



Cisco IP Manager and MPLS VPN Solution Administration Model

The MPLS VPN Solution software Provisioning and Auditing system integrates with the Cisco IP Manager (CIPM) for element management. MPLS VPN Solution software uses the Cisco IP Manager system to read and write router configuration files. In MPLS VPN Solution software, the process *Download to IP Manager* (or *DIPM*) server reads and writes router configuration files and synchronizes object information into Cisco IP Manager during calls to read and write router configuration files.

An aspect of the integration between CIPM and MPLS VPN Solution software consists of keeping the administration models of the two systems synchronized. The MPLS VPN Solution software system holds the master information for the administration model. The synchronization from the MPLS VPN Solution system into the CIPM system “trickles down” during the configuration file download, process, when elements in CIPM are created, and the element attributes are updated. A common naming convention is required to uniquely identify objects in both systems (see the “Naming Convention to Uniquely Identify Domains” section on page A-3).

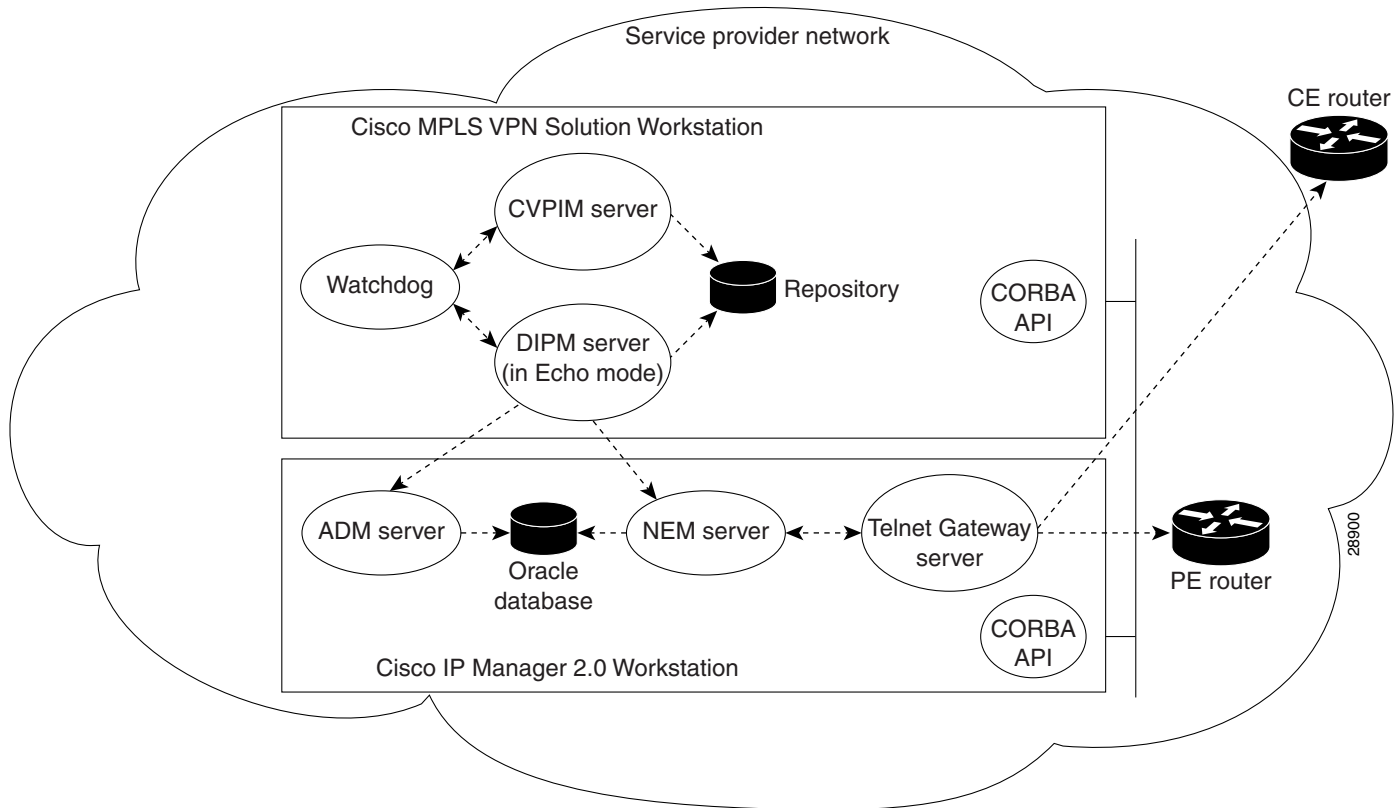
The communication between MPLS VPN Solution software and Cisco IP Manager is through CORBA APIs (for a list of these APIs, refer to Chapter 1, “Overview,” in the *Cisco VPN Solutions Center: MPLS Solution API Programmer’s Reference*).

The Download to IPM (DIPM) Server

The Download to IPM (DIPM) Server is a C++ program that runs as a CORBA server in the MPLS VPN Solution software system. The DIPM Server implements the `CiscoDIPM::DIPMServer` interface in the `DIPM.IDL` file. The DIPM Server registers itself with the Orbix Name Service under the name *DIPMServer*. You can configure the server name in the `/opt/vpnadm/vpn/etc/ csm.properties` file.

The DIPM Server runs as a daemon within the MPLS VPN Solution software system, and is controlled by the MPLS VPN Solution software Watchdog process. The Watchdog “pings” the DIPM Server to make sure it is running. As shown in Figure A-1, the client process CORBA VPN Provisioning and Inventory Manager (CVPIM Server) makes requests to the DIPM Server for getting router configurations, and then for downloading configlets.

Figure A-1 MPLS VPN Solution and CIPM Communication Summary



The DIPM Server also acts as a CORBA client to the Cisco IP Manager Administration (ADM) and Network Element Manager (NEM) servers. The Cisco IP Manager NAM server accesses Cisco IP Manager domain information from the Cisco IP Manager Oracle database. The NEM server accesses element information from the Cisco IP Manager Oracle database, and also accesses the routers via Telnet.

You can also run the DIPM Server in Echo mode for testing and demonstrations. In Echo mode, the DIPM Server receives a router configuration file from the Repository. For downloading, the DIPM Server appends the configlets to the initial router configuration file, just prior to the “\nend” statement. The mode is determined by a property in the `csm.properties` file:

```
DIPMServer.mode = (CIPM,ECHO)
```

The DIPM Server uses the C++ API to read from the MPLS VPN Solution software database.

If all the Cisco IP Manager servers on the CIPM 2.0 workstation go down (after a system reboot, for example), the DIPM Server reconnects when the Cisco IP Manager system is back online. This occurs automatically without having to restart the DIPM Server. This behavior is implemented in the underlying IONA CORBA libraries.

For MPLS VPN Solution 1.1, if any of the Cisco IP Manager servers go down, a “Cisco IP Manager server disconnect” message is placed in the DIPM Server log file.

Configlet Download Process

Cisco IP Manager downloads configlets to the routers (PEs and CEs) in three stages:

1. Collects all the necessary current router configurations.
2. Calculates and construct the configlets.
3. Downloads the configlets to each router and collects the final router configuration files.

The DIPM Server client can specify whether the running configuration should be written to the startup configuration or not. The CVPIM Server is responsible for putting the final router configuration into the Repository. Each request to the Cisco IP Manager servers is a synchronous and blocking call. The requests that the CVPIM Server makes to DIPM Server are also synchronous and blocking.

The Cisco IP Manager CORBA API functions for locking and unlocking objects are not used since all functions to set attributes and read and write router configuration files do implicit locking of the object.

By default, MPLS VPN Solution software uses Telnet to upload and download configuration files to and from Provider Edge Routers (PEs) and Customer Edge Routers (CEs) in the service provider network.

If you wish to change that setting after CIPM is installed and use the Trivial File Transfer Protocol (TFTP) instead, you must complete these tasks:

- On the Cisco IP Manager workstation, set up a TFTP server.
- On the MPLS VPN Solution workstation, edit the `csm.properties` file to change the CIPM transfer mode to *TFTP*.

For information on how to accomplish these tasks, see the “Using TFTP to Transport Router Configuration Files” section on page 2-8.

DIPM Server `csm.properties` File Entries

The DIPM Server reads the MPLS VPN Solution software `csm.properties` file on startup to determine its operational mode and the location of the Cisco IP Manager system and its servers.

In the following properties, the host names are either set during the MPLS VPN Solution software installation, or later modified by hand. The DNS domain name can be blank, but it must match what was entered during the Cisco IP Manager installation.

```
# Cisco IP Manager specific settings
DIPMServer.CIPMNameServer= <CIPM_host>[.<DNS_domainname>]
DIPMServer.CIPMPPrimaryNEMServer= <CIPM_host>[.<DNS_domainname>]
DIPMServer.CIPMBackupNEMServer= <CIPM_host>[.<DNS_domainname>]
```

The backup NEM Server is not supported in Cisco IP Manager 2.0.

Naming Convention to Uniquely Identify Domains

A convention to uniquely identify domains and networks in both of the systems is required.

In MPLS VPN Solution software:

- A domain refers to a DNS domain.
- A network is used for grouping targets (CEs and PEs).
- Networks cannot contain other networks.

- The combination of *hostname.dns_domainname* is unique across the entire MPLS VPN Solution software system.

In Cisco IP Manager software:

- A domain is used for grouping purposes and can contain elements and other domains.
- All domain names are unique.
- All element names must be unique in each domain.

The domain and network naming convention is as follows:

MPLS VPN Solution software network is the equivalent of the Cisco IP Manager domain.

Because the element names are unique:

```
MPLS VPN Solution software network:hostname[.DNS_domainname] =Cisco IP Manager
domain:element_name
```

In Cisco IP Manager, the MPLS VPN Solution software network is created as a domain under the Cisco IP Manager Root domain (if it does not already exist in Cisco IP Manager). The MPLS VPN Solution software network can also preexist anywhere in the Cisco IP Manager domain hierarchy.

Obtaining an Element Reference from Cisco IP Manager

When a service request is first received from the CVPIM Server, an element object reference is retrieved from the Cisco IP Manager system. The DIPM Server searches for the element in Cisco IP Manager, if not found it will create the element in the Cisco IP Manager domain corresponding to the MPLS VPN Solution software network if it exists. If the domain does not exist it will be created in Cisco IP Manager under the “Root” domain, and then the element is created in the newly created domain. This process effectively synchronizes the elements in the MPLS VPN Solution software system into the Cisco IP Manager system, if the Cisco IP Manager system has no elements.

If the DIPM Server finds the element, it checks to see if the connection type is console. If it is, the DIPM Server does not update the user name, user password, and enable password. By using existing elements in the Cisco IP Manager system, the MPLS VPN Solution software system leverages the Cisco IP Manager’s ability to access routers through a terminal server. These elements need to be created and configured (for terminal server access) via the Cisco IP Manager GUI. For more information, see the “Setting Access to Routers with VTY, Console, or TACACS” section on page 2-5.

Element Attributes

The only required MPLS VPN Solution software element attributes are *hostname* (router name) and *network*. This applies for both “ECHO” mode and “CIPM” mode. If an MPLS VPN Solution software DNS domain is given, then it is appended to the hostname to create the element name in Cisco IP Manager. The MPLS VPN Solution software domain can also be in the Cisco IP Manager IP address string—see the next section for details.

The IP address in Cisco IP Manager is a string that can contain an IP address or a hostname. If an IP address is not entered in MPLS VPN Solution software, the DIPM server sets the IP address string in Cisco IP Manager to *element-hostname[.domainname]*. Cisco IP Manager uses whatever is in that string to access the device.

Field Length Element Attribute Mapping Table

The following table lists the MPLS VPN Solution software element fields and the corresponding Cisco IP Manager element attributes that differ in length. For MPLS VPN Solution software, the lengths are not checked before creating and setting in Cisco IP Manager, but Cisco IP Manager returns error 1005, “Input string too long,” if a field length is exceeded.

Table A-1 Field Length Element Attribute Mapping Table

| Repository Fields | MPLS VPN Solution Type | CIPM Element Attributes | CIPM Type |
|-------------------|------------------------|-------------------------|-----------|
| dir_network_name | Char 128 | domain name | Char 128 |
| dir_target_desc | Char 256 | description | Char 30 |
| dir_machine_addr | Char 128 | hostIP | Char 64 |
| dir_machine_desc | Char 256 | description | Char 30 |
| Dir_pw_uid1 | Char 64 | username | Char 32 |
| Dir_password1 | Char 128 | userPw | Char 72 |
| Dir_password2 | Char 128 | secretPw | Char 32 |



Note

For MPLS VPN Solution software, the network name is *not* case sensitive, but the domain name is case sensitive for Cisco IP Manager. Because all host names in MPLS VPN Solution software are lowercase, whenever you create elements in CIPM, be sure to assign names in lowercase.

Error Reporting

The Cisco IP Manager.PSErrorMapFile property contains the filename of the file that records the error strings corresponding to the Cisco IP Manager API function return codes defined in the Cisco IP Manager IDL files. In case of error, these strings and error codes are returned to the client by the DIPM Server. Any CORBA exceptions are returned to the client by the DIPM Server as error strings, along with an error status.

If there are any errors in downloading configlets, the DIPM Server attempts to get the final router configuration file and return it.

You can view the Cisco IP Manager logs using the Cisco IP Manager Log Viewer application. Note that all MPLS VPN Solution software generated log entries are for the vpnadm user. For detailed information about the Log Viewer, see Chapter 7, “System Administration and Log Management” in the *Cisco IP Manager (Lite) User’s Guide*.

