Overview of Cisco EGW 2200

Updated June 1, 2005
Current through Release 1.1(2)

The Cisco EGW 2200 Enterprise Gateway is a media gateway controller that serves as a migration tool for optimizing the transition from existing Digital Private Network Signaling System (DPNSS) PBX enterprises to Cisco CallManager. The Cisco EGW also introduces Cisco Unity into existing DPNSS or QSIG PBX enterprises and supports Toll Bypass for QSIG and DPNSS PBXs. In these deployment scenarios, the Cisco EGW acts as an adjunct to Cisco CallManager and Cisco Unity to complete a connection to the PSTN.

The Cisco EGW consists of an MCS 78*xx* (Media Convergence Server) computer featuring call-control and administrative software.

This chapter contains the following topics:

- Cisco EGW 2200 in the Network Architecture, page 2
- Overview of Cisco EGW 2200 Software, page 3
- Cisco EGW 2200 Communication with Network Components, page 6
- Overview of the Cisco IPT Platform Administration Tool, page 9
- Overview of Cisco EGW 2200 Routes, Route Plans, and Dial Plans, page 12
- Cisco EGW 2200 Workflow, page 13
- Cisco EGW 2200 Alarms, page 14
- Cisco EGW 2200 Call History, page 15

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Cisco EGW 2200 in the Network Architecture

When deployed with Cisco CallManager, Cisco EGW provides signaling, routing, and DPNSS interworking that allows advanced DPNSS calling features to operate transparently between legacy DPNSS PBXs and Cisco CallManager. For more information, go to the following URL:

http://www.cisco.com/iamegw/planning/planning_sol_ippbx.htm

When deployed with Cisco Unity, Cisco EGW provides signaling, routing, and DPNSS or QSIG interworking that allows the legacy QSIG or DPNSS PBXs to operate with Cisco Unity Voice Mail and Unified Messaging applications. For more information, go to the following URL:

http://www.cisco.com/iamegw/planning/planning_sol_unity.htm

Cisco EGW also supports Toll Bypass between legacy PBXs and can serve as a gateway to the PSTN through a PRI ISDN trunk.

Typically, Cisco EGW is deployed in a fault-tolerant pair where one system is active and the other is in standby mode, and call processing can automatically switch over to the standby system for any of these reasons:

- The active system encounters a problem.
- Maintenance activities (such as a software upgrade) is to be performed on the active system.

The active system is provisioned, and when the system is updated, the provisioning data is automatically copied to the standby system.

When serving as an adjunct to Cisco CallManager, Cisco EGW is typically installed in the same location as the Cisco CallManager cluster. Figure 1 shows an example of how Cisco EGW can be positioned in an Enterprise network.

Figure 1 Cisco EGW 2200 Network Environment Architecture

Overview of Cisco EGW 2200 Software

Cisco EGW 2200 release 1.1(2) software is pre-loaded. You install and configure the software at first use. The following components are included in the software:

- Linux operating system Red Hat Enterprise Advanced Server 3.0
- Cisco EGW 2200 call-control application, which includes an H.323 Signaling Interface (HSI)
- Cisco EGW Administration, a browser-accessible application for provisioning network components
- Cisco IPT Platform Administration, a browser-accessible application for administering Cisco appliances, managing updates, and backing up data
- Command-line interface providing a subset of Cisco IPT Platform Administration functions

Note The Linux operating system is not user accessible. You can manage the platform by using Cisco IPT Platform Administration.

Cisco EGW 2200 Secure Communications

The Cisco EGW 2200 software provides secure communication channels to external computer systems. Cisco EGW 2200 supports secure interfaces (ssh, sftp) for operations that communicate with external systems, such as backup and restore and performing upgrades. The Cisco EGW 2200 software is export-restricted and can be obtained through controlled channels only.

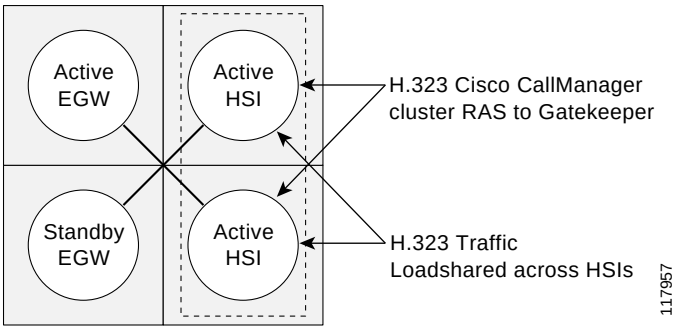
Cisco EGW 2200 Call Control and HSI

Cisco EGW consists of a core call-control module and an H.323 Signaling Interface (HSI) module. In a system featuring only one Cisco EGW, this interconnection is transparent to the user. In a duplex system (that is, a system consisting of two Cisco EGWs), the interconnection is less transparent because while the call-control module is only active on one Cisco EGW host, the HSI module runs in an active mode on both hosts.

Figure 2 shows that the HSI runs in the active mode on the active and standby hosts. This feature provides loadsharing ability on the H.323 interface.

Note The H.323 network relies on TCP/IP connections, and if these connections fail because of a network or hardware failure, then calls will be lost. A duplex system will load-balance calls across the system to reduce loss of calls in a failure condition, and ensure that resources remain available for further calls.

Figure 2 HSI Operation in a Fault-Tolerant Cisco EGW 2200 Configuration



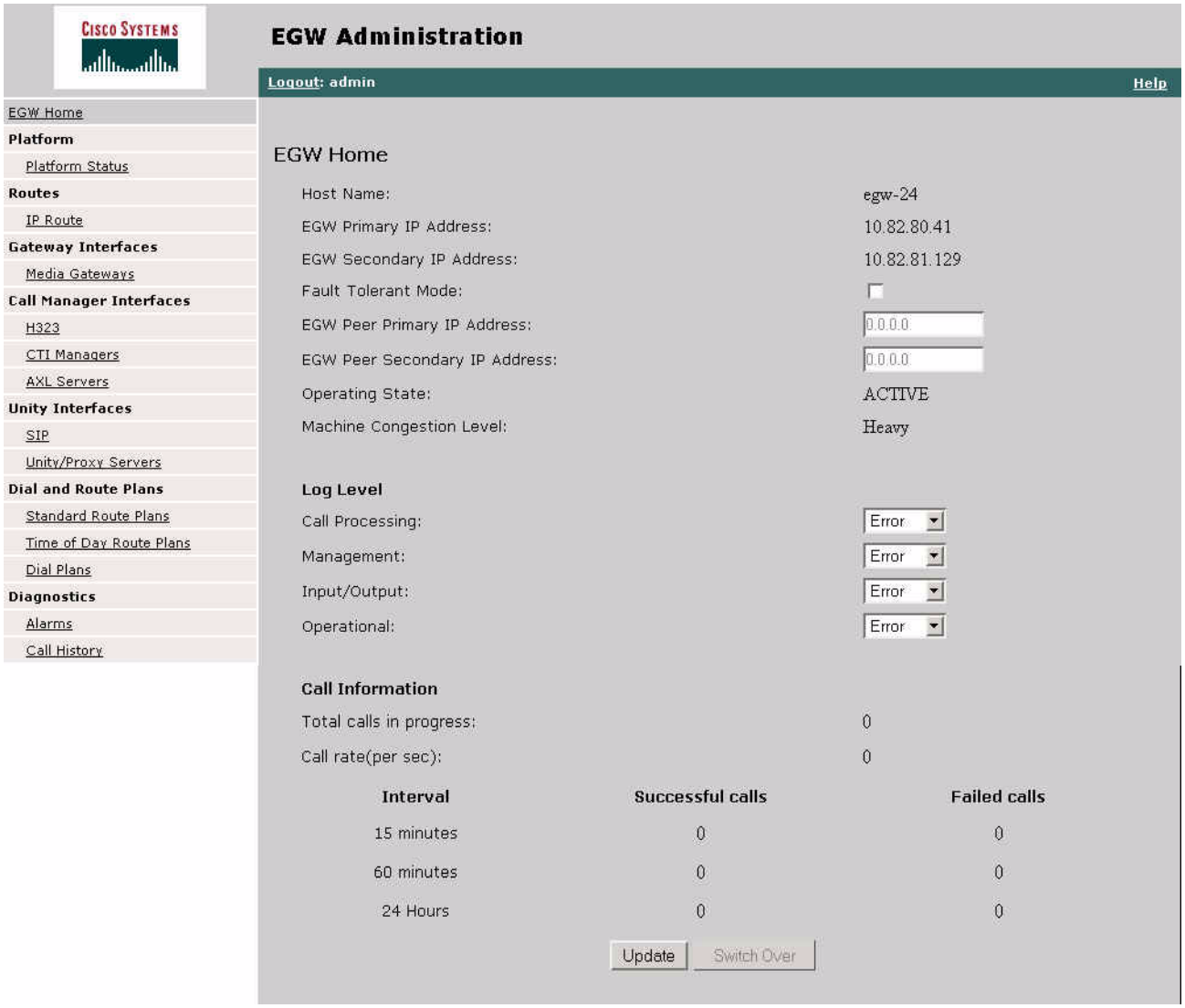
Cisco EGW 2200 Administration

The Cisco EGW Administration application allows you to provision, manage, and troubleshoot components in your network.

Figure 3 shows a sample window from the Cisco EGW Administration application that lists (in the left pane) the network components administrated by Cisco EGW. These network components are described in detail in Cisco EGW 2200 Communication with Network Components, page 6.

Tip Click **Help** to see online help for each window and its fields.

Figure 3 Cisco EGW 2200 Administration Sample Window



Cisco EGW 2200 Communication with Network Components

This section describes the items in the left pane of the Cisco EGW Administration window which represent other components in the network with which Cisco EGW communicates. For information on where Cisco EGW is located in a network, see Figure 1.

For details on required settings for each component, click **Help** at the top right corner of the window (see Figure 3).

Overview of IP Routes

If your network components are on one or more different subnets from the Cisco EGW host, you can set up communication between them by adding IP routes to your network. These routes can be used to route traffic from these components:

- Media gateways
- AXL servers
- CTI managers

Overview of Gateway Interfaces

Cisco EGW supports three types of media gateways:

- DPNSS Gateways, page 6
- QSIG Gateways, page 6
- PRI Gateways, page 7

DPNSS Gateways

A DPNSS media gateway consists of a voice-enabled router that serves as a gateway point between the TDM- and IP-based PBX networks. This media gateway is physically connected through one or more of its E1 or T1 interface to one or more of the legacy DPNSS PBXs.

The media gateway terminates Layers 1 and 2 of DPNSS and backhauls or transports the call control to Cisco EGW by using DPNSS User Adaptation (DUA) and Stream Control Transport Protocol (SCTP). Cisco EGW uses Media Gateway Control Protocol (MGCP) to control the media gateway in terms of codec selection and packetization. The gateway converts DPNSS bearer data into a Realtime Transport Protocol (RTP) stream, and these IP packets are sent to the appropriate destination (Cisco CallManager IP phone, Cisco Unity, or another DPNSS media gateway).

QSIG Gateways

A QSIG media gateway consists of a voice-enabled router that serves as a gateway point between the TDM- and IP-based PBX networks. This media gateway is physically connected through one or more of its E1 or T1 interface to one or more of the legacy QSIG PBXs.

The media gateway terminates Layers 1 and 2 of QSIG and backhauls or transports the call control to Cisco EGW by using Session Manager (SM) and Reliable User Datagram Protocol (RUDP). Cisco EGW uses Media Gateway Control Protocol (MGCP) to control the media gateway in terms of codec selection

and packetization. The gateway converts QSIG TDM bearer data into a Realtime Transport Protocol (RTP) stream, and these IP packets are sent to the appropriate destination (Cisco Unity, or another QSIG media gateway).

PRI Gateways

A PRI access gateway consists of a voice-enabled router that connects Cisco EGW to the PSTN network. This access gateway is physically connected through one or more of its E1 or T1 interface to the PSTN.

Cisco EGW supports Q.931 and EuroISDN connections to the PSTN:

- Q.931—Message-oriented signaling protocol in the PRI ISDN D-channel.
- EuroISDN—European ISDN standard.

The trunking gateway terminates Layers 1 and 2 of PRI ISDN and backhauls or transports the call control to Cisco EGW by using Session Manager (SM) and Reliable User Datagram Protocol (RUDP). Cisco EGW uses Media Gateway Control Protocol (MGCP) to control the media gateway in terms of codec selection and packetization. The gateway converts PRI ISDN TDM bearer data into a Realtime Transport Protocol (RTP) stream, and these IP packets are sent to the appropriate destination (Cisco CallManager, Cisco Unity, or a QSIG or DPNSS media gateway).

Overview of Cisco CallManager Interfaces

In a Cisco EGW network, where IP PBXs are added to legacy TDM PBXs, a Cisco CallManager cluster serves as an IP PBX. For a description of the Cisco CallManager cluster, go to the following URL: http://www.cisco.com/univercd/cc/td/doc/product/access/sc/nirvdoc/plannirv/jbcmr.htm

Cisco EGW provides signaling, routing, and DPNSS interworking that allows the advanced DPNSS calling features to operate transparently across both types of PBXs.

One Cisco EGW (or pair, for fault tolerance) supports a single Cisco CallManager cluster and provides for the following types of Cisco CallManager interfaces:

- H.323 Gatekeeper, page 7
- H.323 Interface, page 8
- CTI Manager Interface, page 8
- AXL Server Interface, page 8

H.323 Gatekeeper

The H.323 gatekeeper provides call admission, registration, status, and bandwidth control call using the Registration, Admission, and Status (RAS) protocol, and allows Cisco EGW to communicate with a Cisco CallManager cluster. A gatekeeper is not required in the Cisco EGW 2200 system, but is advisable if you want to be able to make effective use of network functions like call admission and bandwidth control for large installations. You can set up your Cisco EGW network to operate in Gatekeeper Mode or Direct Mode, depending on whether or not you are employing a gatekeeper in your system.

The gatekeeper provides a means for Cisco EGW to loadshare traffic across the Cisco CallManager hosts, and allows Cisco CallManager to loadshare traffic across HSIs in fault-tolerant Cisco EGW configurations. A Cisco EGW 2200 network without a gatekeeper functions just the same as with the gatekeeper, but the interface to the Cisco CallManager cluster is handled directly through the H.323, CTI, AXL, or XML interfaces in the Cisco EGW system without any RAS protocol messaging.

At the beginning of each call, the gatekeeper is queried by the calling device (Cisco EGW or Cisco CallManager) as to which destination device (Cisco CallManager or Cisco EGW) to use. For a description of the H.323 Gatekeeper, see:

http://www.cisco.com/univercd/cc/td/doc/product/access/sc/nirvdoc/plannirv/hwgkov.htm.

H.323 Interface

The H.323 interface provides H.323 signaling support and enables communication between Cisco EGW and Cisco CallManager.

The H.323 standard consists of the H.225 and H.245 standards:

- H.225—Specifies a message set for call signaling registration and admissions, and supporting call negotiations (synchronization).
- H.245—Provides the ability to open and close logical channels on the network (transmission control).

CTI Manager Interface

Cisco EGW establishes communication with the Cisco CallManager Computer Telephony Interface (CTI) Manager. Cisco EGW registers with the CTI Manager to support the call back feature on behalf of the CallManager cluster. Further, Cisco EGW uses CTI Manager to implement the DPNSS call back and extension status supplementary services.

AXL Server Interface

The Cisco AVVID XML (AXL) Simple Object Access Protocol (SOAP) server interface is used to perform database lookups (in the Cisco CallManager configuration database) for device names and call-forwarding information. The AXL server enables the Cisco EGW to identify and monitor individual end-user lines required for DPNSS call back and extension status supplementary services.

Overview of Cisco Unity Interfaces

Cisco Unity adds advanced voice messaging to your phone setup. A Cisco Unity voice-messaging server provides voice mail, unified messaging, and AutoAttendant services via the following interfaces:

- SIP Interface, page 8
- Unity Server, page 8

SIP Interface

Cisco EGW uses a SIP interface to connect to Cisco Unity. Cisco EGW provides interworking between SIP, DPNSS, or QSIG through a DPNSS or QSIG media gateway to the DPNSS or QSIG PBXs.

Unity Server

The Cisco Unity server interface is used for outgoing calls (from Cisco EGW to Cisco Unity).

The Cisco SIP Proxy Server is a call-control software package that provides a full array of call-routing capabilities. For a description of Cisco Unity, go to the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/access/sc/nirvdoc/plannirv/jbuvr.htm

Note Cisco EGW can be connected directly to a Cisco Unity server, or it can be connected to a Cisco SIP Proxy Server (Cisco SPS), which is in turn connected to a Cisco Unity server. Both these configurations are supported.

Overview of the Cisco IPT Platform Administration Tool

Cisco platform administration software comprises two applications:

- The Cisco IPT Platform Administration browser-accessible application which provides complete platform administration functions.
- A Command Line Interface (CLI) which provides a subset of the browser-accessible administration functions.

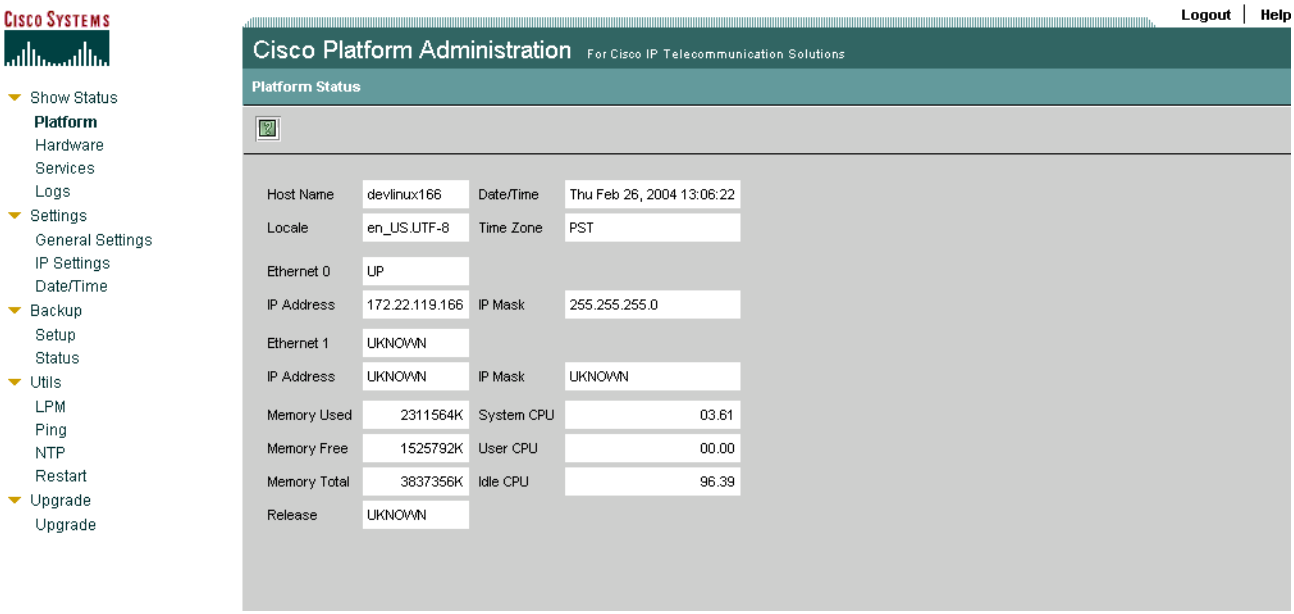
Cisco IPT Platform Administration

The Cisco IPT Platform Administration application allows you to configure and manage the Cisco EGW platform by doing these tasks:

- Check platform and hardware status
- Check IP addresses
- Back up and restore system data
- Ping other network devices
- Synchronize your system with the NTP server
- Set up electronic notification
- Upgrade system software
- Reboot the Cisco EGW
- Set up SNMP packet transmission

Figure 4 shows a sample window that lists (in the left pane) the managed platform elements from the Cisco IPT Platform Administration application.

Figure 4 Cisco IPT Platform Administration Sample Window



Overview of Cisco IPT Platform Administration Functionality

This section describes items in the left pane of the Cisco IPT Platform Administration window (see Figure 4).

For details on using the functionality described in this section, click **Help** at the top right corner of the window (see Figure 4).

Status of Platform Components

- Platform status—Displays information that was entered during Cisco EGW installation including, the Cisco EGW host name, status of Ethernet ports, IP addresses, memory usage, and CPU utilization.
- Hardware status—Identifies the platform model and serial number.

IP Settings

Cisco EGW allows you to change IP address and dynamic host configuration protocol (DHCP) information that was entered when the application was installed.

Backing Up and Restoring System Settings and Data

Cisco EGW allows you to specify a host where system settings and configuration data will be backed up using either secure or non-secure data transmission for the backup and restore operations.

Platform Utilities

- Ping—Allows you to check connectivity with other network devices.
- NTP—Allows you to set the network time protocol for the Cisco EGW network.

Electronic Notification

Electronic Notification (EN) alerts you to the presence of new software that has been uploaded to a remote server. You can then decide if you want to upgrade the software that you are running.

Software Upgrades

You can check your current version of Cisco EGW software, and upgrade software either from a local source (CD-ROM or DVD) or remote source (server on the network).

Rebooting the System

Cisco EGW allows you to reboot your system and continue to use your current software image, or reboot your system and start using an alternate software image.

SNMP Support

You can create new SNMP strings, users, and notification destinations.

Cisco Platform Administration CLI

Cisco EGW users can use the following CLI commands:

- ping
- tracert
- restart
- show status
- show hw
- show security
- show files weblog
- show files activelog
- show files activlog cli.log
- show files inactive log
- show files install
- show files install ks.cfg
- show files install partAlloc
- show files install install.log
- show files install install.post

- set hostname
- set ip (IP)
- set ip (DHCP)
- set ip (GW)
- set security
- set task alarm
- set task trace

For a description of these commands and their usage, go to the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/access/sc/nirvdoc/refnirv/hwrefcli.htm

Overview of Cisco EGW 2200 Routes, Route Plans, and Dial Plans

You set up routes, route plans, and dial plans by using Cisco EGW Administration windows.

Cisco EGW 2200 Routes

Routes are created when you perform the following actions:

- When you add a gateway, a route is automatically created. The route name incorporates the gateway name and the interface on the gateway. For Example, “rt-gw1-0-1” represents a route that was created by the addition of a gateway named “gw1” where the signaling slot is “0” and the signaling port is “1.”
- When you add a Cisco Unity server, a route is automatically created. The route name is the same as the name that was assigned to the Cisco Unity or Proxy server.
- H.323 routes are created automatically when you add an H.323 interface to the system. Because the H.323 interface is already present when you start Cisco EGW, the H.323 route is already created. Examples: If you are running a single Cisco EGW configuration, the route created is rt-h323-a; if you are running a dual Cisco EGW configuration, the routes created are rt-h323-a and rt-h323-b.

Cisco EGW 2200 Route Plans

A route plan uses routes that are created when you add a gateway, H.323, or Cisco Unity server interface are added to the Cisco EGW network.

Cisco EGW route plans are created by accessing the Add Route Plan window in the Cisco EGW Administration application. Route plans are used by dial plans to route calls in the network. The same route plan can be assigned to more than one dial plan. If a route plan is assigned to a dial plan, you are not allowed to delete it. You must de-assign the dial plan before deleting it.

Cisco EGW uses two types of route plans:

- A standard route plan offers sequential or random (load-shared) selection of routes in the route plan.
- A time-of-day route plan implements conditional routing and allows you to select a route that is based on the current time of day and day of the week.

Cisco EGW 2200 Dial Plans

Cisco EGW dial plans are created by accessing the Add Dial Plan window in the Cisco EGW Administration application. Dial plans allow routing decisions (selection of a route plan) based on the called number. In addition, the dial plan can perform digital manipulation on calling and called numbers.

After creating dial plans, they are assigned to gateway, Cisco CallManager, and Cisco Unity interfaces. You can assign the same dial plan to more than one interface, however, an interface can only use one dial plan.

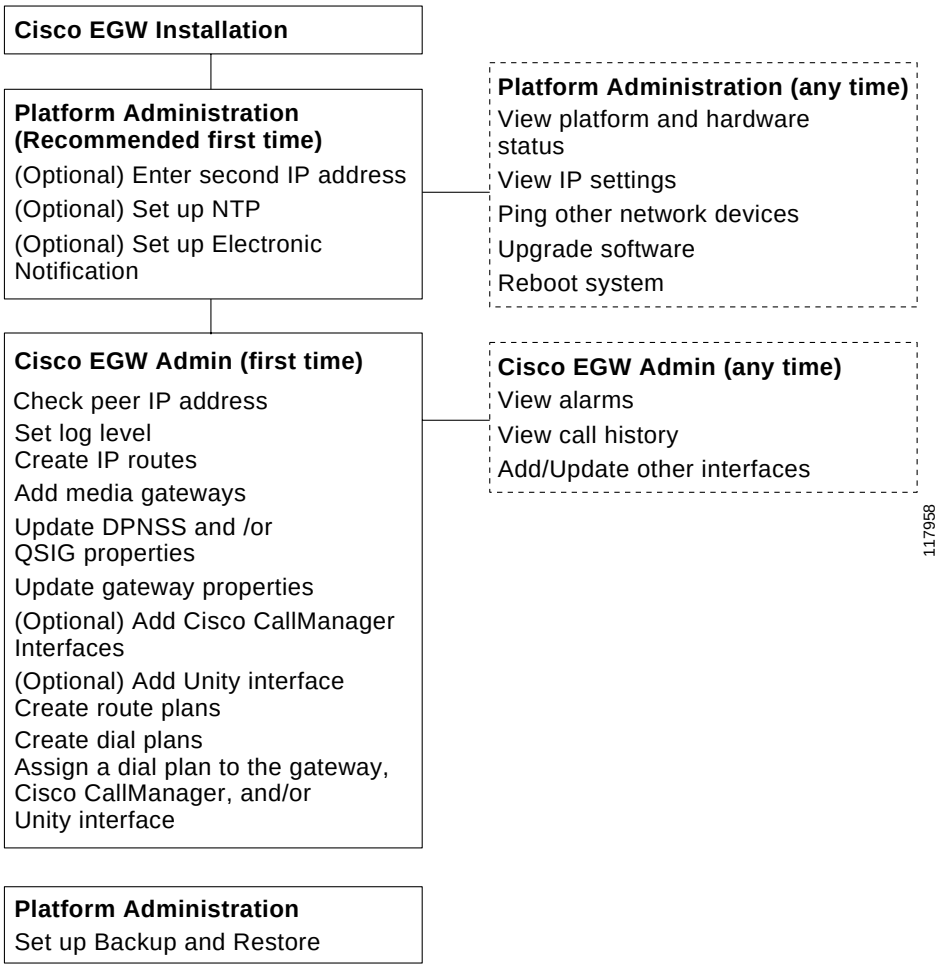
If a dial plan is assigned to an interface, you are not allowed to delete it. You must disassociate the dial plan from all interfaces to which it has been assigned before deleting it.

Cisco EGW 2200 Workflow

Figure 5 shows a recommended first-time workflow through the Cisco EGW product and it identifies tasks that you can perform whenever necessary. Because you may revisit Cisco IPT Platform Administration and Cisco EGW windows as needed, you can determine your own workflow, and any first-time workflow task can be repeated as needed.

The organization of items in the left pane of Cisco EGW also provides an implied workflow. However, if your system does not contain Cisco CallManager or Unity components, disregard the tasks for these components.

Figure 5 Cisco EGW 2200 Workflow



Cisco EGW 2200 Alarms

You can view alarms and select one or more alarms to diagnose from the Cisco EGW Alarms window in the Cisco EGW Administration application.

Alarm information displayed consists of the following:

- Cisco EGW component on which the alarm occurred (example: gateway1-bh-asso); to troubleshoot the alarm, find the information on the component in other Cisco EGW Administration pages.
- Date and time when the alarm occurred (example: 2004-02-02 12:17:22.719 EST).
- Category (actual text) of the alarm (example: Association Fail).
- Severity of the alarm (minor, major, or critical).
- Subsystem on which the alarm occurred (MGC or H.323).

When the alarm condition is no longer present, the alarm notification is removed from the Cisco EGW Alarms window.

For a list of Cisco EGW alarms and their explanations, go to the following URL:

http://www.cisco.com/iamegw/troubleshooting/troubleshooting_home.htm

Note If you are running a dual Cisco EGW configuration, a critical alarm forces a switch over to the standby system.

Cisco EGW 2200 Call History

You can view calls that occurred on the system from the Cisco Call History window in the Cisco EGW Administration application.

Call information that is displayed consists of the following:

- Calling number—Source of the call
- Called number—Destination of the call
- Timestamp—When the call was started
- Duration—Call duration in minutes
- Reason code—Displays the Call Detail Block (CDB) tag value for Tag 2008 (ANSI) and Tag 3008 (ITU). These reason codes are described in:

  http://www.cisco.com/iamegw/troubleshooting/troubleshooting_home.htm