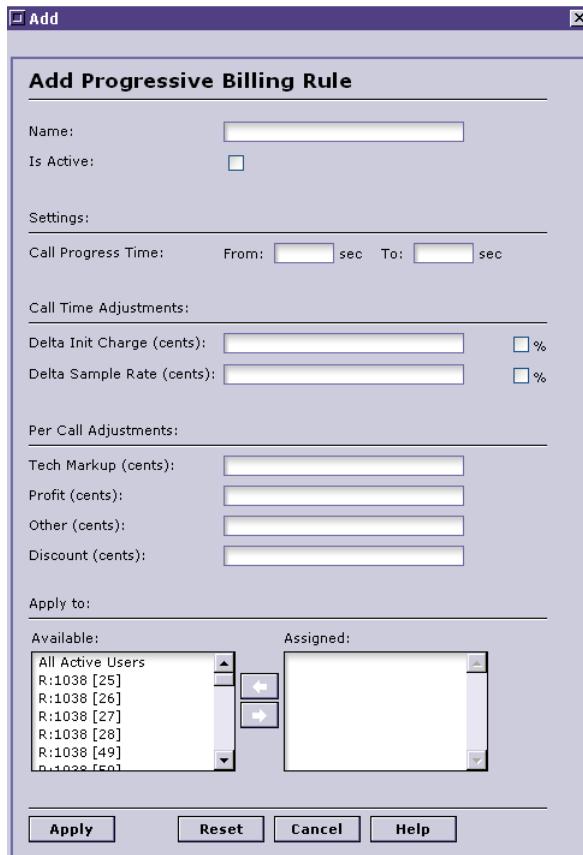
- **Add Progressive Billing Rule.** Create new Progressive Billing rule for designated clients and calls (by area code).
- **Edit Progressive Billing Rule.** Modify an existing Progressive Billing Rule.
- **Delete Progressive Billing Rule.** Delete a rule.
- **Assign Area Codes.** A separate Edit menu option, this is really the last step in adding a rule, and may also be modified when editing a rule.

### Add Progressive Billing Rule

To create a new Progressive Billing module rule:

**Step 1** At the Navigator view, select **Custom Modules>Progressive Billing**.

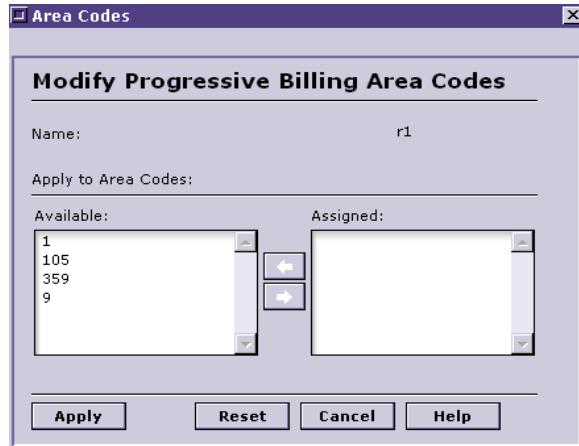
**Step 2** Select **Edit>Add Progressive Billing Rule** and the associated dialog is displayed:



**Figure 1-238Add Progressive Billing Rule**

- Step 3** Assign a name, preferably one that you can associate with rule contents.
- Step 4** Set the rule status. Check the ‘Is Active’ box to activate the rule immediately upon configuration. Leave blank to create the rule but leave it inactive.
- Step 5** Set the rule interval (Call Progress Time) by setting values in the Call Progress Time ‘From’ and ‘To’ entry boxes. The *From* value sets the number of seconds after call initiation to activate Call Progress Time. *To* stops the interval. Call billing after this point is governed by default settings for rule-defined clients.
- Step 6** Now set the Call Time adjustment parameters, in cents:
  - (a) Delta Init Charge. Triggers one-time additional charge for rule-governed calls.
  - (b) Delta Sample Rate. Sets the rate to apply during the Call Progress Time interval specified in the previous step.
- Step 7** Set Per Call Adjustments - Tech, Profit, Other or Discount - as desired.
- Step 8** Select **Apply** to save the configuration parameters and close the dialog. At this point the new rule is added to the Progressive Billing Rule List.
- Step 9** Assign the rule-associated area codes:
  - (a) Select the newly created rule from the Progressive Billing Rule List
  - (b) Select **Edit>Assign Area Codes**. The Assign Area Codes dialog appears.

- (c) Select and move available area codes that you wish to assign to the rule (only calls to these codes by assigned will be governed by configured rates).
- (d) Select **Apply** to enforce the area code assignments.



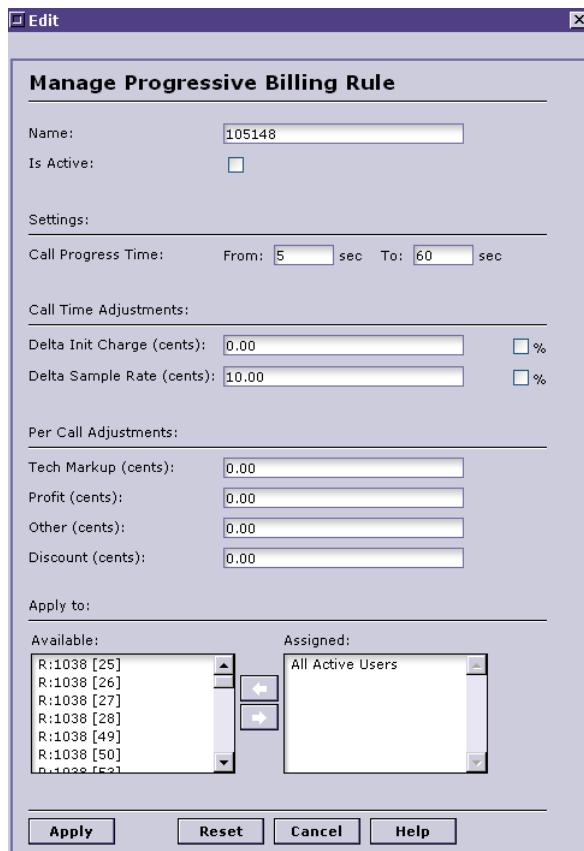
**Figure 1-239Assign Area Codes**

The dialog box is closed and the rule ‘returned’ to the Progressive Billing List. If the rule is set as Active, its billing rates will be applied to assigned clients/customers.

### Edit Progressive Billing Rule

Follow these instructions to edit or modify a current Progressive Billing Rule:

- Step 1** At the Navigator view, select **Custom Modules>Progressive Billing**.
- Step 2** Select the rule from the Progressive Billing list that you wish to edit.
- Step 3** Select **Edit>Edit Progressive Billing Rule**. The associated dialog opens:



**Figure 1-240**Modifying Progressive Billing

- Step 4** Change any aspect of the rule definition.
- Step 5** Select **Apply** to enforce changes.
- Step 6** If you wish to change area code assignments, reselect the rule instance from the Progressive Billing list. Select **Edit>Assign Area Codes**. Assign or remove area codes and select **Apply**.

### Delete Progressive Billing Rule

To delete a Progressive Billing rule:

- Step 1** At the Navigator view, select **Custom Modules>Progressive Billing**.
- Step 2** Select the rule from the Progressive Billing list that you wish to delete.
- Step 1** Select **Edit>Delete Progressive Billing Rule**.
- Step 2** Confirm the deletion to remove it, or cancel to leave the rule in place.

## Provider Time Interval Module

The Provider Time Interval module lets the Administrator change Provider Rate costs during predefined time periods, and can be used in conjunction with least cost routing.

By effectively reconfiguring these rates, you pass on changes in expenses to the customer. This is a critical tool in managing overall administrative costs and maintaining revenues and profits. The provider's own business decisions are thus incorporated into your model and business.

Using this module, an administrator can set one of two rate types for the Rate Plan ID:

- A specific provider rate plan, where plans are imported by provider. Once you identify these, you simply import the appropriate plan for each provider - one plan to a provider.
- Floating Rate. Selecting a Floating Rate fixes costs to specified area codes based on Floating Rate Adjustments (FRA). These adjustments are calculated by 1) a flat amount of additional surcharge or 2) a percentage value.
- Time Setting values determine the start and end of a rule's cycle. They also include the hours of day on which the rule applies during selected days (if the full 24 hour period is not chosen).
  - Peak Interval Start Date. Specifies the start date for the peak interval during which special charges apply.
  - Peak Interval End Date. Specifies the peak interval end date.
- Daily Filters. This means selecting the specific days of the week on which the Provider intervals will apply.
- In addition rate adjustments should be specified:
  - Call time adjustments reflect additional rates specified in absolute values or percentage terms
  - Per call adjustments. Special markups and profit amounts are again incorporated according to the provider for whom the rule is created.

The last steps in designing a provider time interval rule are defining providers and their related area codes. Filtering area codes ties the provider time interval rules more accurately to the provider rate changes.

## Provider Time Interval Configuration

These Edit menu options key the configuration of Provider Time Interval rules:

- Add Provider Time Interval
- Edit Provider Time Interval
- Delete Provider Time Interval

As with any module, most of an Administrator's work involves creating (adding) an interval rule or modifying (editing) an existing rule.

### Add Provider Time Interval

To add a new rule, do the following:

- Step 1** From the Navigator view, select **Custom Modules>Provider Time Intervals**. View the Provider Time Intervals list:
- Step 2** Select **Edit>Add Provider Time Intervals**. The Add Time Interval dialog is presented:

**Figure 1-241**Adding a Provider Time Interval Rule

**Step 3** Assign a name to the new rule.

**Step 4** Select the Rate Plan ID to apply to the rule:

- Select the pull-down menu for the Rate Plan ID option;
- Scroll through the list of Rate Plan IDs until you find the desired one;
- Select it and it is displayed in the box next to 'Rate Plan ID.'

---

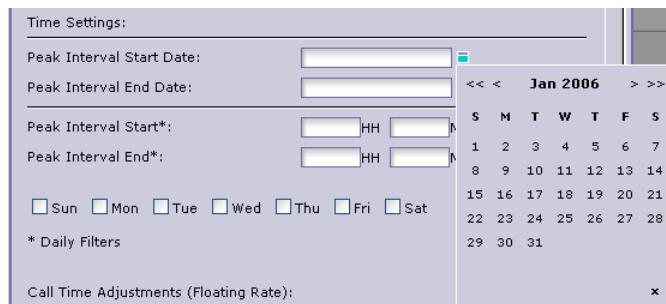
**Note** Select the Rate Plan ID for the correct provider. (There is a one-to-one correspondence.) Selecting a Floating Rate at the Rate Plan ID field to assign single or multiple providers to a rule.

---

**Step 5** Define the Time Interval parameter settings:

- Peak Interval Start Date (select the Calendar shown below, then pick a Start Date)
- Peak Interval End Date (calendar-selection)
- Peak Interval Start
- Peak Interval End

- Daily Filters (days to apply the rule match those specified by the provider).



**Figure 1-242**Calendar Selection Pop-Up

---

**Note** The standard Peak Interval Start/End Date difference is one month. Choosing any period less or greater than one month terminates rate settings at the End Date.

---

**Step 6** Set the Call Time adjustments:

- Delta Init Charge
- Delta Sample Rate

**Step 7** Set any of the four Per Call Adjustments parameters:

- Tech Markup
- Profit
- Other
- Discount

**Step 8** Apply the provider(s) to whom the rule applies.

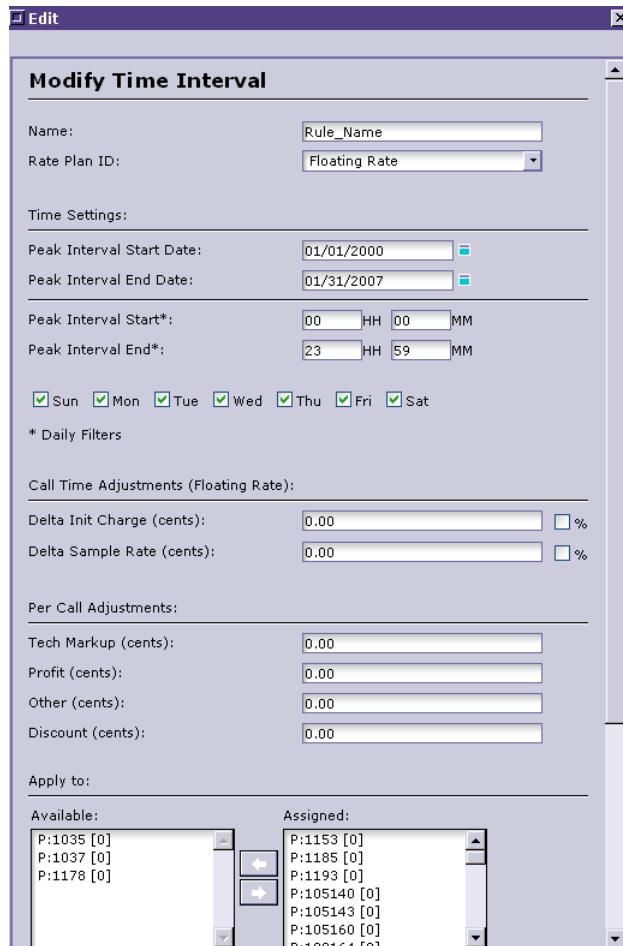
**Step 9** Apply the provider area codes to apply to the rule.

**Step 10** Select **Apply** to complete configuration and save the rule. The dialog is closed and the newly created rule added to the Provider Time Intervals list.

### Edit Provider Time interval

To edit an existing Provider Time rule:

- Select **Custom Modules>Provider Time Intervals** at the Navigator view.
- Select the specific rule to edit from the list.
- Select **Edit>Edit Provider Time Interval** to view and the Modify Time Interval dialog:



**Figure 1-243** Modify Time Interval Dialog

- Step 4** Edit any aspect of the rule, from Name to provider and area code assignments.
- Step 5** Select **Apply** to save modifications.

#### Delete Provider Time Interval

Delete any Provider Time Interval this way:

- Step 1** Select **Custom Modules>Provider Time Intervals** at the Navigator view.
- Step 2** Select the specific rule to delete from the Provider Time Intervals list.
- Step 3** Select **Edit>Delete Provider Time Interval**.
- Step 4** Confirm the deletion by selecting **OK** on the message box, or **Cancel** to abort the action. Deleted rules are removed from the list and the billing rules for the affected customers revert to previous system settings.

# Rate Switching Module

The Rate Switching module allows dynamic billing rate plan switching on customer batches based on an Administrator-specified threshold balance. When a customer assigned to a particular Rate Switching rule exceeds the threshold specified for the rule, the system begins charging that customer based on the designated, alternative rate plan.

The threshold is actually a range that stretches from a minimum (low balance) to a maximum (high balance). As long as the customer's balance falls within the range, the current rate plan applies. However, once the customer's balance (defined as either *monthly* or *credit* balance) dips below the threshold or rises above it, the alternative plan is immediately applied to that customer.

---

**Note** The threshold balance amount is applicable on per month to month basis only.

---

The key parameters for this module are the **Low Balance** and **High Balance** fields that set the threshold limits, and **Change Rate Plan To**, where the alternative rate plan is assigned.

Rules created can be applied to:

- All users
- Resellers batches (and attached users)
- Corporate batches (and their attached users)

Thresholds and alternative rate plans apply to the assigned batches, so they should be configured with the projected groups in mind. Alternative billing rate plans should conform to the customer calling patterns and preferences - all within the context of your business plan and revenue strategy.

## Rate Switching Configuration

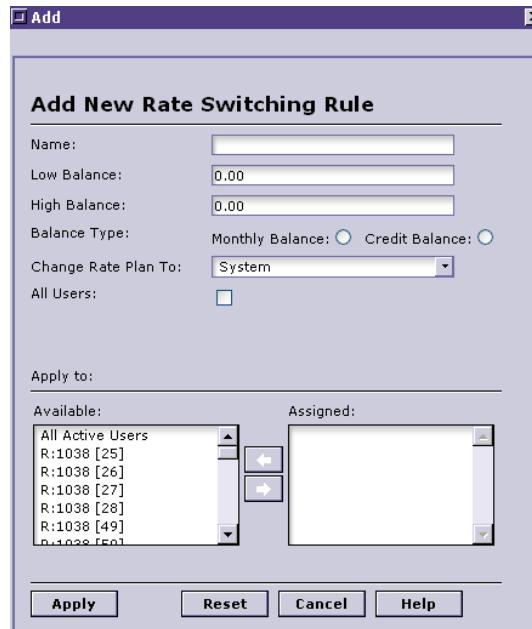
Here are the key Edit menu functions that correspond to Rate Switching configuration tasks:

- **Add Filter.** Select to configure a new Rate Switching rule and apply it to system callers (client batches/users).
- **Modify Filter.** Use to edit any aspect of an existing Rate Switching rule.
- **Delete Filter.** Delete an existing rule that is no longer applicable to system billing needs. **Rate Switching rules must be deleted in order to become inactive.**

### Create Rate Switching Rule (Add Filter)

Follow these procedural steps to add a Rate Switching rule, or filter:

- Step 1** At the Navigator view, select **Custom Modules>Rate Switching**. The Rate Switching list is displayed:
- Step 2** Select **Edit>Add Filter**. The Add New Rate Filter dialog appears:



**Figure 1-244Adding a New Rate Switching Rule**

**Step 3** Name the rule. Assign a name that refers to rule parameters, assigned clients, etc.

**Step 4** Specify low and high balances for the threshold to apply to the rule.

---

**Note** This threshold is not a single value but a range with lower and upper boundaries set at the Low Balance and High Balance fields.

---

- (a) Set a value to define Low Balance. Relevant customer balances falling below this amount are subject to rate switching.
- (b) Set the High Balance. Any rule-defined customer exceeding this value is subject to immediate rate switching.

**Step 5** Set a balance type. The options are Monthly Balance or Credit Balance.

**Step 6** At the **Change Rate Plan To** field, select the alternative rate plan (the one you select takes effect when assigned users exceed either threshold). Open the pulldown menu and select:

- The System rate plan
- Any custom rate plan from the remaining available rate plans displayed

**Step 7** Select the **All Users** check box if you want the rule under construction to apply to all users (callers).

**Step 8** Assign any Reseller Batches to fit the rule. Select available batches and move them to the Assigned box.

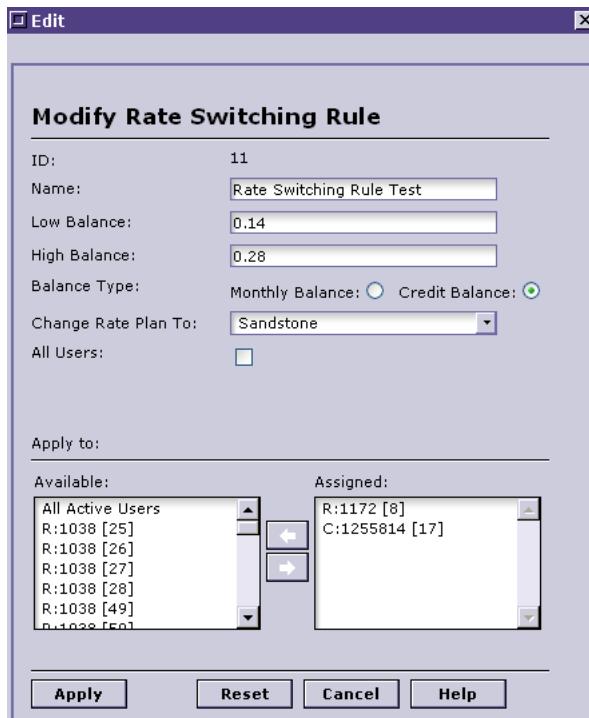
**Step 9** Repeat Step 8 for Corporate Batches.

**Step 10** Select **Apply** to save changes and enforce the rule.

## Modify Rate Switching Rule (Filter)

To open any existing Rate Switching rule and change any aspect of its configuration, follow this procedure:

- Step 1** At the Navigator view, select **Custom Modules>Rate Switching**.
- Step 2** From the Rate Switching rules list, select the rule to modify.
- Step 3** Select **Edit>Modify Filter**. View the Modify Rate Switching Rule dialog:



**Figure 1-245**Modify Rate Switching Rule

- Step 4** Edit any aspect of the rule.
- Step 5** Select **Apply** to enforce changes and the dialog is closed.

## Delete Rate Switching Rule (Filter)

To delete an Rate Switching rule:

- Step 1** At the Navigator view, select **Custom Modules>Rate Switching**.
- Step 2** Select the rule from the list that you wish to delete.
- Step 3** Select **Edit>Delete Filter**.
- Step 4** At the Confirmation prompt, select **OK** to delete the filter or **Cancel** to abort.
- Step 5** Upon confirmation, the rule is deleted and removed from the Rate Switching list.

## Softphone Profiles Module

The VoiceMaster SoftPhone Profiles module enables the installation and configuration of the SoftPhone application. Once configured, subscribers can make VoIP calls using SoftPhone.

In order to administer the SoftPhone Profiles module, an Administrator will need these two key pieces of information:

- SoftPhone License String
- ActiveX Class and Version Info

SysMaster provides both to any VoiceMaster customer that acquires the module.

The Softphone Profiles module is installed on the VoIP provider's web server. Typically, the VoIP service provider will create an icon on the company website that is accessible to designated subscribers.

The icon should be linked to one of the following URLs:

- **http://www.norfa.com/cgi-bin/if.cgi?run=ipp&p=1**  
where p=1 indicates that VM100 SoftPhone will operate in H.323 mode (profile id 1)
- **http://www.norfa.com/cgi-bin/if.cgi?run=ipp&p=2**  
where p=2 indicates that VM100 SoftPhone will operate in SIP mode (profile id 2)

One of the key configuration aspects of the SoftPhone Profile is setting the 'skin' - or appearance - of the call icon that the customer view. The full set of configuration tasks and options is detailed in the next sections.

## SoftPhone Profiles Configuration

The SoftPhone application is configured through the SoftPhone Profile dialog that is accessible through the Custom Modules folder. The module appears as a sub-folder within Custom Modules once installed.

Here are the menus that enable SoftPhone profile rule creation and modification:

- Add Softphone Profile
- Edit Softphone Profile
- Delete Softphone Profile

### Add Softphone Profile

To add a SoftPhone Profile, do the following:

**Step 1** At the Navigator View, select **Custom Modules>Softphone Profiles**.

**Step 2** Select **Edit>Add SoftPhone Profile**, and the relevant dialog box is displayed:



**Figure 1-246 Add Softphone Profile Dialog**

**Step 3** Assign the new profile a name.

**Step 4** Set the SoftPhone Profile *protocol type*. The SoftPhone license should reflect the VoiceMaster configuration and protocol capabilities.

- H.323 SoftPhone
- SIP SoftPhone
- H.323-PBX
- SIP-PBX

**Step 5** Enter the license string. Refer to the information supplied by SysMaster with the module.

**Step 6** Define the codecs (compression protocols) supported by the profile. Enter one or more of these five:

- G.729
- G.723
- G.711 A-law
- G.711 U-law (When using codec G.711 U-law, the actual codec entered is G.711 M-law)

### — GSM

**Step 7** Define the ActiveX Class and Version Info. Again, refer to the information supplied by SysMaster at the time of purchase.

**Step 8** Define the Soft Phone Button URL [1]. This entry reflects a customized SoftPhone button name and URL. The entry should look like:

["Balance","http://URL"]

**Step 9** Enter the Soft Phone Button URL [2]: Customizes the SoftPhone button name and URL. The entry should look like:

["Rates","http://URL"]

**Step 10** Create the Soft Phone Button URL [3]. Once again, this should be a customized name and SoftPhone button URL. The entry should look like:

["Purchase","http://URL"]

**Step 11** Build the Soft Phone Button URL [4] by entering name and URL. The entry should look like:

["Help","http://URL"]

**Step 12** Create entries for PBX Buttons [5] - [14] that customize the name and URL that apply to each of the ten PBX buttons.

**Step 13** Define Soft Phone CGI Authentication. This is the URL of the location where SoftPhone CGI authentication is performed.

Define a prefix. Designates the prefix that the user manually attaches to the number dialed.

The prefix should be entered in the form of:

prefix[i]="999";

where [i] designates the number of digits expected to be dialed by the user. For example, if a user dials a 7 digit number the value of [i] will be equal to 7.

Examples:

```
prefix[1]="999";
prefix[2]="222";
prefix[3]="1415";
prefix[7]="510"
```

**Step 14** Set the Soft Phone Inactivity Timeout (sec). This triggers a timeout when the amount of time entered is surpassed. At that point, user sessions will terminate and the SoftPhone will be unregistered.

**Step 15** Select **Apply** to apply the configuration parameters defined.

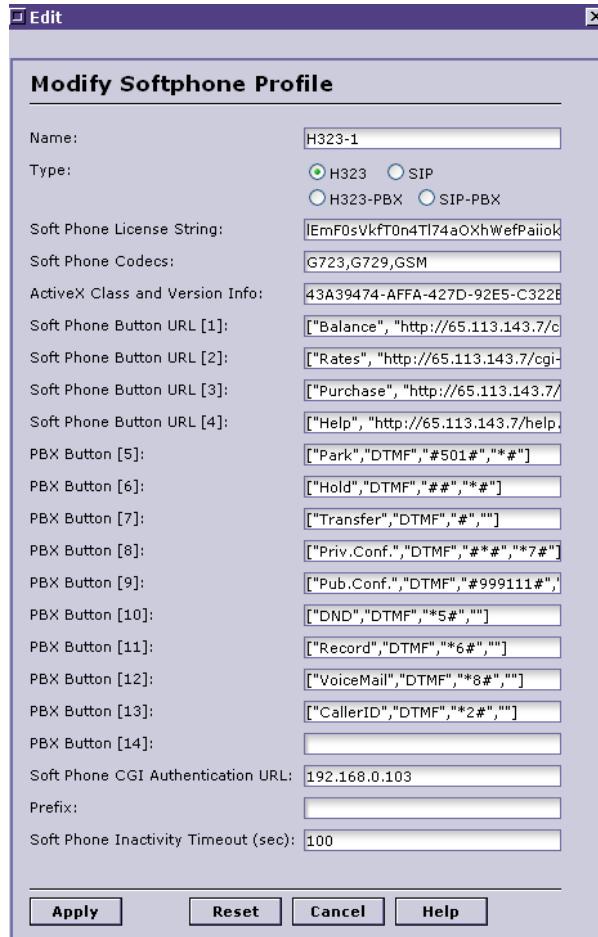
## Edit Softphone Profile

The Administrator can modify any profiles created by doing the following:

**Step 1** At the Navigator view, select **Custom Modules>Softphone Profiles**.

**Step 2** Select the profile that you want to modify (from the SoftPhone Profiles list).

**Step 3** Select **Edit>Edit Softphone Profile**. The Edit dialog is displayed:



**Figure 1-247 Modify Softphone Profile Dialog**

**Step 4** Change any of the fields, from name to type to button definition to timeout period.

**Step 5** Select **Apply** to apply changes.

### Delete Softphone Profile

To delete an existing SoftPhone Profile, perform these actions:

**Step 1** At the Navigator view, select **Custom Modules>Softphone Profiles**.

**Step 2** Select the profile that you want to delete from the list.

**Step 3** Select **Edit>Delete SoftPhone Profile**.

**Step 4** At the confirmation prompt, select **OK** to delete the profile, or cancel the deletion. Deleted profiles are removed from the SoftPhone Profiles List.

## Special Numbers Module

The Special Number module lets an Administrator assign additional charges based on two call characteristics:

- The origination endpoint
- Its type (ANI, DNIS)

Special Number module functionality is designed on a per gateway basis. Special phone numbers are matched as a prefix (e.g. 1510 or 1415) either against an ANI or DNIS phone number.

---

**Note** No ANI or DNIS manipulation is performed during Special Number matching.

---

The actual matching of a designated special number is specified by the type the Administrator assigns it during creation of the applicable Special Number rule.

There are three special number types available:

- ANI – Automatic Number Identification identifies the number of the calling phone.
- DNIS. Dialed Number Identification informs a call receiver of the actual number that the caller dialed.
- ANI/DNIS. Both functions are provided.

Create a special number rule by first specifying type and route and rate adjustments. That is, the Administrator can define a specific Special Numbers rule so that the system notes the Special Number and switches either route or rate (according to Administrator configuration preference).

---

**Note** Neither route nor rate switching configuration are required. The Special Number can simply be allowed to continue on the same route and under the same rate plan. However, the Administrator can also enforce rate changes according to settings in the next fields: Call Time and Per Call Adjustments and Line Expenses. **In order to change routes for any rule, your VoiceMaster must include the Custom Routes module. Otherwise, only the system route will be present.**

---

Call Time Adjustments can include the following:

- **Delta Init Charge** Assigns an additional charge on top of provider rate settings. The value for a Delta Init Charge can also be set as a percentage of the pre-defined Init Charge.
- **Delta Sample Rate** Specifies an additional (delta) charge on top of a Sample Rate charge. Can be set as a percentage of the pre-defined Sample Rate charge.

Per Call Adjustments divide into:

- **Tech Markup** Fee that passes on infrastructure technology charges
- **Profit** Sets an absolute profit amount per call
- **Other** Miscellaneous additional charges

Finally, Line Expenses can be modified according to these parameters:

- Initial Time
- Initial Charge
- Sample Time
- Sample Rate
- Bill Incomplete Calls to Account ID

Special Number rule configuration is completed by the assignment of the rule to designate gateways and clients. Assigning specific devices to the rule further filters it.

Client definition possibilities include:

- All Active Users
- Resellers
- Wholesalers
- Corporate customers

Multiple rules can apply to one number. These rules may or may not be similar to one another, but all apply to the same Special Number.

Here is an example of a ‘duplicated’ rule:

```
IDNumber Type Client Adjusted Rate  
11510 ANI Client1 Sample Rate = +10 cents  
21510 ANI Client2 Sample Rate = +20 cents
```

## Special Numbers Configuration

Configuring Special Numbers Rules is accomplished through the Edit menu options:

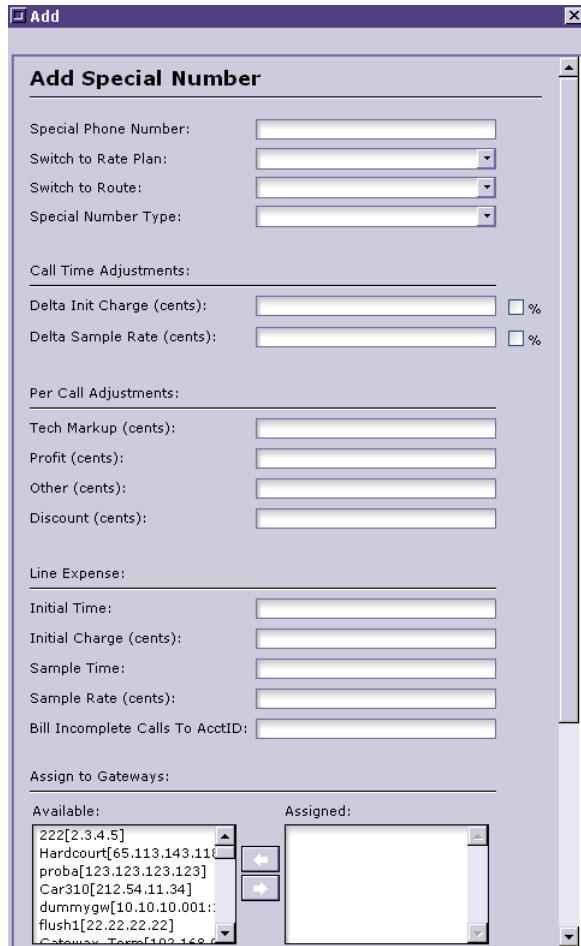
- Add Special Number. Create a new rule for a special number.
- Edit Special Number. Edit an existing rule, changing some parameter or aspect.
- Delete Special Number. Remove a rule from the stock of Special Number rules.
- Display List (toggles with Search [for rule] mode)

### Add Special Number Rule

To add a Special Number rule, follow these steps:

**Step 1** At the Navigator view, select **Custom Modules>Special Numbers**.

**Step 2** Select **Edit>Add Special Number**. The Add Special Number dialog opens:



**Figure 1-248Add Special Number Dialog**

- Step 3** In the first field, type in the Special Number from which the rule will be built.
- Step 4** Select the Switch to Rate Plan pulldown menu to assign a different rate plan to the rule. Select the desired replacement rate plan and your choice ‘populates’ the Switch to Rate Plan field.
- Step 5** Select the Switch to Route pulldown menu to apply a different route to the Special Number rule.
- Step 6** Identify the special number type by selecting the Special Number Type pulldown and choosing from one of the three available options (ANI, ANI/DNIS or DNIS). Select the appropriate type and the field shows your choice:
- Step 7** Set Call Time Adjustments, if any:
  - Set a Delta Init Charge, either as an absolute value or a percentage. This amount will be applied to at the start of any call to which the rule applies.
  - Delta Sample Rate. Applies an additional charge to such calls. As with all adjustments and expenses, the amount is ‘Administrator discretion’ and can be set either as an absolute value or a percentage of the overall call.
- Step 8** Set Per Call Adjustments as desired:

- Tech Markup. A technology fee assessed to compensate for infrastructure costs.
- Profit. An arbitrary amount of profit per call, to override profits that fall beneath this. A profit ‘threshold’ by definition.
- Other. Miscellaneous charges.
- Discount. Apply a discount to calls governed by the rule.

**Step 9** Set (optionally) Line expenses, which break down into:

- Initial Time
- Initial Charge
- Sample Time
- Sample Rate
- Bill Incomplete Calls to AcctID.

The first four charges are variations of the previous adjustment categories. The last option specifies the account billed when rule-regulated calls terminate prematurely.

**Step 10** Assign the gateways that will be referenced by the rule. Select each that you wish to assign and move it to the Assigned box from the Available box. Only calls to or from the Special Number routed through the assigned gateways will be rule-affected.

**Step 11** Finally, assign desired clients to the rule. Calls to and from clients NOT assigned to the rule, including those in which the Special Number is involved, are not affected.

**Step 12** Select **Apply** to save changes and enforce the rule. The dialog is closed and the new rule added to the Special Numbers rules list.

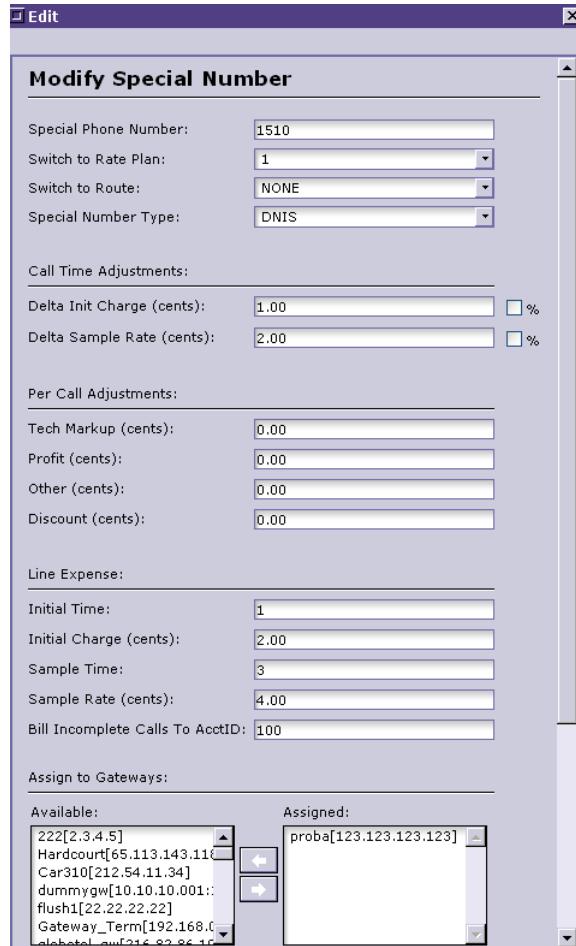
### Edit Special Numbers Rule

To edit any configured Special Numbers rule:

**Step 1** At the Navigator view, select **Custom Modules>Special Numbers**.

**Step 2** From the list, select the rule that you wish to edit.

**Step 3** Select **Edit>Edit Special Number**. The following dialog pops into view:



**Figure 1-249** Modify Special Number Dialog

**Step 4** Change any aspect of the rule's configuration:

- Alternative rate or route plan
- Special number type definition
- Call Time or Per Call adjustments
- Line expense settings
- Gateway and/or client assignments.

**Step 5** Select **Apply** to save changes and close the dialog. The new settings are now in force.

#### Delete Special Number Rule

To delete any current Special Number rules, execute this procedure:

- Step 1** At the Navigator view, select **Custom Modules>Special Numbers**.
- Step 2** From the list, select the rule to delete.
- Step 3** Select **Edit>Delete Special Number**.
- Step 4** Select **OK** at confirmation to delete or **Cancel** to preserve the rule.

**Step 5** Rules whose deletion you confirm are erased and removed from the Special Numbers list.

## Time Interval Module

The Time Interval module lets the Administrator assign time interval-based billing policies to specified clients based on custom time parameters (time of day/day of week). Policies can be applied to a single client, to multiple customers or to all subscribers to your service.

Rules are geared to a specific rate plan that the Administrator selects before assigning intervals or clients. This rate plan is the basis of the rule. By setting time intervals and call adjustments (per time and per call), the Administrator builds a custom rate plan for the rule.

---

**Note** The final phase, or rule filter, involves assigning area codes to which the rule is applied.

---

The Time Interval module provides great flexibility and potential rate combinations for custom billing that is applied to various groups of customers. Use it to add fairly simple rules to apply to a few groups of users, or to create detailed, multiple rules to affect a larger customer pool.

---

**Note** Creating multiple Time Interval rules expands not only billing options but your billing management options.

---

The module is keyed from the Time Interval settings that set 1) interval start and end (day of the month), 2) interval hours (times of day on which the rule and its rates apply) and 3) days of the week on which the rule applies. Assigned days of the week and interval hours filter the rule, that is, create a subset of time blocks during which the rule applies.

The specific Time Interval settings are:

- **Peak Interval Start Date.** Specifies rule start date.
- **Peak Interval End Date.** Specifies rule end date.
- **Peak Interval Start.** On rule-applied days of the week, sets the time of day at which the rule applies.
- **Peak Interval End.** Specifies the time of day (on rule-applied days) at which the special rates end.
- **Week Days.** Configures the Time Interval rule to apply to specified days of the week.

## Time Interval Configuration

Configuring Time Interval rules depends on these Edit menu options:

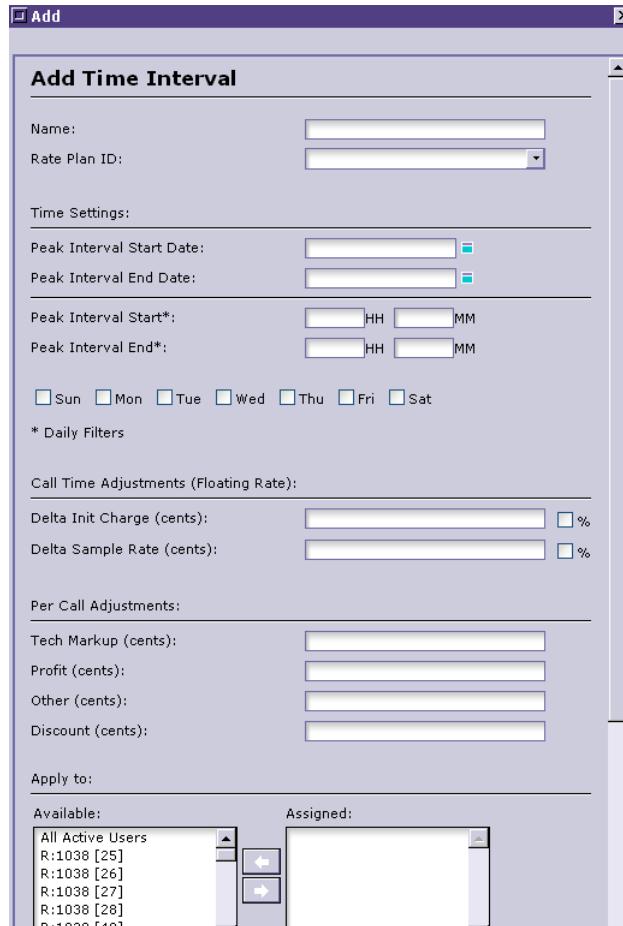
- Add Time Interval
- Edit Time Interval
- Delete Time Interval

### Add Time Interval Rule

To configure a new Time Interval rule, do the following from the Navigator view:

**Step 1** Select Custom Modules>Time Intervals.

**Step 2** Select Edit>Add Time Interval for the Add Time Interval edit dialog.



**Figure 1-250**Adding a Time Interval Rule

**Step 3** Specify a name for the new rule.

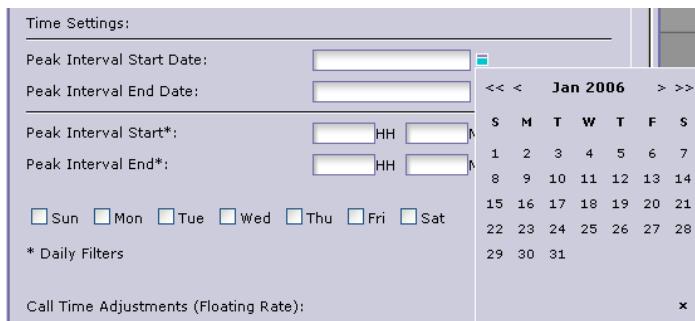
**Step 4** Select a Rate Plan ID from the pulldown menu. Two categories are available:

- (a) Floating Rate
- (b) Specific (Billing) Rate Plan

**Note** Selecting a Floating Rate means that the rule assigns charges to calls made by rule-designated clients based on Floating Rate Adjustments (FRA). These adjustments reflect basic (provider) rates and are calculated either by 1) a flat amount of additional surcharge or 2) a percentage value of provider rates.

When selecting Floating Rate as your rate plan, you can assign 1) a single client 2) multiple clients or 3) all clients (and users). Selecting a specific rate plan limits the universe of clients that can be assigned to the new rule. The clients selected should be associated with the chosen rate plan.

- Step 5** Set time interval settings to apply to the rule. The time interval parameters are:
- Set Peak Interval Start Dates. Click on the colored box to the right of Peak Interval Start Date. View the calendar popup. Select a date on which to begin the Time Interval Rule.



**Figure 1-251** Selecting Peak Interval Dates

- Select the Peak Interval End Date. Select the calendar. Select the desired date and it fills the box.

---

**Note** Time Interval rules assume renewable one-month periods, so the Peak Interval End Date is typically one month after the Start Date. Rules that apply for less than one month will terminate at the End Date.

---

- Step 6** Set a Peak Interval Start. This is the specific time of day at which the configured rule will take effect, on rule-relevant days (set in Daily Filters, below).
- Enter an hour for the interval to begin in the HH box.
  - Tab to the MM box and set the minute at which the interval is triggered.

- Step 7** Repeat the actions in Step 6 for the Peak Interval End. The rule is disabled at the time specified in the HH/MM boxes, on days where the rule is set.

- Step 8** Set Daily Filters. Check the boxes for the days of the week on which you want the Time Interval rule to apply. As mentioned, the Time Interval filter is first defined by the daily filters, then by the peak intervals set in the previous steps.

---

**Note** Leaving a particular day's check box empty means that the rule will not apply on that day. Peak interval start and end times will not be triggered if a day is not selected.

---

- Step 9** Set Call Time Adjustments:
- Delta Init Charge.** Set a base for an initial flat charge to be added to the user's account when the rule applies. Enter either an absolute value or a percentage of the call cost.

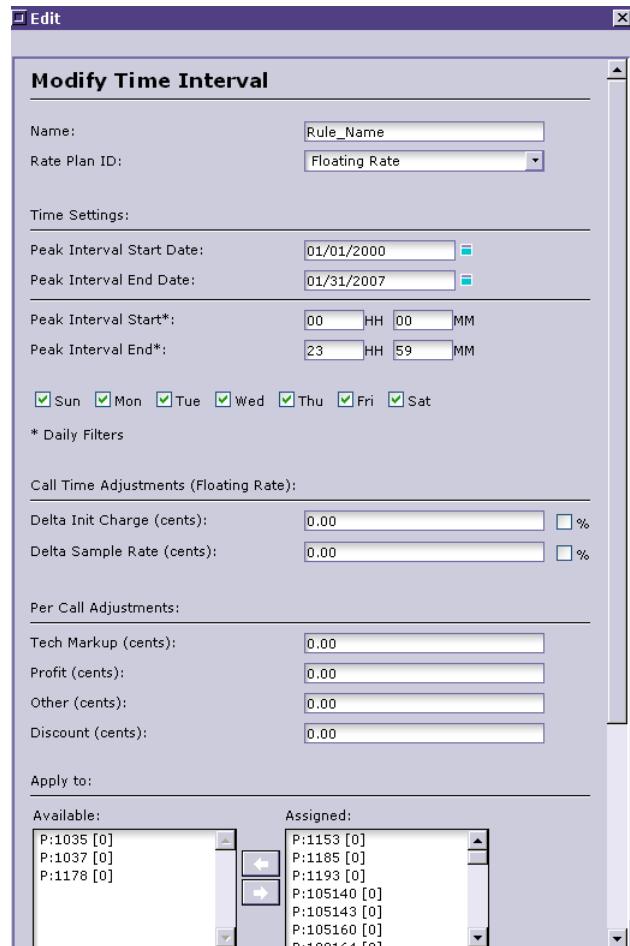
- (b) **Delta Sample Rate.** This value reflects the additional (delta) value added to the Sample Interval for the user *during the relevant interval*. If not specified, the system will use the default Sample Interval. Again, set either a fixed value or a percentage.

- Step 10** Set Per Call Adjustments (all entries in cents):
- (a) **Tech Markup.** Specify a tech markup margin per user call
  - (b) **Profit.** Specify profit margin per user call.
  - (c) **Other.** Assign miscellaneous expenses and adjustments
  - (d) **Discount.** Specify a discount – relevant mostly to resellers. (When you specify a discount, this has the effect of nullifying other per call adjustments.)
- Step 11** **Apply to Clients.** Assigns specific client groups (resellers and corporate clients) or users (all users) to the rule. Select desired groups from the Available box list and move them to the Assigned box. Click on a group, select the right arrow key and it is placed in the Assigned box. Repeat this for as many client batches as relevant to the particular Time Interval rule.
- Step 12** **Apply to Area Codes.** Sets those area codes to apply the rule to. Only designated users calling to specified area codes will be charged according to the particular Time Interval rule rate definition.)
- Step 13** Select **Apply.** The database is updated, the rule is saved, and it is added to the Time Intervals list.

### Edit Time Interval Rule

To modify an existing Time Interval rule, take these actions:

- Step 1** At the Navigator view, select **Custom Modules>Time Intervals**.
- Step 2** From the Time Intervals list, select the Time Interval rule to modify.
- Step 3** Select **Edit>Edit Time Interval**. View the dialog box:



**Figure 1-252Modifying a Time Interval Rule**

**Step 4** Change any aspect of the rule:

- Name
- Applicable Rate Plan ID
- Time Settings
- Call Time and Per Call Adjustments
- Client and area code assignments

**Step 5** Select **Apply** to save changes and close the dialog box. The modified rule remains on the Time Intervals list.

### Delete Time Interval

To delete any Time Interval rule, follow this procedure:

- Step 1** At the Navigator view, select **Custom Modules>Time Intervals**.
- Step 2** From the Time Intervals list, select the rule to delete.
- Step 3** Select **Edit>Delete Time Interval**.

- Step 4** At the Confirmation message, select **OK** to delete the selected rule, or **Cancel** to abort the action.