CHAPTER 2

Network Organization

Overview of Network Management

The Cisco IP Manager software utilizes five distinct information units to model a network management working environment:

- domains
- elements (and associated attributes, configurations, and communications parameters)
- templates (and associated data)
- users
- permissions and permission groups

Domains provide a hierarchical organizational structure for the management of elements (devices) and templates. Templates and associated data are the means by which configurations are generated for devices, either individually or en masse.

Individual users derive their access levels (permissions to manipulate domains, elements and templates) from the permission group to which they belong.

Users and permission groups are created and managed by a single user entity, known to the system as *admin* (the SuperUser referred to in the API reference; *admin* login name cannot be changed).

Domains

Domains are the organizational containers in which elements and templates are created and maintained. (The word *container* is also used within the Cisco IP Manager software to mean a specific type of hardware device which holds multiple routers. As are other devices, these containers are created inside domains.)

The system always includes at least one domain, the *root* domain. This domain is reserved for system use. You should not grant users access to this domain. You should create your own *user root* domain as a subdomain of the system root, then use this user root as your base domain for all other activities (except using the log; log permissions are system wide, not domain based.)

If you create all of your working domains as subdomains to this user root, templates and template data stored in the user root can be shared among users and among domains. These user root templates can be referenced as subtemplates from any of your working domains.

(Users who do not have access to this user root domain will not be able to reference these subtemplates. You will have to copy the templates and associated data into a subdomain to which the users do have access.)

Elements

When elements—network devices, such as routers—are created within the Cisco IP Manager system, they are associated with a specific domain. Any user who has sufficient access to the elements within a domain can configure those elements from a template that is created in any other domain that the user can access.

Templates

Templates are the means by which configurations can be built and reproduced in multiple quantities. A template consists of a template body and a template data object. The template body contains text made up of the static portion of the configuration—text which does not change from device to device (the IOS commands)—and the variable names that will be replaced by data values.

The template data object contains the data values that will be used in place of the variable names when configurations are generated.

Templates are created as objects within specific domains, but a template can be used to configure devices in any domain if the user belongs to a group that has sufficient permission.

A template may reference another template. The referenced template is called a *subtemplate*.

The subtemplate must be in the same domain as the calling template or in a domain higher in the domain hierarchy (must be in a direct line of ancestry from the calling template's domain—that is, it cannot be in a subdomain of any of the ancestor domains).

Templates can be nested only one level deep. A subtemplate cannot reference another subtemplate.

Users

When you create a user, you are only providing the system with a name and password for the user entity, which can be either a person or an application. Users derive working privileges (access to domains, elements, and templates) from the permission group to which they are assigned. A user can only belong to a single permission group.

Only the *admin* user can create or modify a user profile.

Permission Groups

User access to domains, elements, and templates is controlled by the permissions that are granted to permission groups.

Permissions describe what level of access is permitted for various resources; a permissions group defines the permissions that are assigned to its members. Every user who is included in a group has all of the access privileges granted to that group.

Only the *admin* user can create a permissions group and assign or modify privileges.

Permissions are granted as follows (in any combination):

- domains
  - create
  - read

  - modify
  - delete
- elements
  - create
  - delete
  - read
  - modify
  - perform upload/download operations
- templates
  - create
  - delete
  - read
  - modify
- log messages
  - delete
  - read

In order to work on an element or a template, the user must belong to a group that has been given the appropriate access to the element or template *and* has been given at least read access to the domain in which the element or template resides.

Permissions descend downward from the topmost domain in which the group has rights.

Consider the following example:

```
domainA
   subdomainA-1
   subdomainA-2
      subdomainA-2.1
domainB
   subdomainB-1
```

If a permission group is granted the right to create and delete elements and templates in **domainA** only, users in that group can also create and delete elements and templates in **subdomainA-1, subdomainA-2** and **subdomainA-2.1**, but not in either **domainB** or **subdomainB-1**.

If the permission group is granted permission to create domains in **domainA**, users in that group automatically gain the right to create subdomains in any of the domains that exist within **domainA**.

If the permission group is granted permission to delete domains in **domainA**, users in that group automatically gain the right to delete any domains within **domainA**.

Once a domain has been created, however, the administrator can change these inherited permissions.

User Interface

You are not required to use the user interface developed by Cisco. You can develop your own means of communicating with the Cisco IP Manager servers using the CORBA IDL (Interface Description Language) files documented in the companion book “Cisco IP Manager API Reference Guide.”

However, you may find the discussion of the Cisco-developed interface to be of help in understanding the capabilities of the software and how the servers can be made to work. Additionally, you should read the chapter “Getting Started” and the appendix “Advanced Usage” for an understanding of the system and individual servers, and for information about launching individual components of the system.

Cisco GUI Application

The Cisco-developed graphical user interface (GUI) application provides the following tools for working with the network resources described previously:

- **Element Manager**—for creation and management of domains and devices (including uploading of configurations generated in the template manager)
- **Template Manager**—for creation and management of templates and template data, and for generation of configurations

- **User Manager**—for management of individual users
- **AAS Manager**—for creation and management of permission groups (the means by which users are given access rights)

For information about creating and managing domains and elements, see the chapter "Managing Network Elements."

For information about working with templates, see the chapter "Template Management."

For information about managing users and permission groups, see the chapter "System Administration and Log Management."