Managing and Monitoring Cisco Unified CallManager Express Systems

This chapter addresses managing and monitoring Cisco Unified CallManager Express (Cisco Unified CME). The following specific sections describe utilities available for monitoring and management Cisco Unified CME:

Note For additional information, see the "Related Documents and References" section on page xii.

Configuring and Monitoring via Network Management Systems Using the Cisco Unified CME AXL/SOAP Interface

You can integrate Cisco Unified CME with network management applications by using the Cisco Unified CME XML Layer (AXL) application programming interface (API). The AXL API provides a mechanism for inserting, retrieving, updating, and removing data from the Cisco Unified CallManager database using an XML SOAP interface. The AXL API allows programmatic access to Cisco Unified CallManager data in XML form instead of using a binary library or a Dynamic Link Library (DLL). The AXL API methods, or requests, are performed using a combination of HTTP and SOAP. The HTTP payload is encapsulated in SOAP, which is essentially an XML remote procedure call protocol. User requests send XML data to the Cisco Unified CallManager server, which returns an AXL response encapsulated in a SOAP message.

Cisco Unified CME extends the AXL/SOAP capabilities by providing XML APIs for monitoring and configuring IP phones and extensions. A Network Management System (NMS) might use the Cisco Unified CME AXL/SOAP APIs to poll the Cisco Unified CME network elements (NEs), including IP phones and extensions. As with the AXL protocol, communication between an NMS and Cisco Unified CME is based on an HTTP data exchange and can be initiated only by polling from the NMS. However, Cisco Unified CME can enable or disable the sending of data, and also control the polling interval.

Note AXL/SOAP APIs for NMS configuration and monitoring are supported only by Cisco Unified CME, not by Cisco Unity Express.

The next sections describe the features supported by the Cisco Unified CME AXL/SOAP APIs and a test procedure to check if your Cisco Unified CME is set up properly to respond to the AXL/SOAP queries.

Cisco Unified CME 4.0 XML Interface Enhancements

The following updates to the Cisco Unified CME XML interface were adopted with Cisco Unified CME 4.0:

- CME4.0 XML runs on top of IXI engine to replace the previous backend processing of AXL requests for better scalability; parser and transport layers are separated from the application itself.

  Note For backward compatibility, the old interface can still be used by configuring with the old CLIs.

- Cisco Unified CME XML support for configuration and monitoring
  - Monitoring requests—XML message payload is in the format of XML text-monitoring
  - Configuration requests—XML message payload is in the format of CLI list to be saved on a router as CLI commands

  Note The supported functionality of the XML interface remains unchanged.

- The IXI CLI is used to configure the XML interface

The Cisco Unified CME AXL/SOAP Interface

The Cisco Unified CME AXL/SOAP APIs provide many capabilities for monitoring and configuring IP phones and extensions.

For monitoring, Cisco Unified CME AXL/SOAP APIs support the following:

- Getting static information
  - ISgetGlobal—Gets global information
  - ISgetDevice—Gets device information
  - ISgetExtension—Gets extension information
- Getting dynamic information
  - ISgetEvtCounts—Gets the number of events recorded in the buffer
  - ISgetDevEvts—Gets device events if IP phones are in the register, unregister, or decease state
  - ISgetExtEvts—Gets extension events (the virtual voice port is up or down)
- Setting information (configuring) and executing CLI
  - ISsetKeyPhones—Sets the “key” phone

– ISexecCLI—Executes the CLI

The following are supported CLI commands that can be executed by the ISexecCLI API. You might execute all the subcommands under each of these configuration mode commands with the ISexecCLI API.

- **telephony-service**
- **ephone**
- **ephone-dn**
- **vm-integration**
- **ephone-hunt**
- **dial-peer voice**

Note CME AXL/SOAP APIs were first used by NetIQ's Vivinet Manager or AppManager for VoIP management solutions.

Testing the Cisco Unified CME AXL/SOAP Interface

You might use the test page (xml-test.html) that is available with the Cisco Unified CME GUI files to verify that the Cisco Unified CME router is set up correctly to respond to AXL/SOAP requests. The following are the steps to set up and run the test page:

Step 1 Load xml-test.html into Flash.

Step 2 Configure the following on the Cisco Unified CME router:

Router(config)# **ip http server**

Router(config)# **ip http path:flash**

Router(config)# **telephony-service mode**

Router(config)# **log password abcd**

Router(config)# **xmltest**

Step 3 Enter the following URL in the browser:

http://*ip-address of router*/ISApi/AXL/V1/soapisapi.is

Step 4 When the Login window opens, log on as follows:

Username: **any non-empty string**

Password: **abcd**

Step 5 In the test page, input content into the form. The XML request is written to the form at the bottom. Go to the bottom of the page and click **Submit**.

Step 6 Try the preceding steps on your system. If you receive any errors, the following debugs on the router might help:

Router# **debug ip http appinout**

Router# **debug ip http appdetail**

The xml-test.html file is a test program for you to check that the Cisco Unified CME router can respond to AXL/SOAP requests. You must disable the test program when polling from an NMS using the Cisco Unified CME AXL APIs with the following configuration:

Router(config)# **telephony-service**

Router(config-telephony)# **no xmltest**

Note A polling request from an NMS must be sent in clear-text format.

Note For more information about Cisco Unified CME XML provisioning, see this URL: http://www.cisco.com/en/US/products/sw/voicesw/ps4625/products_programming_reference_guide09186a00801c5fab.html

For developer services support, go to the Cisco Developer Support site at http://www.cisco.com/cgi-bin/dev_support/access_level/product_support. You must be a Cisco.com registered user to access this site.

Cisco Unified CME 4.0 XML Configuration Example

The following is an example Cisco Unified CME 4.0 XML configuration:

```
ip http server
! Enables http server

ixi transport http
 no shutdown
! Assigns http as the transport method of IXI

ixi application cme
 no shutdown
! Enables IXI's CME application

telephony-service
 xml user admin password cisco 15
! Configures privilege for CME XML interface
```

Use the following debug command to troubleshoot Cisco Unified CME XML configurations:

debug cme-xml

Monitoring Cisco Unified CME

You might monitor the Cisco Unified CME system with syslog messages and Simple Network Management Protocol (SNMP) Management Information Base (MIB). You also can monitor call activity information through syslog messages and call detail records (CDR).

Monitoring IP Phones Using Cisco Unified CME Syslog Messages

Cisco Unified CME 3.0 introduced type 6 syslog messages, as shown in the following example, for IP phone registration and deregistration events. These syslog messages are useful for a central NMS to manage Cisco Unified CME systems and IP phones.

```
%IPPHONE-6-REG_ALARM
%IPPHONE-6-REGISTER
%IPPHONE-6-REGISTER_NEW
%IPPHONE-6-UNREGISTER_ABNORMAL
%IPPHONE-6-REGISTER_NORMAL

Example Message:
 %IPPHONE-6-REGISTER_NEW: ephone-3:SEP003094C38724 IP:1.4.170.6 Socket:1
  DeviceType:Phone has registered.
```

The IPPHONE-6-REGISTER_NEW message shown in preceding configuration example indicates that a phone has registered and that it is not part of the explicit router configuration. However, the ephone configuration has not yet been created. Cisco Unified CME allows unconfigured phones to register to make provisioning of the Cisco Unified CME system more convenient. By default, phones designated as new are not assigned phone lines; therefore, they cannot make calls until they are configured into the system.

Enable the Cisco IOS logging capability to log all the syslog events into the buffer on the Cisco Unified CME router, or send the syslog messages to a syslog server for offline management, as shown in the following example.

```
Telephony-service#(config)# service timestamps log datetime msec localtime
Telephony-service #(config)# aaa new-model
Telephony-service #(config)# aaa authentication login default none
Telephony-service #(config)# aaa accounting connection H.323 start-stop radius
Telephony-service #(config)# gw-accounting syslog
Telephony-service #(config)# logging 10.10.10.1
!!! 10.10.10.1 is the ip address of syslog server, multiple servers might also be
  specified
```

To synchronize your Cisco Unified CME system to an external NTP server, use the following:

```
ntp server ip-address
 !!! ip address - IP address of the time server providing the clock
  synchronization
```

If there is no external NTP time source, use the internal router clock as the time source:

ntp master

To ensure that the time stamps are correct, set the router clock to the correct time:

clock set 15:15:00 might 31 2001

You can specify multiple syslog servers for redundancy, because syslog uses UDP as the underlying transport mechanism and data packets are unsequenced and unacknowledged.

In addition to the syslog messages from Cisco Unified CME, you can also set up Cisco Unity Express for logging to an external syslog server in addition to logging a message locally to its own storage. Use the following command:

```
CUE(config)# log server 10.10.10.1
```

Monitoring Call Activity

NMS systems can retrieve CDRs and call history information in any of the following ways:

- Cisco Unified CME GUI
- Syslog or RADIUS servers
- SNMP CISCO-DIAL-CONTROL-MIB and CISCO-VOICE-DIAL-CONTROL-MIB
- Voice performance statistics from Cisco Unified CME

The next sections describe how you can monitor call activities, CDR logs, billing records, and voice performance statistics in more detail.

Monitoring Cisco Unified CME Call History

The Cisco Unified CME GUI provides call history information in the **Reports** > **Call History** window so that a network administrator can monitor for unknown callers or disallowed calling activities based on calling patterns. Configure the call history log to perform any forensics and accounting to track down fraudulent calling patterns, as shown in the following example.

```
dial-control-mib retain-timer 10080
dial-control-mib max-size 500
!
gw-accounting syslog
logging 10.10.10.1
```

Logging CDR to External Servers

You might follow the same method discussed earlier in the "Monitoring IP Phones Using Cisco Unified CME Syslog Messages" section on page 11-5 to allow syslog messages to be logged to an external server and to log CDRs to an external server. Cisco Unified CME allows you to log CDRs for accounting or billing purposes to an external AAA server (RADIUS or TACACS). This provides CDR logging, post call record processing, and a billing report generation facility. You can use a MindCTI (http://www.mindcti.com/) RADIUS server or a Cisco Secure Access Control Server (Cisco Secure ACS) to provide billing support and view CDR details.

To configure RADIUS on your Cisco Unified CME router, perform the following tasks:

- Use the **aaa new-model** global configuration command to enable AAA. You must configure AAA if you plan to use RADIUS.
- Use the **aaa authentication** global configuration command to define method lists for RADIUS authentication.
- Use the **line** and **interface** commands to allow the defined method lists to be used.

The following example is a sample configuration that allows the Cisco Unified CME router to generate and send VoIP CDRs to an external RADIUS server.

```
aaa new-model
aaa authentication login default group radius
!! Login Authentication using RADIUS server
aaa authorization config-commands
aaa authorization exec default if-authenticated group radius
aaa authorization network default group radius
!! Authorization for network resources
aaa authorization configuration default group radius
!! Authorization for global config mode
```

```
aaa accounting send stop-record authentication failure
!! Start-Stop Accounting services
aaa accounting update periodic 1
aaa accounting network default start-stop group radius
!! For local Authentication
aaa accounting connection default start-stop group radius
!! For local Authentication
aaa accounting connection h323 start-stop group radius
!! For Voice Call Accounting
aaa accounting system default start-stop group radius
aaa accounting resource default start-stop group radius
aaa session-id common
!
gw-accounting h323
!!  H.323 gateway Accounting
gw-accounting syslog
!! Optional - for system log information
gw-accounting voip
!! VoIP call Accounting
!
Router RADIUS Server configuration:
radius-server host 11.11.11.1 auth-port 1645 acct-port 1646
!! RADIUS Server host address
radius-server retransmit 30
!!  RADIUS messages update interval
radius-server key cisco
!! RADIUS server secure key
```

Using Account Codes for Billing

Cisco Unified CME provides account code support into CDRs, which a RADIUS server or customer billing server then can use for the billing process. The Cisco Unified IP Phone 7960 and Cisco Unified IP Phone 7940 both support an account softkey so that users can enter an account code from an IP phone during the call ringing (alerting) or active (connected) states. This account code is also added to the Cisco-VOICE-DIAL-CONTROL-MIB SNMP MIB.

You can view the Account Code field in the **show call active voice** log, as shown in Example 14-41.

```
Router# show call active voice
Telephony call-legs: 2
SIP call-legs: 0
H.323 call-legs: 0
MGCP call-legs: 0
Total call-legs: 2
!
GENERIC:
SetupTime=97147870 ms
Index=1
PeerAddress=2001
!
TELE:
AccountCode 1234
```

Monitoring Voice Performance Statistics

If you are running Cisco IOS release 12.3(4)T or later, you can take advantage of the Cisco Voice Performance Statistics to collect voice call signaling statistics and VoIP AAA accounting statistics based on user-configured time ranges. The statistics can be displayed on your console or can be formatted and archived to an FTP or syslog server. This feature can help you diagnose performance problems on the network, and identify impaired voice equipment.

The following example shows an example of the amount of memory used for accounting and signaling call statistics records (CSR) by fixed interval and following a reset or reboot. It also shows the estimated memory allocated for future use.

```
Router# show voice statistics memory-usage csr
*** Voice Call Statistics Record Memory Usage ***
        Fixed Interval Option -
                CSR size: 136 bytes
                Number of CSR per interval: 9
                Used memory size (proximate): 0
                Estimated future claimed memory size (proximate): 10
        Since Reset Option -
                CSR size: 136 bytes
                Total count of CSR: 9
                Used memory size (proximate): 1224

*** Voice Call Statistics Accounting Record Memory Usage ***
        Fixed Interval Option -
                ACCT REC size: 80 bytes
                Number of ACCT REC per interval: 1
                Used memory size (proximate): 0
                Estimated future claimed memory size (proximate): 25
        Since Reset Option -
                ACCT REC size: 80 bytes
                Total count of ACCT REC: 1
                Used memory size (proximate): 80
```

Using Cisco Unified CME Supported SNMP MIBs

You might leverage Cisco SNMP router MIBs for Cisco Unified CME management. The following are examples of supported MIBs:

- **CISCO-DIAL-CONTROL-MIB**—Contains information for CDRs and call history
- **CISCO-VOICE-DIAL-CONTROL-MI**B—Extends call detail information to telephony and VoIP dial peers/call legs
- **CISCO-VOICE-IF-MIB**—Allows access to voice interface parameters such as loss and gain values and echo cancellation status
- **CISCO-CDP-MIB**—Lets you manage CDP
- **CISCO-SYSLOG-MIB**—Allows access to syslog messages
- **CISCO-CCME-MIB**—Provides IP phone registration status, fault monitoring parameters and trap notifications.

For more information about Cisco Unified CME MIB support, see the following URLs:

- *Cisco CallManager Express 3.4 SNMP MIB Support*
  http://www.cisco.com/en/US/products/sw/voicesw/ps4625/products_mib_quick_reference_book09186a008056b4ec.html

- *CISCO-CCME-MIB Overview*
  http://www.cisco.com/en/US/products/sw/voicesw/ps4625/products_mib_quick_reference_chapter09186a00805567ba.html#wp1192528

Note **CISCO-CCME-MIB** is supported by the Cisco Unified Operations Manager to provide fault monitoring.

Managing Cisco Unified CME Systems

This section addresses management of Cisco Unified CME systems in the following separate sections:

Cisco Unified CME Management Overview

Service providers (SP) normally deploy Cisco Unified CME systems as one of the following:

- Standalone, single-site managed services
- Large-scale, multisite managed services

A managed-services solution with Cisco Unified CME offers two opportunities for value-added services:

- The customer premises equipment (CPE) router
- Network management support

SPs offer their customers the Cisco Unified CME systems at the end customer's site. They also install, set up, maintain, and manage the systems.

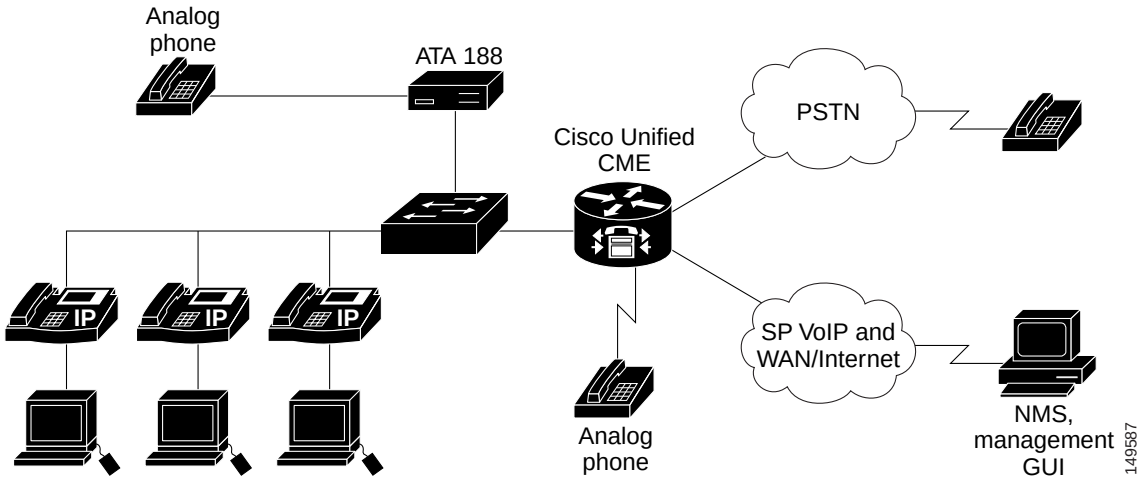
Most of the network management systems (NMS) used by SPs to deploy Cisco Unified CME in a managed-services model also apply to enterprise networks. The difference between a managed-services model and an enterprise model is who offers, owns, and manages the core network.

Note Note that this section covers only management capabilities for Cisco Unified CME systems, not for the larger IP telephony solutions and products offered by Cisco in general. The next sections describe how you can manage standalone or multisite Cisco Unified CME systems. They also cover some general information on the typical Cisco Voice Network Management Solutions that are applicable to Cisco Unified CME.

Managing a Standalone Cisco Unified CME System

Figure 11-1 shows a deployment in which a single Cisco Unified CME system in a branch office connects to a SP VoIP network. All voice and data traffic can be routed over the SP network, or calls can be routed by the PSTN if the destination (called party) cannot be reached via the SP IP network.

Figure 11-1 Managing a Standalone Cisco Unified CME System



To manage a standalone Cisco Unified CME system, we recommend that you provision or configure the system by using the Cisco Unified CME Quick Configuration Tool (QCT) 3.0 to setup your system with basic functionality. You can, as option, use the CLI, the Cisco Unified CME setup utility, or the Cisco Unified CME GUI. This is sufficient for simple moves, adds, changes to the phones, and basic configuration changes for a standalone or single-site deployment. However, you might also use the Zero Touch deployment, monitoring, accounting, and billing management capabilities for multisite Cisco Unified CME deployments.

Cisco Zero Touch Deployment

Cisco Networking Services technology provides the infrastructure for automated configuration of large numbers of network devices. Based on Cisco Networking Services event and configuration agents, it eliminates the need for an on-site technician to initialize the devices. The Cisco Networking Services Zero Touch feature provides a deployment solution in which the router contacts a Cisco Networking Services Configuration Engine to retrieve its full configuration automatically. This capability is made possible through a single generic bootstrap configuration file common across all SP end customers subscribing to the services. Within the Cisco Networking Services framework, customers can create this generic bootstrap configuration without device-specific or network-specific information, such as interface type or line type.

Understanding Cisco Zero Touch Deployment Components

Cisco Zero Touch deployment consists of the following three components:

- Cisco Networking Services Configuration Express, page 11-11
- Cisco Networking Services Configuration Engine, page 11-12
- Cisco Networking Services Configuration Engine, page 11-12

Cisco Networking Services Configuration Express

Cisco Configuration Express is an online ordering system and customizable inline manufacturing process that lets SPs easily deploy customer premises equipment (CPE)-based managed services to their small-to-medium sized business and enterprise customers. When ordering Cisco products, SPs use Cisco

Configuration Express to specify the shipping instructions, including the Cisco IOS software version and a bootstrap configuration, which are configured, tested, and shipped with the CPE. The resulting fully configured CPE is shipped either directly to the end customer site or to the SP warehouse.

The bootstrap configuration integrates with Cisco Networking Services Configuration Engine the moment the CPE devices are plugged into the network at the end-customer site.

Cisco Networking Services Configuration Engine

Cisco Networking Services Configuration Engine runs on the Cisco Networking Services 2100 series Intelligence Engine (Cisco Networking Services IE 2100) hardware platform as well as customer UNIX servers. It is a secure and scalable deployment and configuration management application that provides an intelligent network interface to applications and users supporting up to 5000 Cisco CPE devices.

Cisco Networking Services Configuration Engine includes the Configuration Service and Configuration Server. The Configuration Server communicates with the Cisco Networking Services Configuration Agent running on the managed Cisco Unified CME via HTTP and transfers data in XML format parsed by the Cisco Networking Services Configuration Agent on the Cisco Unified CME router using its own parser.

The Cisco Networking Services Configuration Service delivers device and service configurations to Cisco IOS devices for initial configuration and mass reconfiguration by logical groups. Routers receive their initial configuration from the Cisco Networking Services Configuration Service when they start up on the network the first time. The Cisco Networking Services Configuration Service uses the Cisco Networking Services Event Service to send and receive events required to apply configuration changes and to send success and failure notifications.

The templates created on the Cisco Networking Services Configuration Engine are automatically pushed to the CPE devices running the bootstrap configuration.

For more information on Cisco Networking Services Configuration Engine, see the following URL: http://www.cisco.com/en/US/products/sw/netmgtsw/ps4617/tsd_products_support_series_home.html

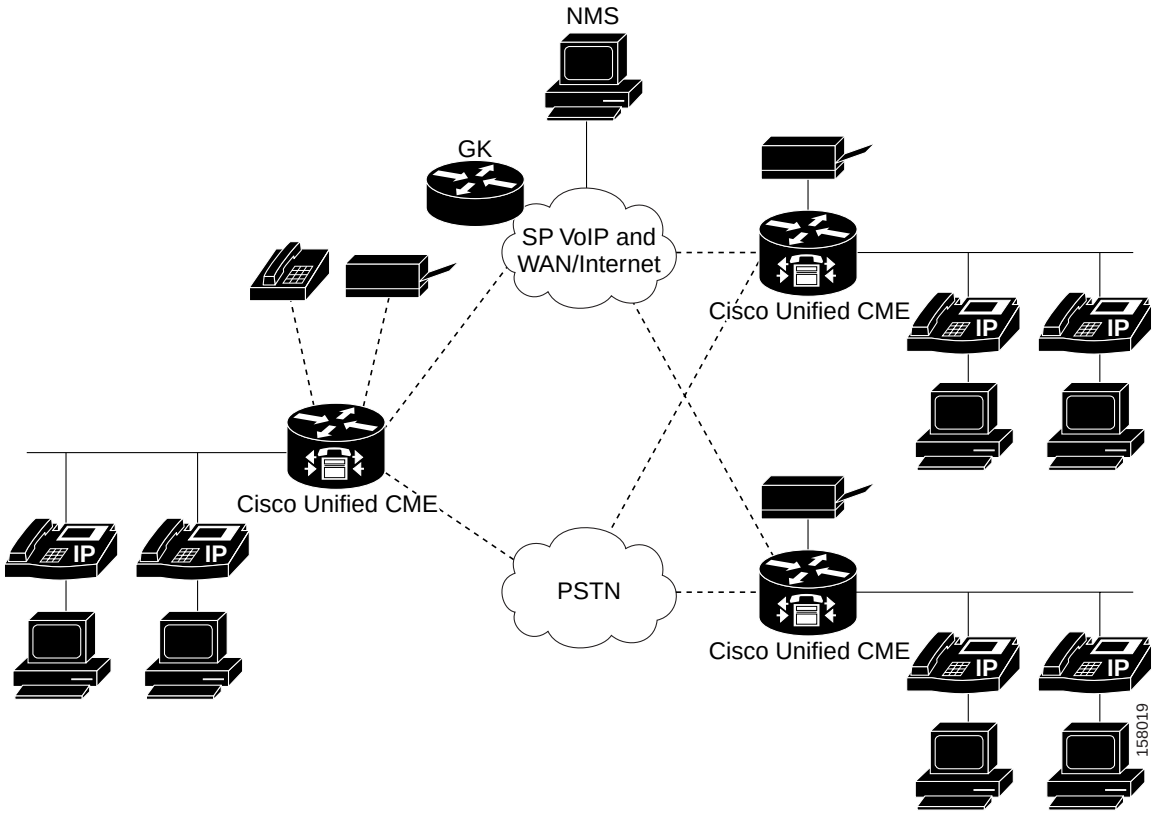
Cisco Networking Services Agent

The Cisco Networking Services Agent is built into Cisco IOS devices to provide intelligence to connect to the Cisco Networking Services Configuration Engine. Using its bootstrap configuration, the CPE device, such as Cisco Unified CME, polls the network and provides inventory to the Cisco Networking Services Configuration Engine.

Managing Multisite Cisco Unified CME Networks

You can also deploy Cisco Unified CME in large-scale enterprise networks or in managed-services networks. Figure 11-2 shows multiple small and medium business or enterprise branch office Cisco Unified CME sites connected to the SP VoIP network.

Figure 11-2 Managing a Multisite Cisco Unified CME Network



When deploying Cisco Unified CME systems in a multisite environment, provisioning, configuring, and managing only one Cisco Unified CME system at a time is insufficient.

Managing Cisco Unified CME Systems with Cisco Network Management Tools

The following sections summarize the Cisco tools that we recommends for managing your Cisco Unified CME systems:

- Cisco Unified CME Quick Configuration Tool, page 11-13
- Cisco Unified Operations Manager and Cisco Unified Service Monitor, page 11-14

Cisco Unified CME Quick Configuration Tool

We recommend using the Cisco Unified CME Quick Configuration Tool (QCT) to install and initialize Cisco Unified CME. For information about the Cisco Unified CME QCT, see the following URLs:

- *Cisco Unified CME QCT Data Sheet*
  http://www.cisco.com/en/US/products/sw/voicesw/ps4625/products_data_sheet0900aecd802e9be9.html
- *Configuring Your System Using Cisco IPC Express Quick Configuration Tool*
  http://www.cisco.com/en/US/products/sw/voicesw/ps4625/products_installation_guide_chapter09186a0080527133.html

Use the following link to download the Cisco Unified CME QCT software:

- http://www.cisco.com/pcgi-bin/tablebuild.pl/cme-qct

Cisco Unified Operations Manager and Cisco Unified Service Monitor

We recommend using the Cisco Unified Operations Manager and Cisco Unified Service Monitor to manage and monitor Cisco Unified CME systems.

Cisco Unified Operations Manager

The Cisco Unified Operations Manager is a separate software application that does not use any agents on any Cisco Unified Communications device or application. It resides on a separate server and uses standards-based access mechanisms, such as SNMP polling, HTTP polling, trap processing, and other diagnostic tests to ascertain the current operational status of the Cisco Unified Communications deployment and makes that information available via either the Cisco Unified Operations Manager user interfaces or other interfaces such as syslogs, SNMP traps or emails.

Cisco Unified Operations Manager provides fault monitoring and management of Cisco Unified CME with the following capabilities:

- Cisco Unified CME in Service Level Views
- Real-time alerts on Cisco Unified CME hardware and software status
- Real-time service quality alerts on calls supported by Cisco Unified CME
- Discovery of Cisco Unified CME and the inventory details,
- Version, maximum number of ephones, extensions, and conference calls
- Current status (Cisco Unified CME enabled/disabled)
- Phone details (phone status and status changes)
- Phone utilization (percentage of ephones registered, key ePhones registered)
- Synthetic tests (phone registration, dial-tone, and end-to-end call)
- SNMP traps processed

You can use Cisco Unified Service Monitor in conjunction with Cisco Unified Operation Manager, by configuring Cisco Unified Operations Manager as a trap receiver for Cisco Unified Service Monitor. Cisco Unified Operations Manager can generate events for Service Monitor traps, display the events on the *Service Quality Alerts* dashboard, and store event history for up to 31 days.

For more information, see the following URLs:

- Cisco Unified Operations Manager data sheets:
  http://www.cisco.com/en/US/products/ps6535/products_data_sheets_list.html
- Technical documentation for Cisco Unified Operations Manager:
  http://www.cisco.com/en/US/products/ps6535/tsd_products_support_series_home.html

Cisco Unified Service Monitor

Cisco Unified Service Monitor analyzes data that it receives from Cisco 1040 Sensors (Cisco 1040s) installed in your voice network. Each licensed instance of Cisco Unified Service Monitor acts as a primary Cisco Unified Service Monitor for multiple Cisco 1040s. A Cisco Unified Service Monitor can also be configured to act as a secondary and tertiary Cisco Unified Service Monitor for Cisco 1040s that are managed by other licensed instances of Cisco Unified Service Monitor. When a Cisco Unified Service Monitor becomes unavailable, Cisco 1040s fail over to secondary or tertiary Cisco Unified Service Monitors temporarily until the primary Cisco Unified Service Monitor becomes available again.

Cisco Unified Service Monitor examines the data it receives from Cisco 1040s, comparing Mean Opinion Scores (MOS)—computed by Cisco 1040s for each RTP stream—against a user-specified threshold value. When MOS drops below the threshold, Service Monitor generates SNMP traps and sends them to up to four trap receivers. Optionally, Service Monitor stores the call metrics it receives from Cisco 1040s to disk files.

Cisco Unified Service Monitor provides real-time measurement of voice quality and mean opinion score (MOS) reporting to provide the following capabilities:

- Unified dashboard to monitor the whole system and to rapidly troubleshoot problems
- Real-time view of Cisco Unified Communications System
- Alerting and diagnostics
- Phone and device inventory reports (phone status and phone tracking)

For more information, see the following URLs:

- Cisco Unified Service Monitor data sheets: http://www.cisco.com/en/US/products/ps6536/products_data_sheets_list.html
- Technical documentation for Cisco Unified Service Monitor: http://www.cisco.com/en/US/products/ps6536/tsd_products_support_series_home.html

Managing Cisco Unified CME Systems with Cisco Partner Applications

In addition to the Cisco management solutions discussed in the previous sections, various Cisco partners offer management solutions. This section describes these solutions:

- NetIQ Vivinet Manager, page 11-15
- Stonevoice, page 11-21
- ISI Telemanagement Solutions Inc. Infortel Select, page 11-28
- Integrated Research Prognosis, page 11-29

NetIQ Vivinet Manager

NetIQ’s Vivinet Manager allows you to gain access to Cisco Unified CME data, and then analyze and manage Cisco Unified CME systems. With NetIQ Vivinet Manager for Cisco Unified CME, you gain easy access to a new set of tools you can leverage to gather a wide range of diagnostic and management data, which can help prevent outages and keep things running smoothly.

NetIQ Vivinet Manager for Cisco Unified CME is an add-on module to NetIQ Vivinet Manager version 2.1. Equipped with Cisco Unified CME AXL/SOAP API support, you can use Knowledge Scripts included in Vivinet Manager for Cisco Unified CME to create jobs that monitor the health, availability, and performance of key devices. These scripts allow you to monitor and manage crucial device

properties at a depth unparalleled by any other solution. You can configure each Knowledge Script to send an alert, collect data for reporting, and perform automated problem management when an event occurs.

The Vivinet Manager Knowledge Scripts let you monitor phone status (registered, unregistered, and deceased), reset IP phones, specify key phones, monitor for duplicate extensions, and show inventory information for phones attached to Cisco Unified CME systems. The following are the supported Knowledge Scripts for the Cisco Unified CME module:

- **CiscoCME_Device_Reset**—Resets Cisco Unified CME IP phones for reasons such as troubleshooting or picking up new default firmware. Use this script in conjunction with CiscoCME_Device_Status to ensure that the selected phones have upgraded successfully.
- **CiscoCME_Device_Status**—Monitors the status of key Cisco Unified CME phones.
- **CiscoCME_Extension_Check**—Monitors for duplicate phone extension numbers. This script looks for all phones configured in Cisco Unified CME, regardless of whether they are registered.
- **CiscoCME_Phone_Inventory**—Generates an inventory of the phone details for phones that are attached to Cisco Unified CME.
- **CiscoCME_Set_Key_Phones**—Designates one or more “key” phones. After you designate key phones, you can choose to monitor only key phones.

The following features are provided by NetIQ Vivinet Manager for Cisco Unified CME:

- It discovers Cisco Unified CME systems with Cisco Unified CME version and device information.
- It provides Knowledge Scripts for day-to-day and diagnostic monitoring.
- It monitors Cisco Unified CME resources, including CPU, memory, flash memory, power supplies, and temperature sensors.
- It supports Cisco Unified CME 3.0 and later.
- It monitors and reports scripts in the Network Device module in addition to the scripts created especially for the Cisco Unified CME module.

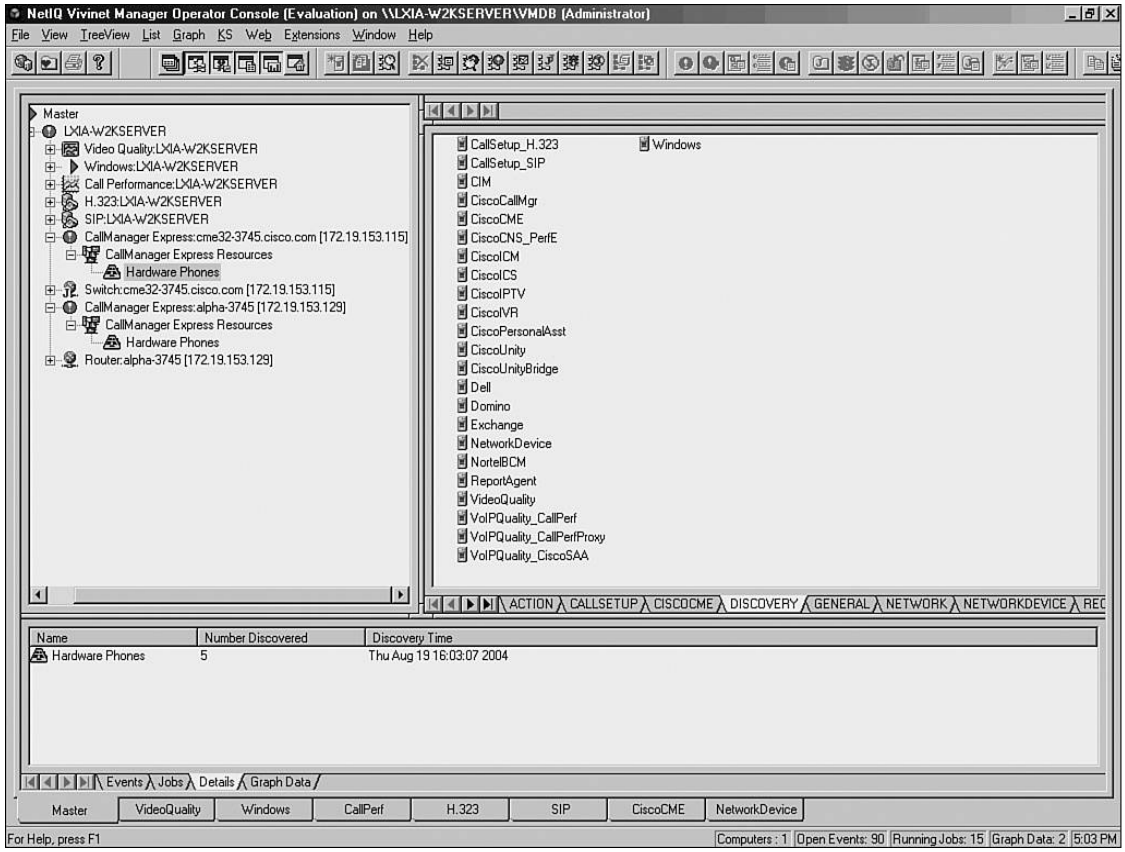
NetIQ for Cisco Unified CME is an add-on module to the NetIQ Vivinet Manager. Get the installation CD-ROM from NetIQ (http:/www.netiq.com/products/vm/) for Cisco Unified CME, and install it to the NetIQ Vivinet Manager.

The following example shows the required configuration on a Cisco Unified CME system.

```
snmp-server community public RO
! Set up the community string
!
telephony-service
   log password abcd
   no xmltest
   ! doesn’t show when “no xmltest” is configured
   no xmlschema
   ! doesn’t show when “no xmlschema” is configured
```

Figure 11-3 shows the operator console of NetIQ Vivinet Manager for Cisco Unified CME.

Figure 11-3 NetIQ Vivinet Manager Operator Console for Cisco Unified CME



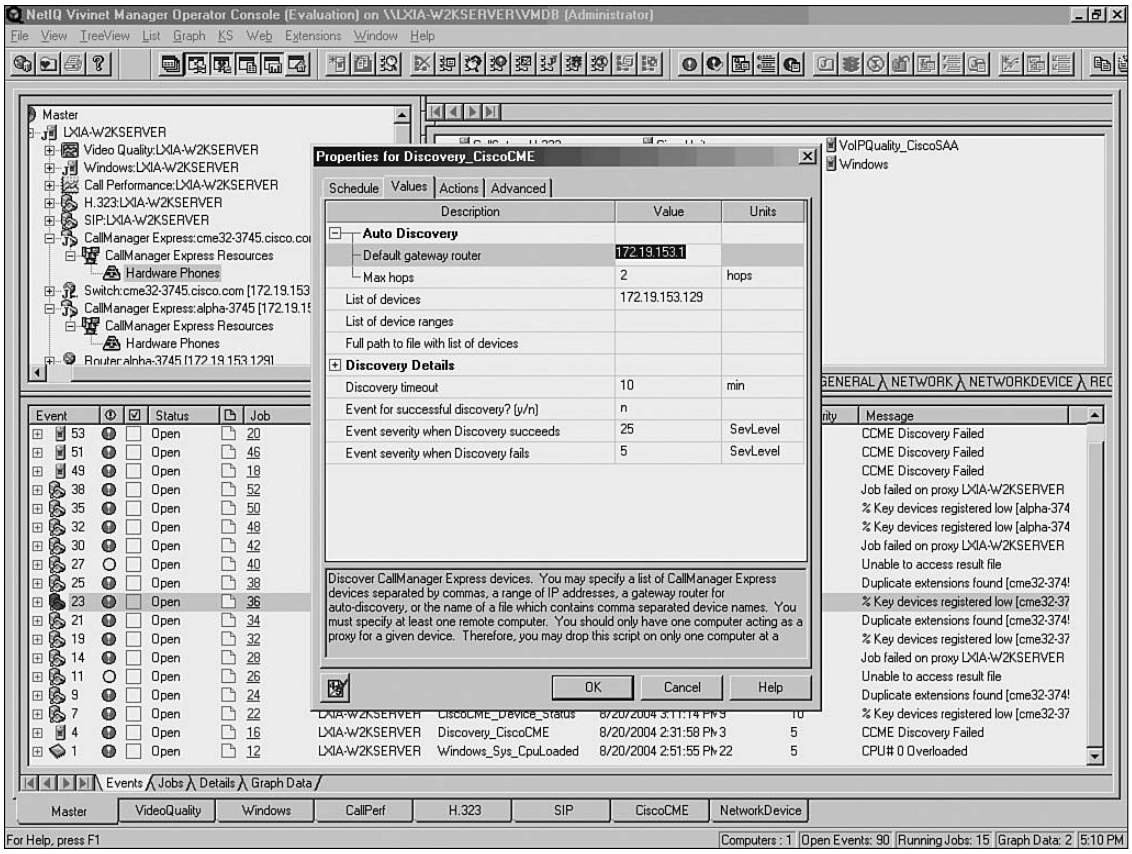
The following sections provide some highlights of how you can use the NetIQ Vivinet Manager for Cisco Unified CME.

Discovery of Cisco Unified CME

You might use the Discovery script (Discovery_CiscoCME) found on the Discovery tab of the Knowledge Script pane to discover the Cisco Unified CME managed object on a device in the TreeView pane of the Operator Console.

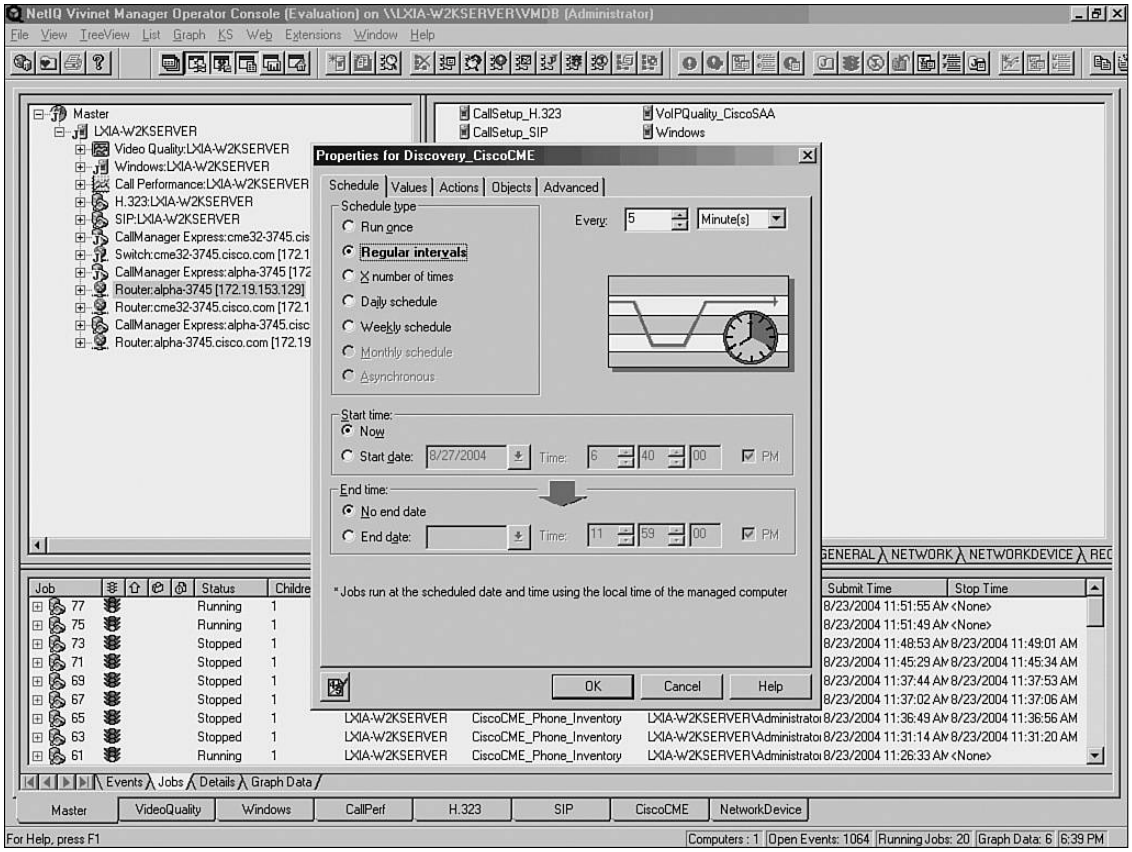
From the Discovery tab of the Knowledge Script pane, drag and drop the Discovery_CiscoCME script onto a proxy computer in the TreeView pane. Set the Values tab parameters, as shown in Figure 11-4.

Figure 11-4 Discovery Property



To set when you want to run the Discovery script, click the Schedule tab which will then result in the popup window shown in Figure 11-5.

Figure 11-5 Scheduling a Job

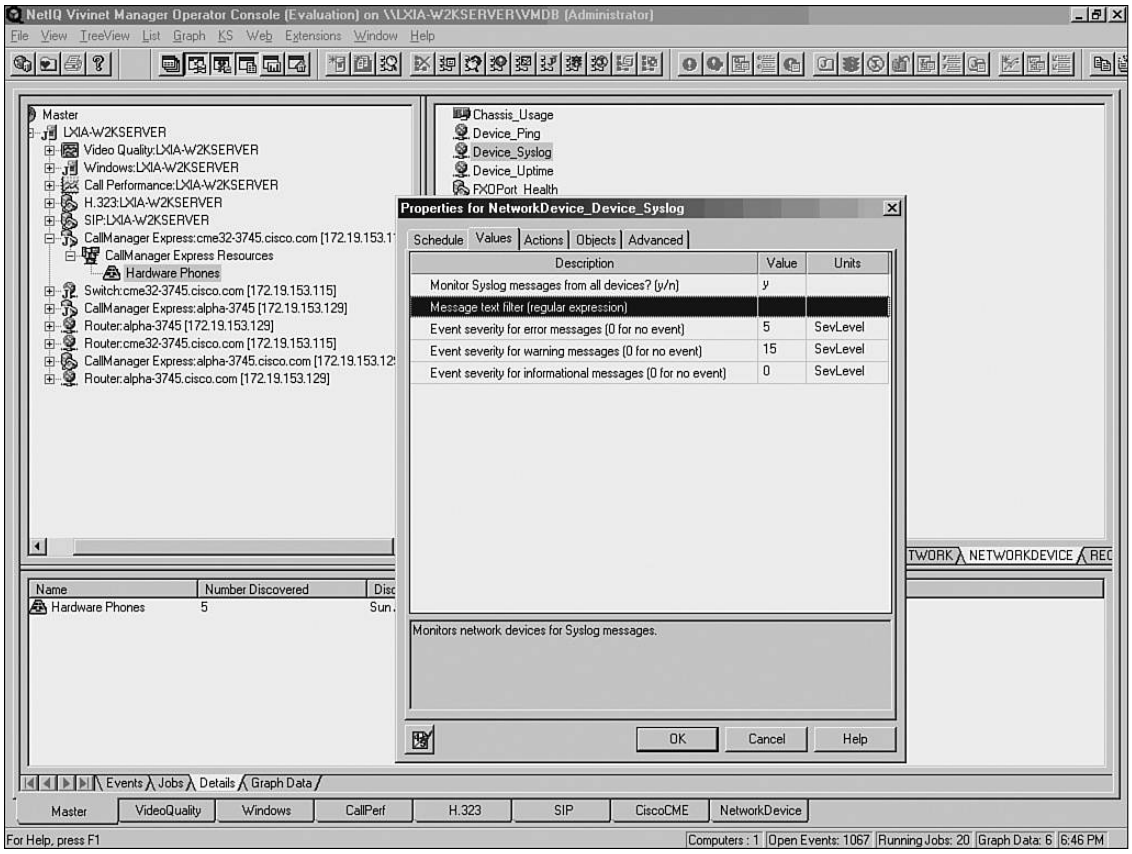


Choose the Schedule type to run once, at regular intervals, or on a daily/weekly schedule. Select a Start time and End time, and then click **OK** to schedule a job. The job scheduled is displayed in the Jobs tab as Running or as Stopped if the job is complete.

Monitoring New Phones

You can use the NetworkDevice_Device_Syslog script to inform you when a configured phone (known) or a new phone (unknown) registers with a Cisco Unified CME. In the NETWORKDEVICE pane, drag and drop Device_Syslog onto a Cisco Unified CME router in the TreeView panel. The Properties for NetworkDevice_Device_Syslog window appears, as shown in Figure 11-6.

Figure 11-6 Device Syslog Setup



In the Values tab, change the value for Monitor Syslog messages from all devices? (y/n) to y, and change other values if needed. You might configure an action to be taken (in the Actions tab) when events or errors occur.

As described in the "Monitoring IP Phones Using Cisco Unified CME Syslog Messages" section on page 11-5, a syslog message is generated when an IP phone registers with Cisco Unified CME. In addition, a different syslog message is generated when a new or unknown phone requires Cisco Unified CME to create an ephone configuration entry. You can configure NetworkDevice_Device_Syslog to watch for these entries and to generate events as needed.

When a new phone registers and has no ephone configuration entry, the register message is IPPHONE-6-REGISTER_NEW. When a configured phone registers, the register message is simply IPPHONE-6-REGISTER. The following example gives a sample registration message.

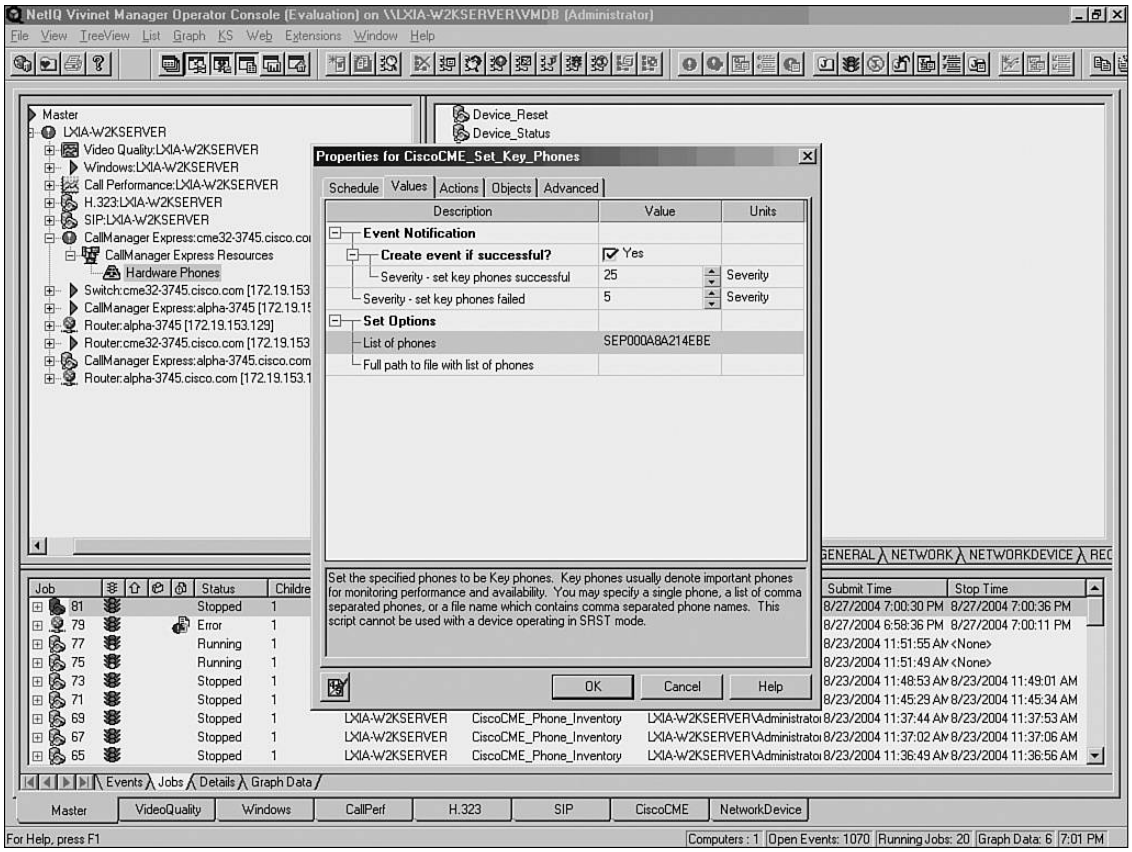
```
1w2d: %IPPHONE-6-REG_ALARM: 25: Name=SEP00036B7FFF59 Load=3.2(2.14)Last=
  Initialized
1w2d: %IPPHONE-6-REGISTER_NEW: ephone-4: SEP00036B7FFF59 IP:192.168.1.16 Socket:3
  DeviceType:Phone has registered. Reseting SEP00036B7FFF59
1w2d: %IPPHONE-6-UNREGISTER_NORMAL: ephone-4: SEP00036B7FFF59 IP:192.168.1.16 Soc
ket:3 DeviceType:Phone has unregistered normally.
1w2d: %IPPHONE-6-REG_ALARM: 22: Name=SEP00036B7FFF59 3 Load=3.2(2.14)Last=
  Reset-Reset
1w2d: %IPPHONE-6-REGISTER: ephone-4: SEP00036B7FFF59 IP:192.168.1.16 Socket:3
  DeviceType:Phone has registered.
```

Managing Key Phones

You might set certain phones as key phones so that you monitor only a selected set of important phones. You can use the CiscoCME_Set_Key_Phones Knowledge Script to designate one or more phones as key phones. Although you can use a Knowledge Script to set a key phone, you must use the CLI to remove a key designation from a phone.

Drag and drop Set_Key_Phone on the Cisco Unified CME Resource in the TreeView. Configure the MAC address of the phone you want to set as a key phone, or configure a filename with a full path if multiple phones are being established as key phones, as shown in Figure 11-7.

Figure 11-7 Setting Key Phones



Stonevoice

Stonevoice, a business unit of Computer Design in Italy, offers an application suite for Cisco Unified CME IP Telephony Solutions with the following capabilities:

- **Switch Answering Machine (SSAM)**—Manages voice mail integration with Cisco Unified CME via H.323.
- **Billy**—A call accounting and reporting tool based on CDR records (see Figure 11-8).
- **IVR Manager**—Equipped with canned scripts and prompts.
- **Concerto**—An MOH server to change a music file on-the-fly.

- **Speedy**—A directory manager that lets users add, delete, or modify public and personal directories.
- **CallBarring**—Call blocking and restriction based on time and day.
- **Service Manager**—An embedded tool to manage XML services and user subscriptions.
- **Idle URL Manager**—Displays text and images on the phone display when the phone is idle.

The View Call Report window associated with the Stonevoice Billy accounting application is shown in Figure 11-8.

Figure 11-8 View Call Report Window Associated with Billy Accounting Application

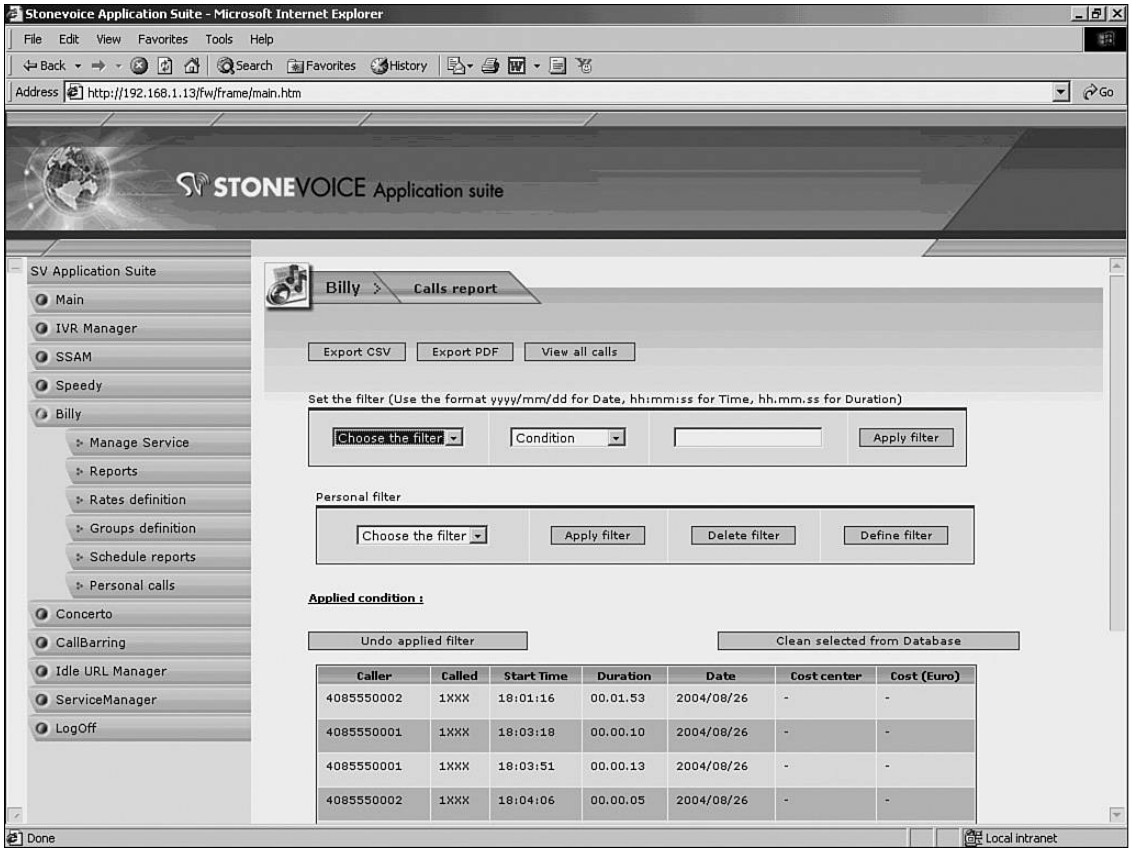


Figure 11-9 shows the IVR Manager window through which you can set up different system behaviors.

Figure 11-9 Using IVR Manager to Set Up Behaviors

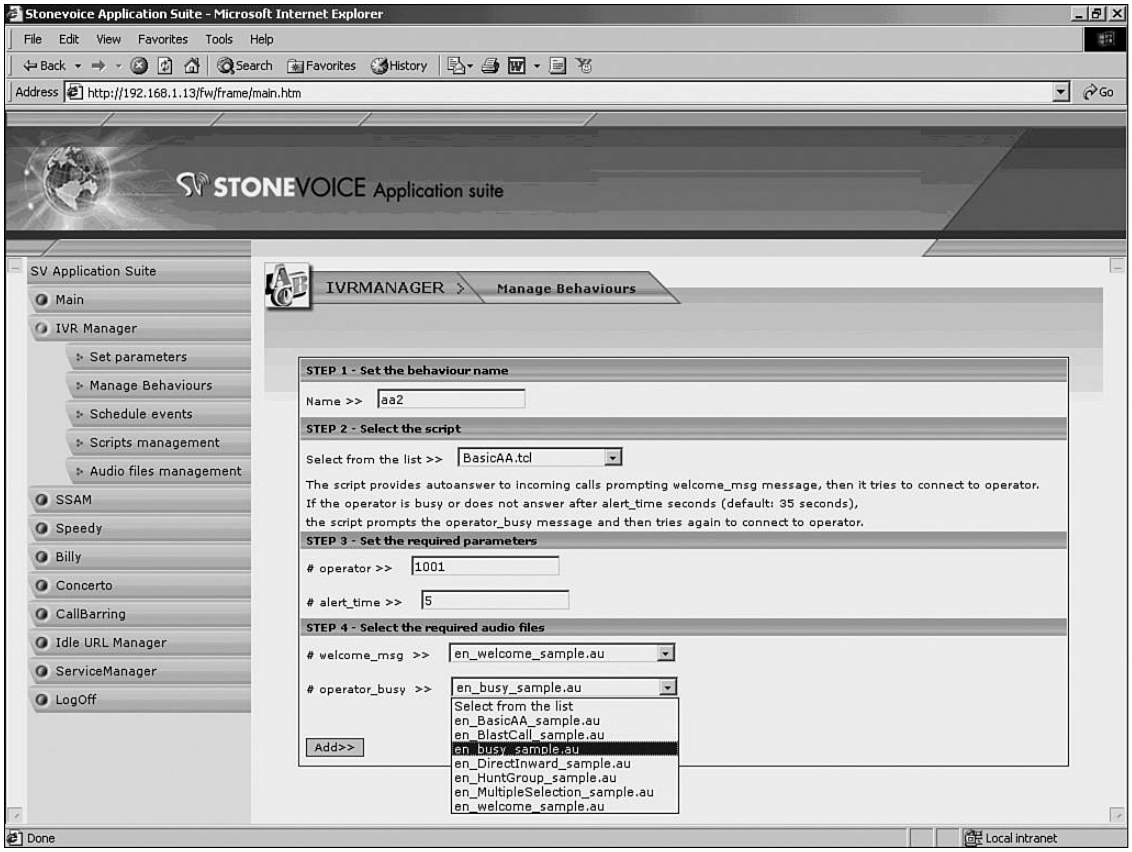


Figure 11-10 shows the IVR Manager window through which you can review the TCL scripts in your system and where you can run a particular TcL script.

Figure 11-10 Viewing TcL scripts using IVR Manager:

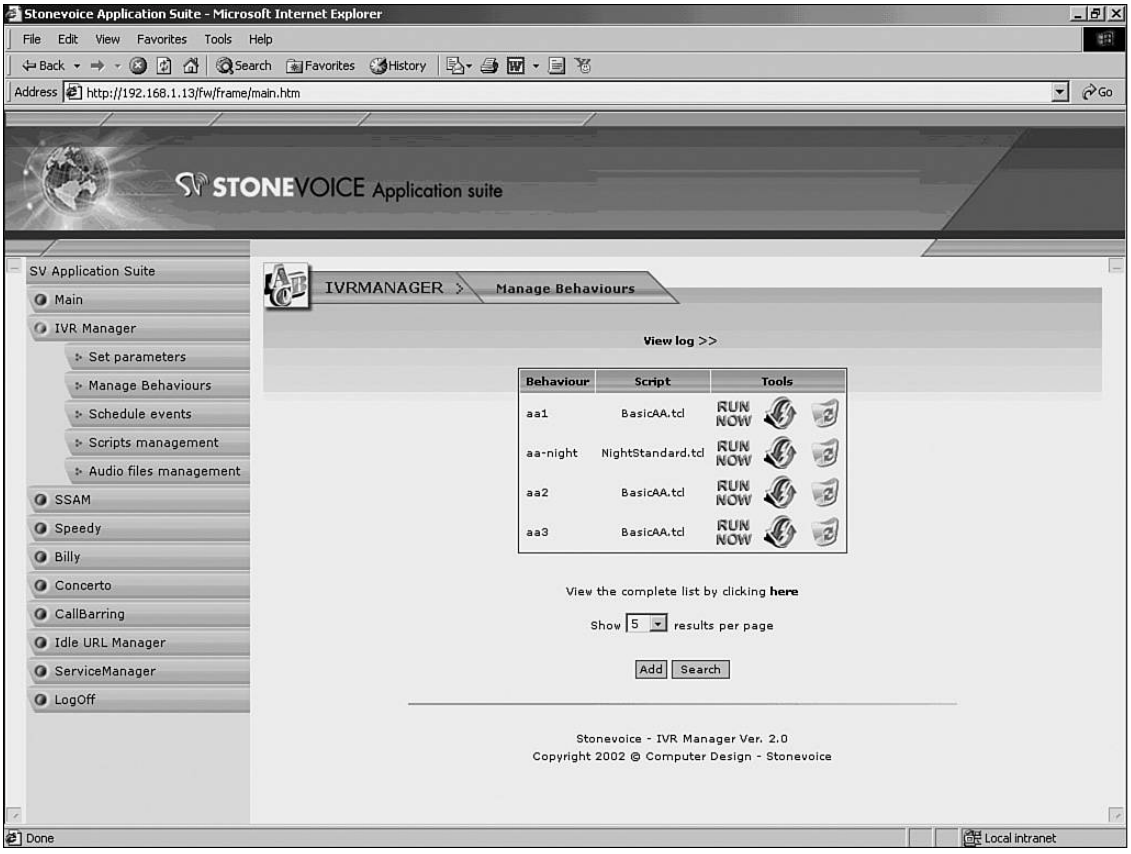


Figure 11-11 shows the IVR Manager window through which you can manage TcL scripts.

Figure 11-11 Managing TcL scripts using IVR Manager

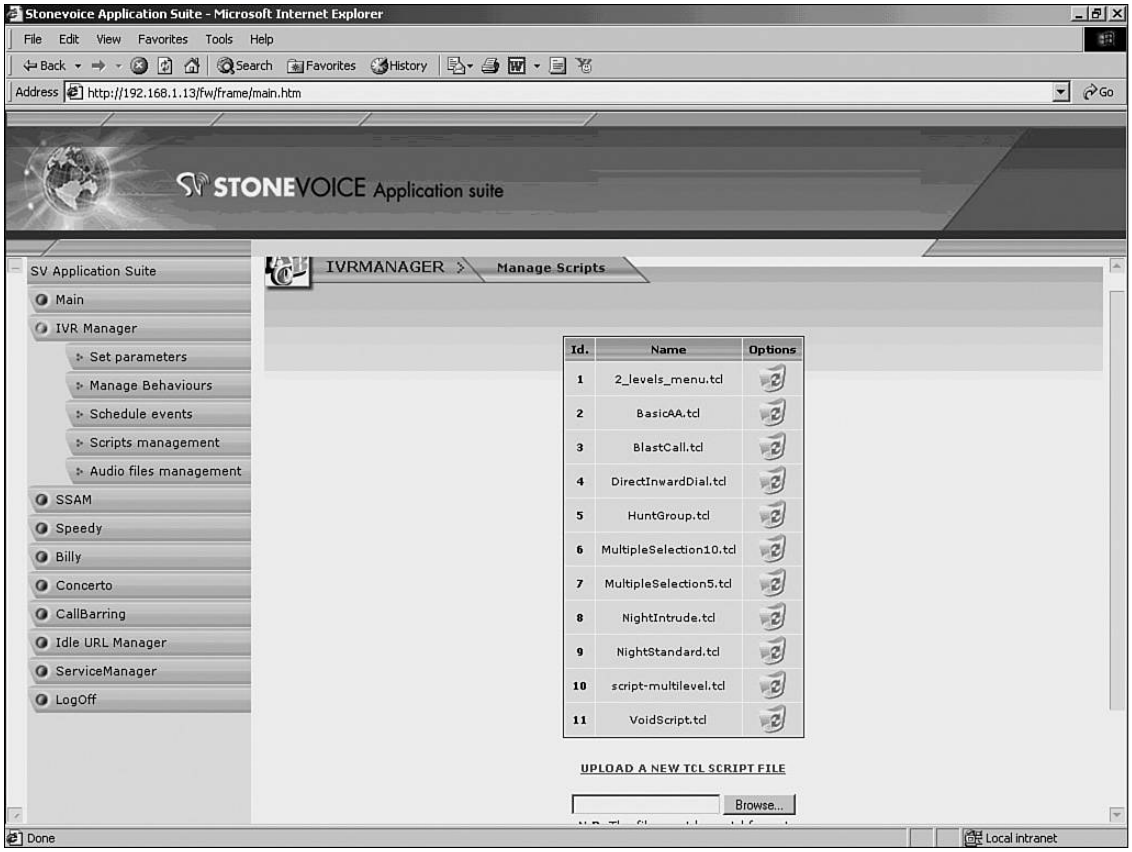


Figure 11-12 shows the IVR Manager window through which you can manage .wav and .au audio files on your system.

Figure 11-12 Managing Audio Files using IVR Manager

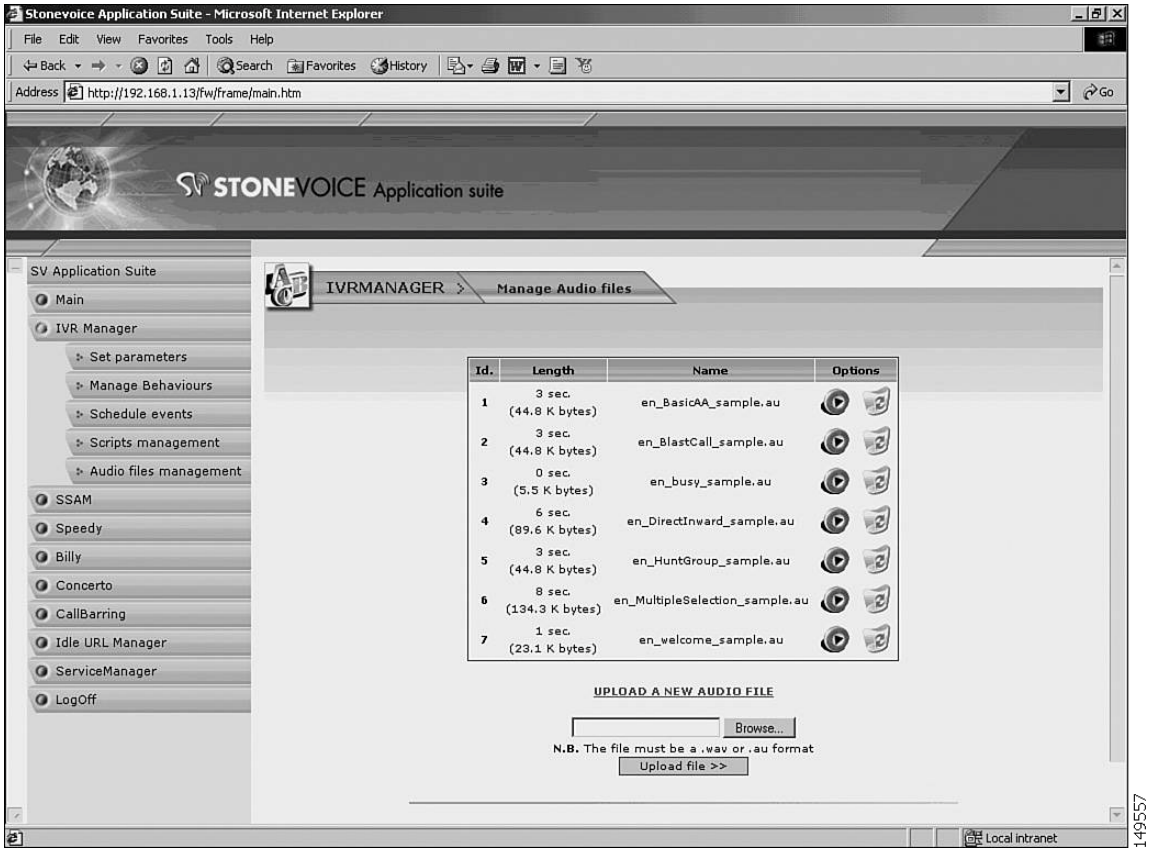


Figure 11-13 illustrates the Concerto MOH management application window.

Figure 11-13 Uploading a MOH File using Concerto

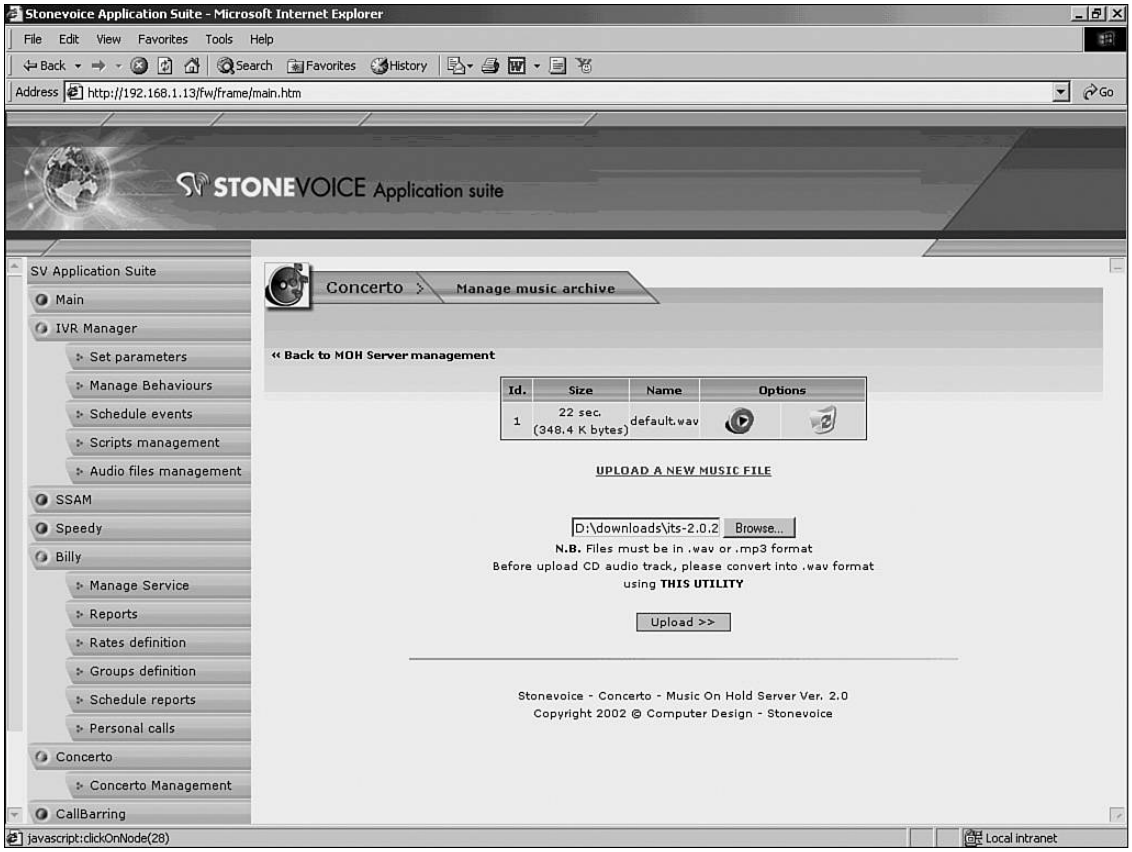
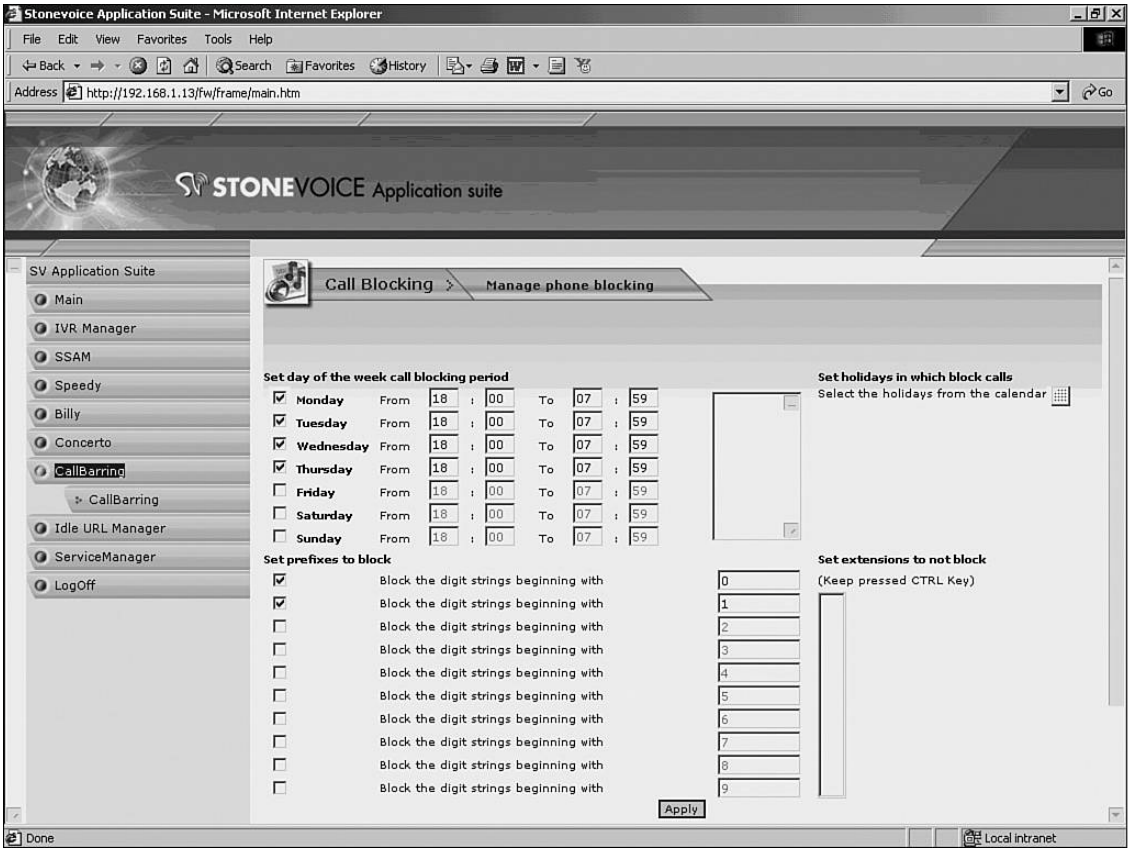


Figure 11-14 shows the CallBarring application window, which lets you set up digit strings that might not be called.

Figure 11-14 Setting Up Call Blocking using CallBarring



ISI Telemanagement Solutions Inc. Infortel Select

Infortel Select from ISI Telemanagement Solutions, Inc.can be used for tracking billing information for Cisco Unified CME. ISI provides the following functions:

- Infortel Select provides leading call accounting solutions
- Infortel Select helps you manage costs, improve productivity and increase profitability through control of your telecom environment
- Usage-based allocation of variable and fixed telecommunications expenses
- Identification of potential abuse or misuse
- Analysis of telephone-related employee productivity
- Analysis of traffic and trunk utilization for troubleshooting and facility planning
- Investigation of corporate security concerns
- Historical archive of call activity

Note For more information, see this URL: http://www.isi-info.com/

Integrated Research Prognosis

Integrated Research's *Prognosis* tool can be used for monitoring Cisco Unified CME and Cisco Unity Express. Prognosis provides the following monitoring functions:

- Call quality monitoring—Monitors latency, packet loss, jitter and MOS scoring
- Availability monitoring —Monitors dash board view of phone, device and call availability; monitors percentage of phones and devices up and down
- Call detail metrics—Monitors call types and route patterns, origin and duration of calls
- Key phone metrics—Monitors offhook, registration, mac-address data
- Configuration metrics—Monitors phone, h323 gateway, dial-peer, telephony-service, software/hardware inventory
- Systems and protocol monitoring—Monitors CPU and process memory, software version, application/voice traffic

Note For more information, see this URL: http://www.prognosis.com/