CHAPTER 1

Cisco IP Manager Overview

The Cisco Service Management System

The Cisco IP Manager software is part of the Cisco Service Management System of provisioning and management tools for service providers and operators of large enterprise networks. The Cisco IP Manager program interacts with other tools in the suite to provide a fully scalable element-level management system for high quality, rapid network services.

An API enables you to create communication links with other management tools such as Provisioning Center, Netsys Service Center, and existing operational support systems (OSS) for automated provisioning of network services.

The Cisco IP Manager software meets business requirements for scalable, reliable Layer 3, IOS-based element management in very large networks by:

- Enabling rapid, high-quality service deployment through automated infrastructure provisioning
- Integrating with an existing or new OSS via flow-through interfaces, including Provisioning Center, order processing and management, subscriber management and billing, and workforce automation
- Supporting new end-to-end network services
- Allowing partitioning of domain control and permissions to conform to business requirements

Operators may use the software to either configure new devices before they are brought on-line, or to change existing configurations in live elements to support new services. Import/export features allow you to write current device configurations to files prior to provisioning the network with new data and restore the saved configurations if you need to perform a rollback.

Cisco IP Manager Features

The Cisco IP Manager software provides automated, push-button services for network-element configuration. Its features include:

- Template-driven configuration file generation and command editing
- Configuration command analysis and verification
- Configuration file access control
- Network configuration file upload and download, with verification
- Network element status verification (such as **ping** and **show**)
- Activity log

Creating, Validating and Managing Configurations

Operators can propagate multiple configuration files across a large network from a single template, allowing use of standardized configuration variables such as hostnames, IP addresses and subnet masks.

The template-building interface provides a mechanism for defining variables in a template file and their values in a companion data file. Configuration files can then be generated en masse, similar to a word processing application's mail-merge operation.

Variables may also pass through a CORBA IDL interface for other network management systems or OSSs.

The IP Manager software utilizes syntax and integrity check validation technologies originally developed for Cisco's Netsys software suite, to ensure accuracy and to identify inconsistencies in the configuration files before they are deployed to the live network.

The software can manage multiple discrete customer networks which use the same unregistered IP address ranges. The flow-through interface enables communication with static or dynamic IP address pool management tools. System administration allows user-based authentication. Managers can organize elements into domains and sub-domains and assign permissions to each, based on user group. Operators must enter a password to obtain access to permitted domains.

The Cisco IP Manager software also partitions and controls data access.

- Service provider customers or their connected systems can be granted limited rights to view only those network elements which pertain to their part of the network. This is highly useful for networks that use the same infrastructure to provide services to multiple customers.
- Selected users can create, read, update, or delete selected data. Managers can limit visibility in sub-domains so that, for instance, a user can view or amend a router configuration, but cannot view or amend IP addresses within it.

IP Manager Software Configuration

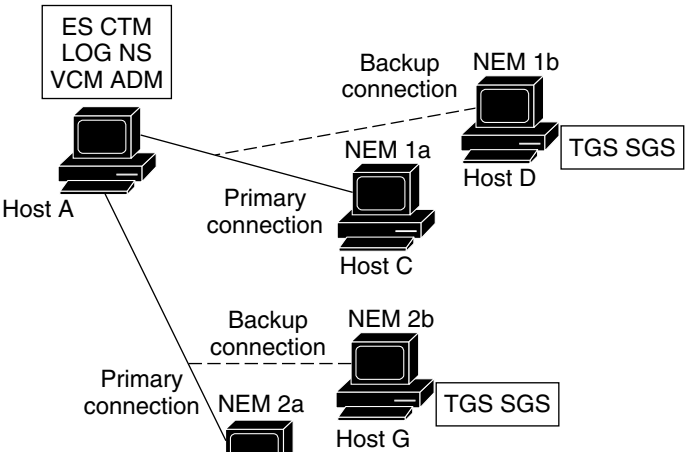
A fully installed Cisco IP Manager system consists of the following elements:

- **AASServer**—controls access to the system and its data for the other servers; manages Cisco IP Manager permissions groups
- **AUTHServer**—manages user information
- **CNGSServer**—evaluates device configurations before deployment and generates reports on connectivity issues
- **CTMServer**—manages templates and template data
- **Event Server**—used by the individual elements of the system to keep track of events occurring throughout the rest of the system
- **INGServer**—the gateway to the Netsys functionality
- **LOGServer**—maintains records of system activity
- **Naming Service**—Orbix registry of servers and their locations
- **NAMServer**—manages domains
- **NEMServer**—manages network elements; establishes communications between servers and network elements
- **GUI application**—provides a user interface for working with the Cisco IP Manager servers
- **Oracle database**—the data repository

If your machine has sufficient resources, you can install all of these components on the same host, or you can deploy various elements to different hosts. (Servers are described more fully in the appendix "Advanced Usage;" the installation process is described in the chapter "Getting Started.")

The installation scripts supplied by Cisco can be used to install the GUI application and NEMServer on any number of machines, the CNGSServer and INGServer on another machine, and the central servers AASServer, AUTHServer, CTMServer, ES, LOGServer, NAMServer, and NS on another machine.

Figure 1-1 Servers deployed on multiple hosts

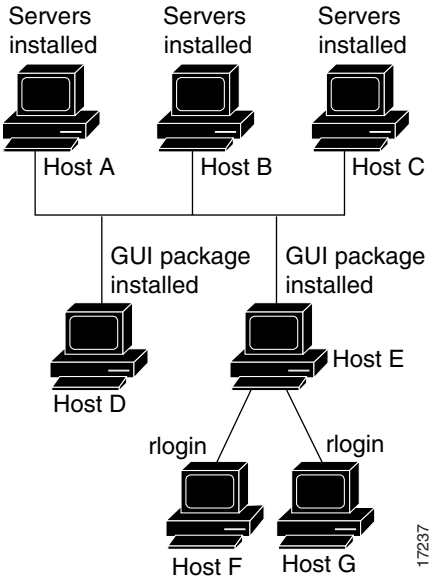


You can run multiple copies of the NEMServer file simultaneously. You can manage one set of network elements using one NEMServer as your primary communications server and a second NEMServer as a backup in case of failure of the primary; and you can manage a second set of nework elements using a separate primary/backup pair of NEMServers.

If you choose to install without using the Cisco-supplied script, any combination of servers and hosts is possible.

You can install the GUI package on as many machines as you want, or you can install it on a single machine (may or may not be the same as the server host) and log on remotely—as long as the host has sufficient resources.

Figure 1-2 GUI package deployment



Equipment

The following sections describe the equipment that can be provisioned by the Cisco IP Manager software and the equipment required to run it.

Devices Supported

The Cisco IP Manager software supports any IOS-based Cisco products (such as routers, router blades, and so on) running with version 11.2 and compatible releases. However, it is possible a special condition may be required for some devices using Telnet or other network communication protocol. Your Cisco customer service engineer can advise you about such conditions.

Products currently certified include the 1600, 2505, 2514, 2518, 2524, 2525, 3810, 4500, 5200, 5300, 7200, 7507 (with IOS versions 11.0, 11.1 and 11.2), 7513, LS1010, and GSR12000.

See the release notes for a detailed products/IOS-release matrix.

Minimum System Requirements

Your system must have the following software installed:

- Solaris 2.6 (all client and server machines), using the Common Desktop Environment (CDE); other window managers which support the Java run-time environment (JRE) 1.1.5 should work, but have not been tested
- Solaris SUNWsprot and SUNWbtool packages (on the machine on which the ING server is installed)
- Oracle Enterprise Server, version 7.3.4, installed according to Oracle's documentation. (Regardless of the platform on which you run your Oracle instance, you will also need an Oracle installation CD for the Solaris platform in order to install SQL*Net on each Cisco IP Manager host.) If you are installing Oracle for the first time, you should include the following Oracle components:
  - Oracle UNIX Installer
  - ORACLE7 Server (RDBMS)
  - SQL*Net (V2)
  - SQL*Plus
  - TCP/IP Protocol Adapter (V2)

Recommended Hardware

Specific hardware requirements can vary greatly depending on configuration of the software and client/server distribution. For information about installation options, you should consult with your Cisco customer service engineer. Also, see the chapter "Getting Started."

A Sun Ultra 1 with 256MB of RAM is the minimum recommended machine for running the *center* and *ding* server packages. (Memory requirements for the *ding* package, which installs the INGServer, can vary widely depending on the nature of your network and the contents of individual device configurations. Large numbers of interfaces or a large number of access lists can take up a large amount of memory, even if the number of devices is small, for example.) The *dnem* package can be run on a Sparc 5 with 256 MB of RAM.

A Postscript printer is required to use the print command on the **File** menu of certain windows.

Memory and swap space requirements vary considerably, depending on your installation configuration and the size of your network. A general rule for swap space is twice RAM.

The following table shows the disk space required to install the various packages:

Table 1-1 Disk Space Requirements for Installation

Package	Installation (includes tar file)	Installed (tar file deleted)
center	200 MB	100 MB
ding	180 MB	90 MB
dnem	40 MB	20 MB
gui	180 MB	90 MB
Orbix	90	45 MB
Total of all packages	690 MB	345 MB

You will need to copy and uncompress the *.*Z* files from the CD to your hard disk. After installation, you can delete the tar files.

You can uncompress any of the compressed files from the CD to one volume and install to a different disk, thereby reducing the maximum space required on any one disk to the lower number (but you will need two of them—one for the tar file, and one for the installation).