An Overview of Cisco Universal Gateway Manager

With the Cisco Universal Gateway Manager (Cisco UGM), you can configure and manage the Cisco AS5300, AS5350, AS5400, AS5800, and AS5850 devices in your network.

Cisco UGM provides a graphical user interface (GUI) for network information and device management, including access to gateways functioning in the network.

This chapter contains the following topics:

Deployment Scenarios for Cisco UGM

The Cisco UGM product consists of two main components:

- Cisco Element Management Framework (Cisco EMF) software
- Cisco UGM software which manages these Cisco devices:
  - Cisco AS5300
  - Cisco AS5350
  - Cisco AS5400

- Cisco AS5800
- Cisco AS5850

Each device provides ports through which users can access the network.

Cisco EMF is a client-server environment supporting various deployment options. The best configuration for you depends on the number of servers, clients, and users in your network.

From the Cisco EMF client, you can access another Cisco EMF client or the Cisco EMF server through a remote X-terminal. You do not need a Cisco EMF client between your client and the Cisco EMF server, but doing so improves performance for large or medium deployments.

Figure 1-1 Directly Accessing the Cisco EMF Server

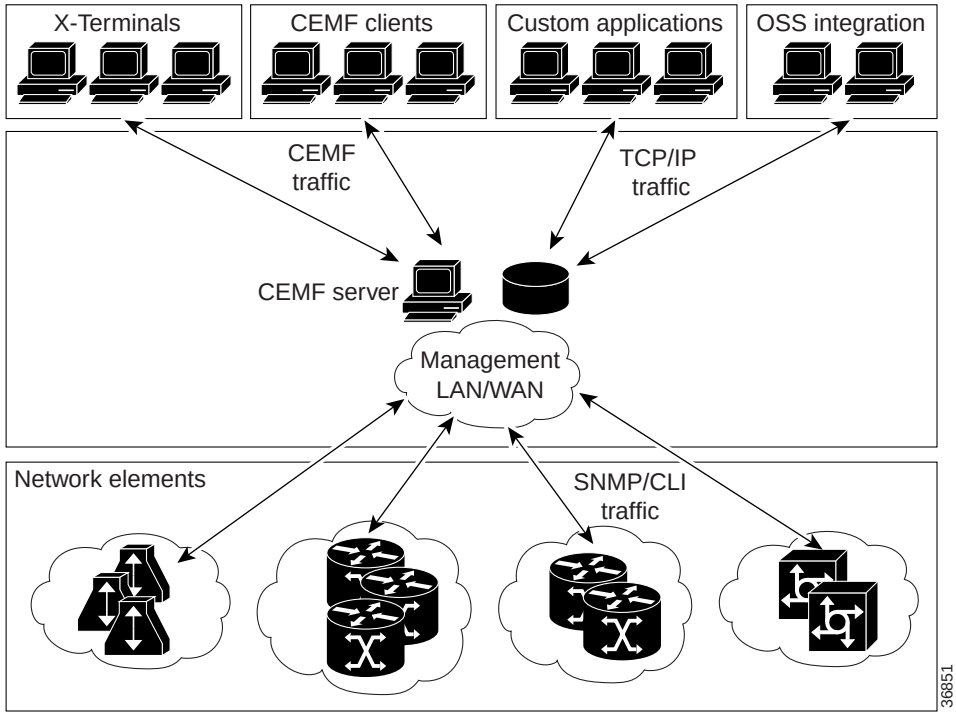
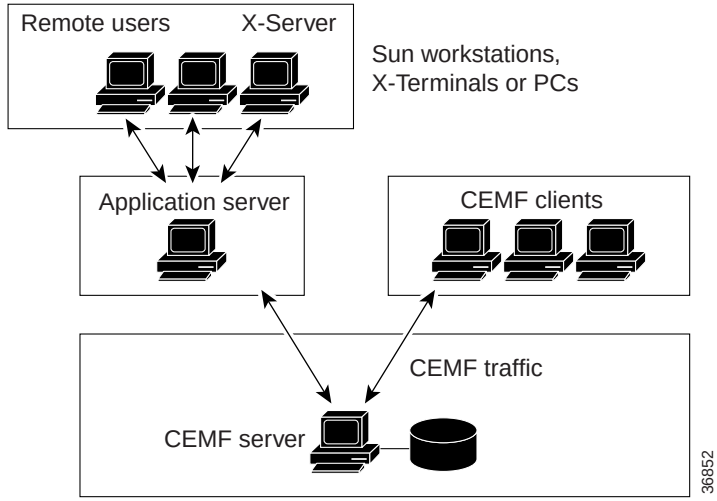


Figure 1-2 Accessing the Cisco EMF Server Through a Client



Features in Cisco UGM

Cisco UGM provides a powerful range of network management capabilities, including support for network configuration, device and component management, fault and performance management, and security.

Configuration

Cisco UGM provides various configuration services for the managed devices and their components:

- Autodiscovery and manual deployment of managed devices and components

  See Chapter 2, "Deploying, Discovering, and Exporting Inventory Data with Cisco UGM."

- Software image downloads

  See Chapter 4, "Managing Images and Scheduling Actions with Cisco UGM."

- Configuration file management

  See Chapter 3, “Configuring Devices with Cisco UGM.”
- Configlet support for incremental configuration changes

  See Chapter 3, “Configuring Devices with Cisco UGM.”
- Menu-launched telnet sessions for CLI device management

Device and Component Management

Cisco UGM inventories and maintains a current record of network gateways and their managed components. This inventory data can be exported in a flat file. See Chapter 2, “Deploying, Discovering, and Exporting Inventory Data with Cisco UGM.”

Managed network components include the following:

- Chassis
- Voice cards
- Modem cards
- Trunk cards
- Universal port
- Controller cards
- Router shelf controller cards
- Combination cards

Cisco UGM performs asynchronous database updates in response to network equipment configuration and status changes.

Fault Management

Cisco UGM provides device- and port-specific alarm frequency and severity information. The fault management GUI supports point-and-click alarm acknowledgement and clearing functions, and also enables trap forwarding. See Chapter 8, "Managing Faults with Cisco UGM."

With the Cisco EMF event browser interface, you can consolidate alarm viewing and filtering, and view alarms and events on a color-coded topology map. Fault management functions include:

- Alarm monitoring
- Alarm filtering
- Alarm clearing
- Alarm acknowledgement
- Alarm archive and history
- Alarm-based performance threshold alerts
- Trap registration and forwarding of traps to remote SNMP managers

Performance Management

Cisco UGM collects performance information from each managed device and its components. This information allows you to monitor the network by viewing and graphing performance data associated with an object. See Chapter 7, "Managing the Performance of Cisco UGM-Controlled Devices."

CiscoView also provides additional gateway statistics, including AAA statistics and both active and historical call statistics that complement the statistics provided by Cisco UGM. Cisco UGM can be used to launch CiscoView if it is available in the managed network.

Security

Cisco UGM supports role-based access to its management functions. You can define user groups and assign users to these groups. This function also supports control of administrative state variables for Cisco UGM resources. See Chapter 6, "Managing Security on Cisco UGM."