

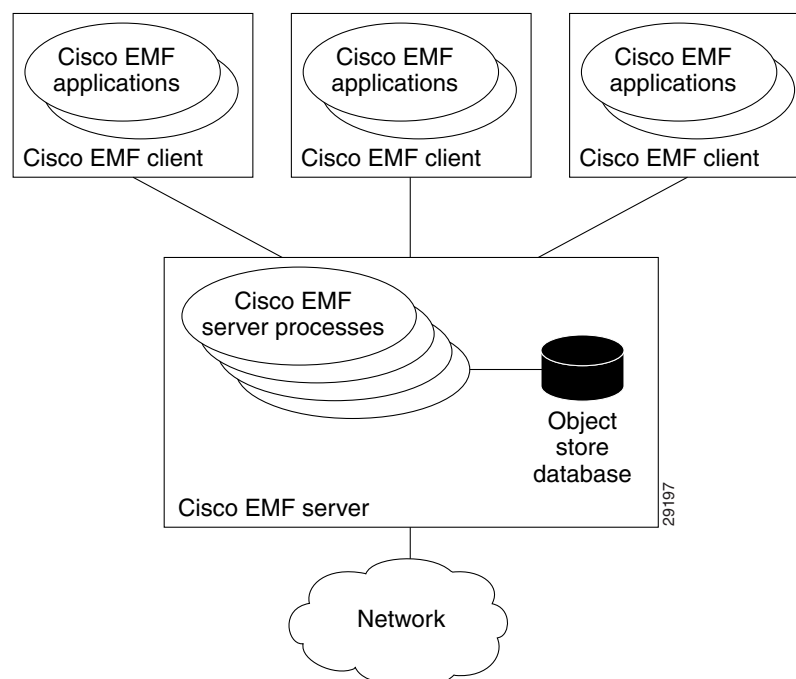
Cisco EMF Concepts

Cisco EMF is a carrier class network management framework. This framework was designed specifically to address the challenges of developing and deploying robust, large scale, multi-vendor, multi-technology, management solutions. Cisco EMF has been designed to overcome the limitations of traditional enterprise network management solutions, particularly in the broadband access market, and also in other network management applications where the aforementioned characteristics are important. Cisco EMF is being used to quickly develop and deploy element, network, and service-level applications in technologies ranging from Digital Subscriber Line (DSL), used for high speed internet access, cable modems, and Voice Over IP, to complex ATM/IP routing multi-service switches.

Cisco EMF Components

Cisco EMF consists of a series of applications that form a “front-end” graphical user interface (GUI) to process input and a series of “back-end” server processes which maintain a model of the network, and actually carry out the interfacing to the network elements.

Figure 2-1 Cisco EMF Processes



The standard Cisco EMF system comes with the following set of applications:

- Launchpad
- Map Viewer
- Auto Discovery
- Access Manager
- Event Browser
- Object Group Manager
- Performance Manager
- Deployment Wizard
- Netscape Help Browser.

Only a brief overview of these applications are provided in this chapter. Detailed instructions for each application are provided in later chapters.

Element Managers

The most common form of a Cisco EMF installation includes at least one plug-in module referred to as an Element Manager. The Element Manager modules add custom GUI windows and modeling behavior to the standard Cisco EMF system in order to allow the management of a specific type of network element.

Multiple Element Managers can be installed onto a single Cisco EMF server, thereby allowing multi-device and multi-vendor management from a single system.

The extra concepts and operating instructions for a particular Element Manager are provided with that specific module.

Cisco EMF Model of the Network

The Cisco EMF system keeps a model of the managed network within its database. This model is used to keep track of the current state of the various network elements and various abstractions of this network.

Some of the concepts behind this model must be understood in order for you to make full use of the features within the system.

Objects

Each element managed by Cisco EMF is modeled as an object.

An object can represent some part of the network; for example, a router or a switch. An object can also represent an abstraction of the network, that is, a site or a region; or it can represent some of the services provided by the network; for example, a PVC. An object may also be used to represent something (or someone) that interacts with the network, such as a subscriber or a customer.

Object Classes

Each object within Cisco EMF has an associated object class. Each class of object simply indicates a different kind of element. Examples of classes are: routers, line cards, sites, etc.

Each class of object has different data stored against it and displays different behavior.

In the Map Viewer application, the class of the object is indicated with a different icon used within the Map View browser.

The use of classes also allows powerful queries to be carried out based upon the kind of object. Examples of this type of query could be: show all events in the system from cable modems or create a group of router objects.

Object Types and Attributes

Each object has a number of attributes which can be accessed. An attribute is a piece of information either stored against the object or accessible from the object through some network protocol. Examples of attributes are: IP address, interface table, upstream power, etc.

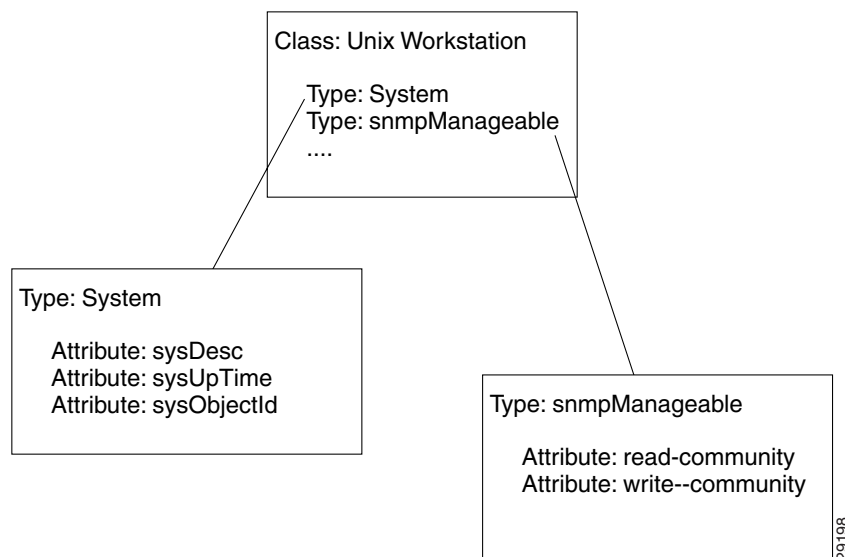
These attributes are associated with the object according to the granularity of object types.

A type is simply a collection of related attributes and each class usually has a number of types.

An object's class defines which types, and therefore, which attributes, it is allowed to have and which types it has by default.

An example of the association between classes and types is shown in Figure 2-2.

Figure 2-2 Example of Object Types and Attributes



In the above example, a **UnixWorkstation** class is specified. This class of object includes two types: **System** and **snmpManageable**. The **System** type includes the **sysDesc**, **sysUpTime**, and **sysObjectId** attributes. The **snmpManageable** type includes the **read-community** and **write--community** attributes.

Views

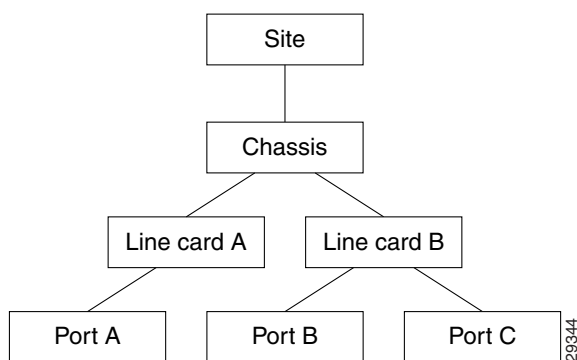
A view is a collection of objects in a hierarchical relationship. Each object can have a number of “parents” and “children.”

You can access Cisco EMF objects by navigating through one of the views to find the object. Each view represents a different way of containing and grouping the objects. Most Element Managers add additional views onto the standard set supplied by Cisco EMF. The standard views provided are the Physical and Network view.

Physical View

The Physical view is used to show the actual physical location of an element. An example of a physical containment relationship is shown in Figure 2-3.

Figure 2-3 Example of a Physical View



Network View

The Network view is used to represent the network devices within their relevant networks and subnets. This view is used by the Auto Discovery subsystem of Cisco EMF to calculate which devices have already been added to the system so that it does not try to discover the same device multiple times.

Object Groups

An object group is simply a collection of objects which are related in some way. They may all be the same type of equipment or all belong to the same customer.

Object groups can be built either manually or by building a query. Some Cisco EMF subsystems may also build object groups which may be visible and usable by the Cisco EMF user.

Object groups are accessible through the Object Group Manager application (refer to Chapter 7, “Object Group Manager,” for more information).

The Cisco EMF Session

This section describes Cisco EMF sessions.

Sessions

When you want to use Cisco EMF, log in to a Cisco EMF session. All activities you perform happen within this session.

Cisco EMF provides User Access Control which allows a system administrator to control what different users are able to do. Each user has a different login name and password, with a specific set of privileges within the system.

A standard Administrator user (**admin**) is available by default. The Administrator user has access to all features at all times. The Administrator user may not be edited other than to change the password.

Multiple User Sessions

Cisco EMF allows you to open multiple user sessions. Each user session has access to the tools displayed in the Launchpad. Any changes in a user session are reflected immediately in all other user sessions.

User Features

Each Cisco EMF application provides a set of features which can be accessed by all other applications within Cisco EMF. Using this model, the suite of applications appears to be one single integrated application.

You can log into a Cisco EMF session and use the features of any application within the Cisco EMF suite. The features run within the context of your session.

Examples of some Cisco EMF features can be found by right clicking on a network element within the Map Viewer application. The pop-up menu shows a set of features currently available to you in this network element.

The selection of available features depends upon the class of element and the user's access permissions.

Access Control

Within Cisco EMF, access to features can be restricted on the basis of the user's access level to a subset (or group) of these features.

For example, administration of particular managed objects should only be performed by operators who are responsible for that particular site, or for a region in which that site belongs. However, these operators may also require visibility of objects outside their own area of control.

The basic building blocks used to control user access are described below. Refer to Chapter 9, "User Access Control," for more detailed information.

User Groups

Cisco EMF user accounts can be collected by an administrator into groups. These user groups can be used to model user roles. A typical set up would involve a user group for system administrative users, or for network fault detail users, or for operators to manage a given site.

It is on the basis of these user groups that Cisco EMF applies access control. The Cisco EMF administrator configures access control by assigning access specifications to the relevant user groups.

Feature Lists

All features offered to a user are grouped together into feature lists. The benefit of feature lists is that it is easy to give access to a related set of features by simply choosing a feature list instead of having to assign features individually.

Any given feature may appear in more than one feature list.

Access Specifications

Access specifications connect together the user groups, the features that can be invoked by a group, and the objects upon which these features can be invoked.

A number of access specifications are provided by default with the Cisco EMF system. More access specifications can be built at the discretion of the system administrator.

The installation of an Element Manager also usually causes extra access specifications to be added to the system in order to give access to the new features provided by this module.

Each access specification may include the following components:

- feature lists—lists the Cisco EMF features which the users in this group have access to. A feature list can appear in more than one access specification
- user groups—Cisco EMF user accounts can be collected by an administrator into groups. These user groups can be used to model user roles. It is on the basis of these user groups that Cisco EMF applies access control.
- a permission level—for example, read-only, read-write, etc.
- an optional object group—where an object group is supplied, the users in the group have access to the features specified by this access specification only for those objects contained within the group. Where no object group is supplied, the access specification provides the specified access to features for all objects. This object group could be used to grant the administrative user group for a site read-write access to the objects on that site, while another access specification would be used for read-only access for non-administrative users.

The Event Model

A Cisco EMF event represents a notification from a managed entity that a certain condition has just occurred. These events usually represent error conditions on managed elements.

Each event is associated with the object for which it provides notification. Therefore, an object can have a number of events related to itself at any one time.

Sources of Events

SNMP Traps

When managing devices over SNMP, Cisco EMF receives traps from the managed devices. These traps are converted into Cisco EMF events which are then raised against the managed devices which sent the traps.

Element Manager

An Element Manager component installed onto the standard Cisco EMF system may raise events into the system to indicate various error conditions on objects under the Element Manager's control. An example of this would be the loss of communications with an SNMP agent.

External System

An external system may raise events into the Cisco EMF system through a custom integration channel.

Event Information

The default information stored against all Cisco EMF events includes:

- the object on which the event was raised
- the time the event was raised
- the severity of the event
- a description of the event
- the state of the event.

Descriptions of event state and severity are given below.

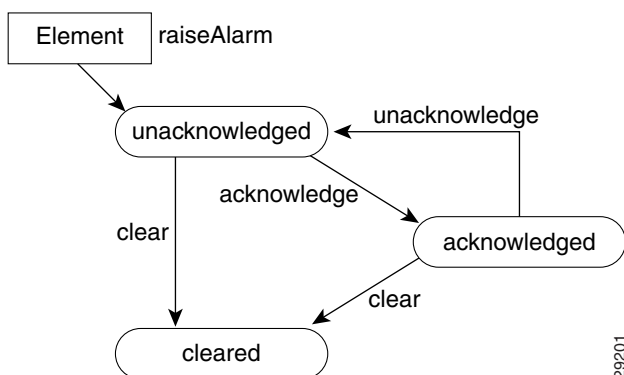
Event State

The event state indicates whether the event is acknowledged or unacknowledged and active or cleared.

When a new event is received by the system, its state is active/unacknowledged. You may acknowledge the event, which indicates to other users that the event is being handled. Once the event has been dealt with, you may clear the event. When you cannot clear an event due to an existing problem, it can be returned to the unacknowledged state and subsequently acknowledged or cleared by another user.

When an event is in the unacknowledged or acknowledged state, it is counted as being active, and therefore, it is still affecting the state of the object upon which it was raised.

Figure 2-4 State Diagram for Events



Events continue to be stored within the system after they are cleared in order to maintain an event history for an element. These events can be viewed and manipulated in the same way as any other event.

Severity

Each event has a severity, indicating the importance of the event, and is identified with a corresponding color as follows:

- Informational (white)
- Normal (green)
- Warning (cyan)
- Minor (yellow)
- Major (orange)
- Critical (red).

Source Domain

The source domain identifies where an event was generated. In Cisco EMF, the source domain can be one of the following:

- SNMP—event was generated by the managed network
- Internal—event is generally generated by Cisco EMF
- ASCII—event was generated by the Event Manager Event Translator
- Thresholding—an Event Manager event was generated by the Event Thresholder.

Management Domain

This is the management domain of SNMP trap information. The SNMP MIB specific information typically defines the equipment type generating a trap.

Viewing and Querying Events

Events stored within the system can be viewed and manipulated using the Event Browser. Detailed information about the application can be found in Chapter 6, “Event Browser.”

Clearing Events

Events can be cleared either directly, by moving the event to a cleared state, or by the system clearing the event as a result of clear correlation.

Manual Clearing

When you select to clear an event, a Clearing Event is generated.

A user generated clearing event contains the name of the user who performed the clear, and the date and time at which it was performed. It is possible for you to enter text to be associated with the clearing event.

When multiple events are being cleared, you can elect to use the same clearing information for all events.

The Event Browser displays an additional gadget for clearing an event.

Clear Correlation

The Cisco EMF system can be configured to automatically clear an event as the result of another event entering the system.

This configuration is performed on a per Element Manager basis and is provided with any Element Manager package you install.

A common example of a clear correlation is where the arrival of one SNMP trap signifies a previous SNMP trap is no longer valid. For example, a link up trap indicates a previous link down trap is no longer outstanding on a device.

Event Propagation

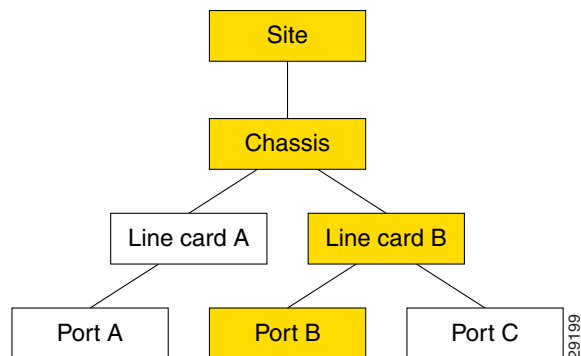
In order to make the identification of potential problems easy, the Cisco EMF system propagates the alarm state of objects upwards through each object view.

In real terms, this means that if an object receives an event, then not only does it change color to reflect its new state, but all parent objects within a view, also change color, to reflect the most severe alarm on any of the children. The example in the following diagram shows a typical physical view of the network. The line cards are contained within the chassis, the chassis within a bay, the bay within a site, etc.

Example

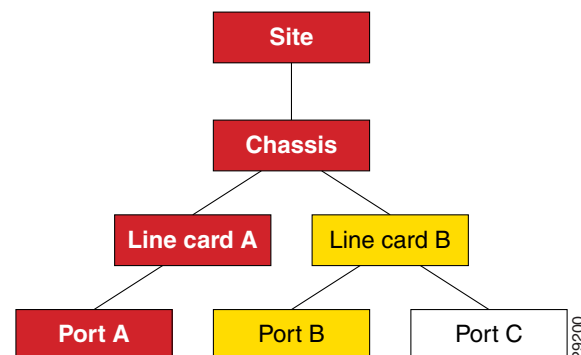
If a minor alarm was received on Port B, then it, and all of the objects up to the region, turn yellow to indicate a potential minor problem.

Figure 2-5 Example Minor Event Propagation



If a critical alarm was then received on Port A, then it, and all of the objects up to the region, turn red to indicate a potential critical problem.

Figure 2-6 Example Critical Event Propagation



If the critical alarm is then cleared, the icons return to yellow.

Maps

A map is a graphical representation of related objects being managed by Cisco EMF. Each object within each view has a separate map. In other words, the same object in different views could have a different map in each view.

You can view different levels of complexity in your managed network by looking at high level maps or by navigating to submaps which represent lower levels of detail in the managed network.

Each map is a two-dimensional canvas that displays nodes and links, each of which represents a Cisco EMF object. Refer to Chapter 3, “Map Viewer,” for detailed information.

Nodes and Links

Nodes and links are graphical symbols which represent managed objects in the network or abstracted objects. A node appears as an icon on a map, a link appears as a line connecting two nodes. Links can only exist as a connection between two nodes.

Each node and link clearly indicates the current operational and administrative state of the object it represents.

State indication is covered in Chapter 3, “Map Viewer.”

Background Images

A background image can be applied to any map within the system. Normally, this would be a geographical map, a floor plan, or some form of schematic. Nodes and links can then be placed on top of this image as desired.

Persistent and Transient Maps

As you traverse through the views within the system using the Map Viewer, you see the map representation for the level being displayed on screen.

In many cases, what you see is all of the child objects laid out in a grid pattern within the display. This is referred to as a transient map, as it is actually generated by the map sub-system “on the fly” and is not stored within the Cisco EMF database.

If you wish to make manual changes to a transient map (for example, to place the objects at particular locations or to add a background map) you simply must open the map for editing. From then on, it is stored persistently within the Cisco EMF database.

Other sources of persistent maps can be maps generated by element manager modules (commonly used to show schematic diagrams of equipment). As these maps are generated by the system, they may restrict you from making manual changes.

Deployment

Deployment is the term used within Cisco EMF to mean the addition of objects to the Cisco EMF network model.

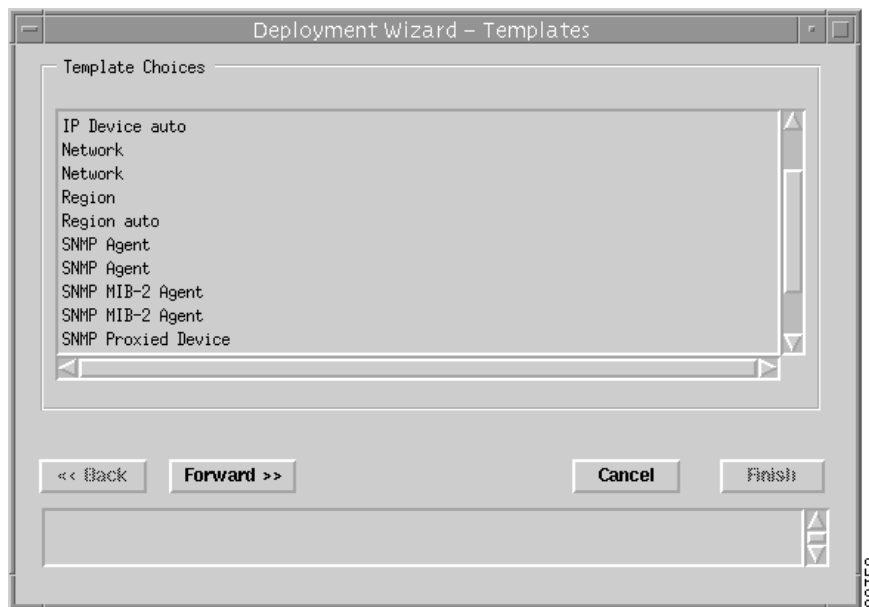
You can add objects to the model in the following ways:

- Deployment Wizard
- Auto Discovery.

Deployment Wizard

The Deployment Wizard is the graphical interface used to prepare the Cisco EMF Server for the deployment and subsequent management of new network elements. Cisco EMF uses a wizard style interface because it is particularly suitable for the act of deployment; a sequential series of tasks which require input at each stage. Refer to Chapter 4, “Deployment Wizard,” for detailed information.

Figure 2-7 Example of a Deployment Wizard with a List of Deployments



Usually the first screen presented in the wizard is a list of the possible deployment scenarios you can perform. Depending upon which scenario you choose, you are then presented with a series of screens asking various questions regarding the objects you wish to deploy.

Auto Discovery

Auto Discovery allows you to use ICMP pings and SNMP requests to automatically find and add objects to the object model. Refer to Chapter 5, “Auto Discovery,” for detailed information.