<table>
<thead>
<tr>
<th><strong>A</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>AAA</strong></td>
</tr>
<tr>
<td><strong>AAA client</strong></td>
</tr>
<tr>
<td><strong>AAA mode</strong></td>
</tr>
<tr>
<td><strong>access port</strong></td>
</tr>
<tr>
<td><strong>acknowledging discrepancy</strong></td>
</tr>
<tr>
<td><strong>acknowledging discrepancy</strong></td>
</tr>
<tr>
<td><strong>Associated ACL</strong></td>
</tr>
<tr>
<td><strong>Active Directory</strong></td>
</tr>
<tr>
<td><strong>Active end host</strong></td>
</tr>
<tr>
<td><strong>Active state</strong></td>
</tr>
<tr>
<td><strong>Active switch</strong></td>
</tr>
<tr>
<td><strong>activity trace</strong></td>
</tr>
</tbody>
</table>
adapter
Program that links a domain manager to its environment. Adapters forward inventory and event information to a domain manager for analysis. These adapters send the results of the analysis to other network management applications or other adapters.

Add devices
Sub-step in the Server Set up workflow. LMS allows you to add devices using multiple methods, simultaneously. You can add devices using the Import from File or NMS feature, and Campus Device Discovery.

Address Resolution Protocol
See ARP.

Adhoc Devices
Cisco devices or devices with a unique IP address.

Adhoc Target Device
External target devices that are added to LMS.

aggregate device
Device that contains more than one intelligent management agent, each with its own IP address. Cisco Prime recognizes such devices as multiple devices. For example, an MSFC on a switch. Also called a Containing or Composite device.

AIX
Advanced Interactive Executive: IBM's version of Unix.

alert
Indicator that is generated in LMS that indicates an abnormal condition in the network. An alert consists of related events. A finite set of alerts are displayed on the Alerts and Activities display.

Alias devices
Devices in LMS with different hostnames or IP addresses. When a new device is added to LMS, it may already exist in LMS, with another hostname or IP address. This device will be in the Alias state.

Allocate devices
Sub-step in the Getting Started workflow. This helps you to allocate devices that are managed by the functions in LMS.

ANIServer
Process that performs Data Collection. See also Data Collection.

Apache
Web server used in LMS on both UNIX and Windows systems. This hosts the base Cisco Prime Home Page and all major applications.

API
Application Programming Interface. A language and message format used by an application to communicate with the operating system and other services, such as a database management system or communications protocol.

Application Programming Interface
See API.

Application Registration
1. Process of registering the LMS applications with LMS Home Page on the local or remote servers.
2. Process of moving the information from LMS to ACS Server. Only when the applications are registered, can LMS use the AAA services from the integrated ACS server for user authentication and authorization.
<table>
<thead>
<tr>
<th><strong>Application Service Adapter</strong></th>
<th>See ASA.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Application specific groups</strong></td>
<td>Groups based on device types or states specific to LMS. The application-specific groups appear in the device selector of the respective applications.</td>
</tr>
<tr>
<td><strong>Application view</strong></td>
<td>Views that are displayed in Cisco Prime LMS Portal. These views are based on the installed applications. For instance, CS View (Common Services View).</td>
</tr>
<tr>
<td><strong>Approver</strong></td>
<td>Predefined role in LMS. Users assigned with this role can approve all LMS tasks.</td>
</tr>
<tr>
<td><strong>Archive Management</strong></td>
<td>Maintains an active archive of the configuration of devices managed by LMS. It enables you to fetch, archive, and deploy device configurations. It also lets you search and generate reports on archived data, compare and label configurations, compare configurations with a baseline, and check for compliance.</td>
</tr>
<tr>
<td><strong>archived report</strong></td>
<td>A report is archived when a scheduled report job is completed successfully.</td>
</tr>
<tr>
<td><strong>ARP</strong></td>
<td>One of the Discovery protocols supported by LMS Device Discovery. This Discovery module depends on the Routing Table Discovery module.</td>
</tr>
<tr>
<td><strong>AS</strong></td>
<td>Single Sign-On Master server providing authentication services to other LMS configured in the same domain.</td>
</tr>
<tr>
<td><strong>ASA</strong></td>
<td>Application-specific information repository. It is a source of devices and attributes that are grouped by the Groups server. It is also an interface among applications and the Groups server.</td>
</tr>
<tr>
<td><strong>ASCII</strong></td>
<td>American Standard Code for Information Interchange. 8-bit code for character representation.</td>
</tr>
<tr>
<td><strong>Assertion error</strong></td>
<td>Sybase Assertion error that occurs when the LMS databases do not run. This error appears if any anti-virus software or third-party backup software is used in the LMS.</td>
</tr>
<tr>
<td><strong>Audit Trail</strong></td>
<td>It tracks and reports changes that the administrator makes on the LMS server.</td>
</tr>
<tr>
<td><strong>AUS</strong></td>
<td>Web-based interface to upgrade device configuration files and software images on firewalls that use the Auto-update feature. You can use this interface to add, edit, and delete devices.</td>
</tr>
<tr>
<td><strong>Auth password</strong></td>
<td>SNMPv3 authentication password used to operate the devices in AuthNoPriv and AuthPriv modes.</td>
</tr>
<tr>
<td><strong>Auth protocol</strong></td>
<td>SNMPv3 authentication algorithm used in AuthNoPriv and AuthPriv modes. The authentication algorithm can be MD5 or SHA-1. These protocols ensure message integrity and protection against message replays.</td>
</tr>
<tr>
<td><strong>Authentication mode</strong></td>
<td>Mode selected to authenticate the LMS users when logging into the LMS. Either the ACS server or the LMS can provide the authentication services, based on the AAA mode set up in LMS.</td>
</tr>
<tr>
<td><strong>Authentication Profile</strong></td>
<td>Authentication profile selects the method of authentication to be used. Multi-method profiles provide a fallback order, if the first method fails, the second method will take over.</td>
</tr>
<tr>
<td><strong>AuthNoPriv</strong></td>
<td>One of the security levels within SNMPv3 providing message integrity and authentication security features.</td>
</tr>
<tr>
<td><strong>Authorization mode</strong></td>
<td>Mode selected to authorize the user after authentication. The Authorization services can be provided by the ACS or by the LMS.</td>
</tr>
<tr>
<td><strong>AuthPriv</strong></td>
<td>One of the security levels within SNMPv3 providing message integrity, authentication, and data encryption features.</td>
</tr>
<tr>
<td><strong>Auto mode</strong></td>
<td>Mode in which devices are managed in LMS. In this mode, all devices in DCR are automatically managed in LMS. Filter policies can be set to manage certain devices/set of devices.</td>
</tr>
<tr>
<td><strong>Automonitoring</strong></td>
<td>Monitors the inter-link switches automatically.</td>
</tr>
<tr>
<td><strong>Auto Smartports</strong></td>
<td>Auto Smartports macros dynamically configure ports based on the device type detected on the port. When the switch detects a new device on a port it applies the appropriate Auto Smartports macro to the port.</td>
</tr>
<tr>
<td><strong>Auto Smartport macros</strong></td>
<td>Allows you to save and share common configurations. Each Smartport macro is a group of CLI commands. When you apply a Smartport macro on a port, the CLI commands within the macro will be deployed on the port. If the command fails when applying a macro, either because of a syntax error or a configuration error, the macro continues to apply the remaining commands on the port. As part of provisioning Smartport, LMS provides the following Netconfig tasks: Auto Smartports—Task applicable for Device based Netconfig flow. See also Auto Smartports. Manage Auto Smartports—Task applicable for Port based Netconfig flow. See also manage Auto Smartports. Smartports—Task applicable for Port based Netconfig flow. See also Smartports.</td>
</tr>
<tr>
<td><strong>Auto Update server</strong></td>
<td>See AUS.</td>
</tr>
<tr>
<td><strong>Availability</strong></td>
<td>Checks the reachability of the target device, based on the successful completion of the RTT operation from source to target. The availability is reported as a percentage.</td>
</tr>
</tbody>
</table>
B

Backup data  See database backup.

bandwidth utilization  Measure of traffic flowing across a link.

Baseline template  You can identify a set of standardized policy-based commands that you want to have on a set of devices.

You can create a Baseline template (a set of commands identified through baselining) that contain placeholders for device-specific values to be substituted.

Best PracticeDeviation  Best practices that are recommended by Cisco but not implemented in the network.

BGP  One of the discovery protocols supported by LMS Device Discovery.

This discovery module uses Border Gateway Peer Table to identify its BGP peer.

BIRT  Business Intelligence and Reporting tool.

Border Gateway Protocol  See BGP.

broker  LMS software that communicates between a domain manager and its clients.

Browser server security  Security feature that LMS provides for secure access between the client browser and the management server.

LMS uses SSL to provide browser server security.

Bug Toolkit  Application in LMS that helps you identify the bugs filed against devices in their network. It also helps you to check the status of the bugs.

Built-in Group  In a Smart Install network, these groups are used to configure homogenous groups.

C

CA  Authority in a network that issues and manages security credentials and public keys for message encryption.

As part of a public key infrastructure, a certificate authority checks with a registration authority to verify information provided by the requestor about a digital certificate. If the registration authority verifies the requestor's information, the certificate authority issues a certificate.

called number  Destination telephone number of the call.

calling number  Telephone number from which the call originated.
| **Catalyst Integrated Security features** | You can use the Catalyst Integrated Security Features task to configure Port Security, DHCP Snooping, Dynamic ARP Inspection, IP Source Guard and Security Violation on ports. The Catalyst Integrated Security Feature is supported only on Catalyst 2960, 3560, 3560E, 3750, 3750E switches. This task is available only in the Port based flow of a NetConfig job. |
| **category** | Command or option specific to a selected device in CiscoView. You can modify or view categories to configure and monitor a device, card, or port. |
| **CCO** | Cisco Connection Online (former name of Cisco.com). The name of Cisco Systems’ external web site. |
| **CCR** | LMS component that manages the seamless installation, upgrade, patching and uninstallation of Multiple Device Controller modules, and the Core module. |
| **CDP** | Media- and protocol-independent device-discovery protocol that runs on all Cisco-manufactured equipment, including routers, access servers, bridges, and switches. It runs on all media that support SNAP, including LANs, Frame Relay, and ATM media. Using CDP, a device can advertise its existence to other devices and receive information about other devices on the same LAN or on the remote side of a WAN. |
| **certificate** | See security certificate. |
| **Certificate Authority** | See CA. |
| **CFM** | Connectivity Fault Management. |
| **Change Audit** | Tracks and reports changes made in the network. Change Audit logs information changes to a central repository. Device Configuration, Inventory, and Software Management changes can be logged and viewed using Change Audit. |
| **Change Audit reports** | Contains all change information provided by LMS, based on filter criteria. You can generate a Change Audit report for selected devices. It displays all changes that have been logged for the devices. The types of Change Audit reports are, 24-hour report, Exception period report, and Standard report. |
| **Change of Authorization (CoA)** | CoA provides a mechanism for changing the attributes of a session after it has been authenticated. |
| **Channel Interface Processor** | See CIP. |
chassis view  
Browser page that displays a graphical representation of a device’s front or back panel after you select a device in CiscoView. Device components are color-coded according to their status and refreshed according to the polling frequency you have defined.

Child group  
Groups and sub-groups that are part of container group.

CIP  
Channel attachment interface for Cisco 7000 series routers. The CIP connects a host mainframe to a control unit, eliminating the need for an FEP for channel attachment.

Cisco Discovery Protocol  
See CDP.

Cisco IOS software  
Cisco Internetwork Operating System software. Cisco system software provides common functionality, scalability, and security for many Cisco products.

The Cisco IOS software allows centralized, integrated, and automated installation and management of internetworks. It supports a wide variety of protocols, media, services, and platforms.

Cisco Medianet Solution  
The Cisco Medianet solution is an end-to-end architecture for a media-optimized network comprising advanced, intelligent technologies and devices in a platform that is optimized for the delivery of rich-media applications.

Cisco TAC  
Cisco Technical Assistance Center. There are four TACs worldwide.

Cisco.com Fetch Interval  
LMS allows you to configure the interval at which PSIRT and End of Sale or End of Life information is retrieved from Cisco.com.

The information retrieved is stored in the database. This database is queried to generate PSIRT Summary report or the End of Sale and End of Life reports.

CiscoView Planner page  
Page from which you can download the latest CiscoView device packages.

Cisco Prime Command Line Interface  
See cwcli.

Cisco Prime LMS Home Page  
Default home page that appears if you log into a LMS. If you have installed LMS Portal on the same LMS, LMS Portal will be the default home page.

Cisco Prime LMS Local mode  
One of the AAA modes. In the Cisco Prime LMS local mode, authentication and authorization services are provided by the local server. Also known as Non-ACS mode.

CLI  
Interface that allows you to interact with the operating system by entering commands and optional arguments. The Solaris operating system and DOS provide CLIs.

Cluster Discovery Module  
One of the discovery protocols supported by LMS Device Discovery.

This module discovers the devices in a DSBU cluster and queries the Cluster MIB to discover all members of the cluster.
<table>
<thead>
<tr>
<th><strong>Cluster managed device</strong></th>
<th>One of the device management types in DCR Administration. The Cisco clusters and their member devices are managed using this device management type.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cluster Switches</strong></td>
<td>A group of switches connected to each other, where one switch is designated as the Command switch and up to 15 switches can be designated as Member switches.</td>
</tr>
<tr>
<td><strong>CN</strong></td>
<td>Certificate Common Name.</td>
</tr>
<tr>
<td><strong>CNS managed devices</strong></td>
<td>One of the device management types in DCR Administration. Refers to the devices managed by Cisco Networking Services.</td>
</tr>
<tr>
<td><strong>collector</strong></td>
<td>Entity that encompasses a source router, a target device, an operation, and collector schedule details.</td>
</tr>
<tr>
<td><strong>collector groups</strong></td>
<td>Allows you to associate a group of collectors. The collector groups are defined based on a set of criteria such as operation name, operation type, source address, target address.</td>
</tr>
<tr>
<td><strong>collector schedule duration</strong></td>
<td>Indicates for how long (in days, hours, and minutes) the collector runs and gathers information from the source router. The default Start Time for a Collector is Immediate. The default End Time for a Collector is Forever. The polling period is set from 00:00:00 hours to 23:59:59 hours on a daily basis.</td>
</tr>
<tr>
<td><strong>Command Line Interface</strong></td>
<td>See CLI.</td>
</tr>
<tr>
<td><strong>Command sets</strong></td>
<td>Represents a logical grouping of commands. Each command set is associated with a unique name.</td>
</tr>
<tr>
<td><strong>Comma Separated Values</strong></td>
<td>See CSV.</td>
</tr>
<tr>
<td><strong>Common Name</strong></td>
<td>See CN.</td>
</tr>
<tr>
<td><strong>Common Object Request Broker Architecture</strong></td>
<td>See CORBA.</td>
</tr>
<tr>
<td><strong>community string</strong></td>
<td>Text string that acts as a password and authenticates messages sent between a management station and a router containing an SNMP agent. The community string is sent in every packet between the manager and the agent. Also called a community name.</td>
</tr>
<tr>
<td><strong>Compliance Management</strong></td>
<td>Option in LMS Configuration Management which deals with creating, maintaining and comparing Baseline Templates. You can create a baseline template and compare it with the configurations available on devices to check compliance.</td>
</tr>
<tr>
<td><strong>composite device</strong></td>
<td>See aggregate device.</td>
</tr>
<tr>
<td><strong>Config Editor</strong></td>
<td>Option in LMS that provides easy access to configuration files. Config Editor allows a network administrator with the appropriate security privileges to edit a configuration file that exists in the configuration archive.</td>
</tr>
<tr>
<td>Term</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Configuration Dashboard</td>
<td>Configuration Dashboard in LMS provides information such as, date of last configuration change, status of the configuration jobs, summary of inventory configuration protocol, Hardware and Software summary.</td>
</tr>
<tr>
<td>Configuration Management</td>
<td>Stores the current, and a user-specified number of previous versions, of the configuration files for all supported Cisco devices maintained in the LMS. It tracks changes to configuration files and updates the database if there are any changes.</td>
</tr>
<tr>
<td>Configure Range</td>
<td>Tab on the Run Discovery on server page (Add Devices) allows you to limit discovery by IP addresses in your network. Establishing IP address boundaries prevents discovery from occurring outside these boundaries.</td>
</tr>
<tr>
<td>conflicting device</td>
<td>Device that is both in the import source and in DCR but differs in its attributes. The DCR Import Status report displays the conflicting devices after every Import operation.</td>
</tr>
<tr>
<td>Connectivity Group</td>
<td>This is a custom group which is used to set up the image and configuration file for all client switches that match connectivity.</td>
</tr>
<tr>
<td>Connectivity status</td>
<td>Table in LMS that provides information on device connectivity. It displays the Ping, Trace route, Telnet statuses of the device, along with other related information.</td>
</tr>
<tr>
<td>contained device</td>
<td>Subordinate device that resides inside an aggregate (or containing) device. For example, an MSFC in a switch).</td>
</tr>
<tr>
<td>container group</td>
<td>Groups without a rule. The group membership is the union of the membership of its subgroups. If a container group does not have subgroups, the membership list will be blank.</td>
</tr>
<tr>
<td>containing device</td>
<td>See aggregate device.</td>
</tr>
<tr>
<td>context menu</td>
<td>Menu that appears when you right-click a device or its components in CiscoView. The items in this menu are context-sensitive and vary according to the device and your selection.</td>
</tr>
<tr>
<td>Contract Connections</td>
<td>Application allows you to see the status of service contracts of all IOS devices in the network. Contract Connection allows you to verify which of your Cisco IOS devices are covered by a service contract.</td>
</tr>
<tr>
<td></td>
<td>Contract Connection (CC) uses Inventory Manager, Cisco.com, and Cisco's internal contract tracking service, Contract Agent, to provide the status of the service coverage. You can generate Contract Connection reports using Reports Center.</td>
</tr>
<tr>
<td>COS</td>
<td>Class of Service.</td>
</tr>
</tbody>
</table>
CORBA

Industry standard middleware architecture developed and maintained by the Object Management Group.

CORBA services act as communication mechanisms to develop distributed applications. CORBA is platform and language neutral. This means that a C application running on a PC can communicate with a Java application running on Solaris.

Core Client Registry

See CCR.

core file

File created by the Operating System in LMS when a program is abnormally terminated.

The core file is created in the NMSROOT\bin directory on LMS and stores important data about processes.

Critical Device Poller

Polls only a critical set of devices in the network. You can use this option to see the device and link status without running Data Collection.

CS

Represents a common set of management services that are shared by LMS. This provides a foundation for LMS to share a common model for data storage, login, user role definitions, access privileges, security protocols, as well as navigation.

CSR

Certificate Signing Request file.

CSV

Interchange file format used to export and import spreadsheets or other tables. Each line in the ASCII file represents a row of data from a table. Each line contains the data elements from a row of the table, with individual table values separated by comma characters.

custom layout

Special layout of report columns to suit specific needs. The layout can be designed by selecting and arranging the required columns from the available ones.

custom report

Report with a customized layout to suit specific needs.

Custom Report feature

Cisco Prime LMS allows you to create reports using MIB variables that are either common to all Pollers or specific to a Poller polled by LMS. These reports are called Custom Reports.

Custom Report Template

Option available under Reports that allows you to create new report templates, customized according to their requirements. You can edit, or delete existing custom templates.

Customer Edge Router

Router on the border between a VPN provider and a VPN customer that belongs to the customer.

cwcli

A netshow command that let you use NetShow features from the command line. You can use the cwcli netshow commands to view, browse, create, delete, and cancel NetShow jobs and Command Sets.

cwcli config

Cisco Prime configuration command-line tool of LMS. It allows you to update devices and archive configurations, delete configurations and compare configurations.
cwcli export
Cisco Prime export command-line tool of LMS. This command-line tool provides servlet access to Inventory, Configuration and Change Audit data.

cwcli inventory
Cisco Prime Device Management application command-line tool of LMS. You can use this tool to check the device credentials, export the device credentials, view or delete the LMS devices.

cwcli invreport
Cisco Prime Inventory command-line tool of LMS. It allows you to run previously created Inventory Custom reports and also system reports. The output is displayed in the (CSV) Comma Separated Value format.

cwcli netconfig
Cisco Prime netconfig command-line tool of LMS. It allows you to use NetConfig from the command line.

cwcli netshow
Cisco Prime NetworkShow (NetShow) command-line tool that enables users to use NetShow features from the command line. You can use the cwcli netshow tool to view, browse, create, delete, and cancel NetShow jobs and Command Sets.

D

Daemon Manager
Daemon is a long-running background process that answers requests for services. Daemon Manager controls the various daemons running and can be used to start, stop, or monitor them.

Dashboard
Dashboards provide you with a quick snapshot of specific functions in LMS. The following functional dashboards are available in LMS:

- Monitoring Dashboard
- TrustSec Dashboard
- EnergyWise Dashboard
- Inventory Dashboard
- Configuration Dashboard
- Device Status Dashboard
- System Dashboard

Data Collection
Fetches the device list from DCR and collects complete information about the devices.

Data Collection filters
Filters that you can set to either include or exclude of IP address ranges in Data Collection.

Data Extraction Engine
Utility to export LMS data in XML format.

data trace
Specifies standard network traffic trace between IP addresses or named devices.

database backup
Saving the database to maintain a safe copy of data. To start backing up data, you must have enough storage space on the target location.
<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>database restore</strong></td>
<td>Restoring the data that you had backed up earlier on the LMS.</td>
</tr>
<tr>
<td><strong>data-link switching</strong></td>
<td>See DLSw.</td>
</tr>
<tr>
<td><strong>DCR</strong></td>
<td>Common repository of devices, their attributes, and credentials that are used by various network management applications.</td>
</tr>
<tr>
<td><strong>DCR Administration</strong></td>
<td>Interface to administer the common repository of devices, their attributes, and credentials used by LMS.</td>
</tr>
<tr>
<td><strong>DCR Master</strong></td>
<td>Hosts the authoritative, or a master-list of all devices and their credentials. All other DCRs in the same management domain that are running in the Slave mode, normally share this list.</td>
</tr>
<tr>
<td><strong>DCR modes</strong></td>
<td>DCR works based on a Master-Slave model. The Master hosts the authoritative, or a master-list of all devices and their credentials. All other DCRs in the same management domain that are running in the Slave mode, normally share this list. DCR can also be in the Standalone mode. In the Standalone mode, DCR maintains an independent repository of device list and credential data. See also DCR.</td>
</tr>
<tr>
<td><strong>DCRDevicePoll</strong></td>
<td>LMS backend process that initiates device polling. It uses SNMP and ICMP protocols to check whether the devices are reachable.</td>
</tr>
<tr>
<td><strong>DCR Slave</strong></td>
<td>DCR mode that runs as a Slave to a Master server in the same management domain and shares the device list from the Master.</td>
</tr>
<tr>
<td><strong>DCR Standalone</strong></td>
<td>DCR mode that maintains an independent repository of the device list and the credential data.</td>
</tr>
<tr>
<td><strong>dcrcli</strong></td>
<td>Utility provided with LMS to perform the device management tasks through CLI.</td>
</tr>
<tr>
<td><strong>debugging</strong></td>
<td>Finding reasons for runtime issues. Enabling debugging options creates log files. You can use these log files to find the cause for a runtime problem.</td>
</tr>
<tr>
<td><strong>default credentials</strong></td>
<td>Default credentials are stored in DCR and are not associated with any device. You can use them to add or import a set of devices in DCR with common credentials. See also default credential set.</td>
</tr>
<tr>
<td><strong>default credential set</strong></td>
<td>Credential set that comprises Primary credentials, Secondary credentials, SNMP credentials, HTTP credentials, AUS managed credentials, and Rx-Boot mode credentials. You can configure multiple default credential sets. You can set these default credential sets for a range of devices to be added or imported to DCR based on certain policies.</td>
</tr>
<tr>
<td><strong>Delete interval</strong></td>
<td>Time interval at which records from End host table, IP Phone table, Wireless end hosts table, and the History table are deleted.</td>
</tr>
<tr>
<td><strong>Desktop Switching Business Unit</strong></td>
<td>See DSBU.</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>----------------</td>
</tr>
<tr>
<td><strong>Detailed Device report</strong></td>
<td>One of the Inventory reports. It displays detailed hardware, software characteristics and physical containment information for one or more selected devices. The hardware and software characteristics include System, Port Interface, Bridge, Memory Pool, Flash Devices, and Image. The physical containment information includes Stack, Chassis, Module, and Processor information.</td>
</tr>
<tr>
<td><strong>Device Allocation Policy</strong></td>
<td>The policy you must configure to manage the devices in your network.</td>
</tr>
<tr>
<td><strong>Device and Credential Repository</strong></td>
<td>See DCR.</td>
</tr>
<tr>
<td><strong>device attributes</strong></td>
<td>Unique identifiers of a device such as domain name, hostname, device identity and management IP Address.</td>
</tr>
<tr>
<td><strong>device based acquisition</strong></td>
<td>Process that discovers the End Hosts on all the VLANs in the selected device. Helps you to collect information only on End Hosts connected to the specified device.</td>
</tr>
<tr>
<td><strong>Device Based VRF report</strong></td>
<td>Displays the VRF details specific to the VRF configured devices selected while generating the report. See also VRF-Lite.</td>
</tr>
<tr>
<td><strong>Device Center</strong></td>
<td>Provides a device-centric view for LMS and device-oriented navigation paradigm. This provides device-centric features and information from a single location.</td>
</tr>
<tr>
<td><strong>Device Credentials</strong></td>
<td>Values that are used by applications to access and operate on devices. It is typically an SNMP community string or a user ID and password pair.</td>
</tr>
<tr>
<td><strong>Device Diagnostic Tools</strong></td>
<td>Portlet from where you can launch Device Troubleshooting workflow and Device Center. See also Device Troubleshooting.</td>
</tr>
<tr>
<td><strong>Device Discovery</strong></td>
<td>Discovers the devices available in the network, starting from the seed device and updates the information to DCR. See also seed device.</td>
</tr>
<tr>
<td><strong>Device Management</strong></td>
<td>Device Management refers to adding, editing and deleting devices in LMS. In other words, it refers to managing devices in LMS. In addition to these tasks, Device Management also verifies the device credentials. Device Management also consists of Inventory Management and Group Administration.</td>
</tr>
<tr>
<td><strong>Device Management mode</strong></td>
<td>Mode in which the devices are managed in LMS application. It can be either Auto mode or Manual mode.</td>
</tr>
<tr>
<td><strong>Device Map</strong></td>
<td>List of all supported devices on a LMS maintained by Software Center.</td>
</tr>
<tr>
<td><strong>Device package</strong></td>
<td>Software update that enables CiscoView to support new features for a particular device.</td>
</tr>
</tbody>
</table>
| **Device Package Updates** | Applications that provide support for a range of devices by installing device packages.

You can add device packages to the applications anytime after the initial product release or installation. When new device packages become available, they are placed on Cisco.com. |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Device Poller</strong></td>
<td>Process that polls the devices in the network. Polling checks if the devices managed by LMS are SNMP reachable, and if the interfaces in the devices are up or down.</td>
</tr>
</tbody>
</table>
| **Device report** | In LMS, this report displays all performance parameters of a device, such as memory utilization, CPU utilization, interface utilization, environmental temperature, Poller failures and so on.

The Device report also displays the polled data for MIB variables added in the user-defined templates.

LMS generates Device report based only on the data for the last 24 hours. |
| **Device Selector** | Device Selector allows you to search the devices in DCR. It helps to locate the devices and quickly perform the various device management tasks. |
| **device state** | Management state of a device. Can also pertain to the device discovery state. See also management state and Discovery state device. |
| **Device Troubleshooting** | One of the LMS workflows. Device Troubleshooting workflow helps you identify why a device is unreachable.

The generated Device Troubleshooting report contains details on device topology, network inconsistencies, misconfiguration, and Alerts and Syslog Messages for the selected device. |
| **DfmServer/ DfmServer 1** | Infrastructure device domain manager, a program that provides backend services for Fault Management. Services include SNMP data retrieval and event analysis. The DfmServer log is NMSROOT/objects/smarts/logs/DFM.log.

If there are two instances of the DfmServer running, each will have a log file, DFM.log and DFM1.log. |
<p>| <strong>DHCP</strong> | Dynamic Host Configuration Protocol. Allows you to allocate IP addresses dynamically so that addresses can be reused when hosts no longer need them. |
| <strong>DiscoveryCli</strong> | A command line utility used to start, stop and view the current status of Device Discovery. |
| <strong>Discovery, device</strong> | In LMS, this is the process of probing to analyze a network element. Also referred to as collection. |
| <strong>Discovery Filters</strong> | Allows Device Discovery to exclude or include devices from the network, based on some rules. |
| <strong>Discovery Modules</strong> | Various protocols used by Device Discovery to discover the devices from a network. |</p>
<table>
<thead>
<tr>
<th>Discovery state</th>
<th>Condition that a device passes through while being probed. After Discovery, the device information is added to the inventory. Device Discovery states include Known, Learning, Questioned, Pending and Unknown.</th>
</tr>
</thead>
<tbody>
<tr>
<td>discrepancy</td>
<td>Network inconsistencies or anomalies or misconfigurations in the discovered network. They have a severe impact on the network connectivity.</td>
</tr>
<tr>
<td>Diskwatcher</td>
<td>Back-end process that monitors disk space availability on the LMS. This process calculates the disk space information of a drive (on Windows) or a file system (on Solaris) where LMS, are installed and stores them in diskWatcher.log file.</td>
</tr>
<tr>
<td>Distinguished Name</td>
<td>See DN.</td>
</tr>
<tr>
<td>DLSw</td>
<td>Data-link switching. Interoperability standard, described in RFC 1434, allows you to forward SNA and NetBIOS traffic over TCP/IP networks using data-link layer-switching and encapsulation.</td>
</tr>
<tr>
<td></td>
<td>DLSw uses SSP instead of SRB, eliminating the timeouts, lack of flow control, and lack of prioritization schemes. See also SRB and SSP.</td>
</tr>
<tr>
<td>DN</td>
<td>Unique name used by authentication servers when you integrate LMS with external MS Active Directory or IBM SecureWay Directory servers. Distinguished Name is usually composed of the three parts: prefix, usersroot and login.</td>
</tr>
<tr>
<td>DNS</td>
<td>Domain Name System. System used in the Internet for translating names of network nodes into addresses.</td>
</tr>
<tr>
<td>Domain manager</td>
<td>See DfmServer/ DfmServer 1.</td>
</tr>
<tr>
<td>Domain Name System</td>
<td>See DNS.</td>
</tr>
<tr>
<td>domain server</td>
<td>See Domain manager.</td>
</tr>
<tr>
<td>Dormant MAC</td>
<td>MAC Addresses that are inactive for the specified number of days.</td>
</tr>
<tr>
<td>DSBU</td>
<td>Desktop Switching Business Unit. One of the business units of Cisco.</td>
</tr>
<tr>
<td>DSBU cluster</td>
<td>See Cluster managed device.</td>
</tr>
<tr>
<td>duration</td>
<td>Number of minutes that a collector actively collects network performance statistics at the source router. The default value is Forever.</td>
</tr>
<tr>
<td>dynamic group</td>
<td>Group for which the membership list is automatically recomputed whenever it is invoked and is always current.</td>
</tr>
<tr>
<td>Dynamic Host Configuration Protocol</td>
<td>See DHCP.</td>
</tr>
</tbody>
</table>
Dynamic Updates
Same as Dynamic User Tracking.

Dynamic User Tracking
Asynchronous updates based on SNMP MAC notifications traps. These updates are used by LMS to track real-time changes in the end hosts connected to the network.

Echo
Measures the total round-trip latency and other statistics and errors from the source router to the target device.

EDS
Event management software that allows you to send messages from one process to another in a networked and distributed environment.

EEM
Embedded Event Manager is an IOS technology that runs on the control plane of the Cisco Catalyst 6500 device. This EEM technology is integrated within Cisco IOS Software and because of this, the Cisco IOS Software EEM is aware of the state of the network from the perspective of view of the device on which it is operating.

Embedded Event Manager
See EEM.

End Host/IP Phone Down
One of the LMS workflows. The generated End Hosts/IP Phone Down report helps you locate and track the End Hosts/IP Phone in your network. They also provide information to troubleshoot and analyze the connectivity issues.

End of Sale/End of Life report
See EoS/EoL report.

End of Sale/End of Life Hardware report
Inventory report that is generated based on the End of Sale/End of Life information retrieved from Cisco.com at regular intervals.
This report helps you to ascertain the end-of-sales and end-of-life information for devices and modules in the network. It provides a summary of the end-of-sale or end-of-life alerts based on the selected devices.

End of Sale/End of Life Software report
Reports that provide information on the end-of-sale, end-of-life, and the end-of-engineering dates for the software image versions running on the devices in your network.
You can generate an EoS/EoL Software report for software images based on the information retrieved from Cisco.com at regular intervals.

EnergyWise
EnergyWise is a comprehensive program for power management in your network.

EnergyWise in Cisco Prime LAN Management Solution 4.2 provides a set of management functionalities to simplify and automate the energy management lifecycle of network infrastructure, and of devices attached to the network.

EnergyWise Domain
An EnergyWise domain consists of Cisco domain members and end points. A domain can represent a geographic location, a specific place in the network, or any energy specific logical representation.
EnergyWise Endpoint Groups
You can create endpoint groups to group endpoints based on certain filters like role, importance, and keywords. The endpoints can be part of one or more domains. After you create an endpoint group, you can apply policies to the group.

EnergyWise Policies
You can configure EnergyWise policies, a set of recurring events, to manage the power usage of devices in the network.

EoS/EoL report
See End of Sale/End of Life Hardware report and End of Sale/End of Life Software report.

Error device
Device that is not successfully added or imported to DCR. The error devices are listed in DCR Device Addition Summary or DCR Import Status report after the Add or Import operation.

ESS
Asynchronous messaging service that provides a messaging infrastructure based on a publish-and-subscribe paradigm. It enables distributed, loosely coupled interprocess communications.

ethernetJitter
Ethernet Jitter is an IPSLA Operation.
LMS provides the option to create, modify, or delete your own Ethernet Jitter operations from the List of Operations page for measuring performance between a source and MEP.

ethernetJitterAuto IPSLA
Ethernet Jitter Auto IPSLA is an Auto IPSLA Operation.
LMS allows you to create, modify, or delete your own Ethernet Jitter Auto IPSLA operations from the List of Operations page for measuring performance between a source and MEP.

ethernetPing
Ethernet Ping is an IPSLA Operation.
LMS allows you to create, modify, or delete your own Ethernet Ping operations from the List of Operations page for measuring Round-trip time latency and Errors between a source and MEP.

ethernetPingAuto IPSLA
Ethernet Ping Auto IPSLA is an Auto IPSLA Operation.
LMS allows you to create, modify, or delete your own Ethernet Ping Auto IPSLA operations from the List of Operations page for measuring performance between a source and MEP.

event
Indicator that is generated in LMS when a fault occurs on a network. Related events are “rolled up” into alerts. A finite set of events is displayed on the Alerts and Activities Detail page.

Event Distribution System
See EDS.

Event Forensics
Event Forensics refer to additional information related to the specific events that are polled by LMS server.

Event Monitor
A centralized place where in you can view the event details of all devices.
Event Services Software
See ESS.

Extensible Markup Language
See XML.

Extensible Stylesheet Language
See XSL.

F

fallback option
Allows you to access the software if the login module fails, or if you accidentally lock yourself or others out. The fallback options are available only for non-ACS login modules.

Faster Discovery
Discovered devices gets added to DCR every 2 mins. This enables faster discovery results to the end user. “Device Newly Added to DCR” and “Device Updated to DCR” will be updated on regular intervals, before completion of the entire discovery cycle.

FAT
A file system table used by the FAT file systems.

Fault Monitor
A centralized browser where you can view the information on faults and events of devices in a single place.

File Allocation Table
See FAT.

File Transfer Protocol
See FTP.

firewall
One or more routers or access servers designated as a buffer between any connected public networks and a private network to ensure security.

FPM
Flexible Packet Matching (FPM) is a next-generation Access Control List (ACL) technology that is capable of filtering IP packets at a bit-level. As part of provisioning, LMS provides the following netconfig tasks that allow you to configure FPM in the devices:

- **FPM Package Group**—Task applicable for Device based Netconfig flow
- **FPM Package-Info**—Task applicable for Device based Netconfig flow
- **FPM Policy**—Task applicable for Port based Netconfig flow

FPM Package Group
You can use the FPM Package-Group task to add, edit and remove FPM package groups.

The FPM Package-Group task is available only in the Device based flow of a NetConfig job.
FPM Package-Info
You can use the FPM Package-Info task to configure FPM package info on the devices.

The FPM Package-Info task is available only in the Device based flow of a NetConfig job.

FPM Policy
You can use the FPM Policy task to attach or detach package groups to or from an interface.

The FPM Policy task is available only in the Port based flow of a NetConfig job.

FQDN
Fully Qualified Domain Name consisting a host name and domain name.

Frequently Used Links portlet
Helps you to view the frequently used links. You can also add, modify and remove the frequently accessed links.

FTP
File Transfer Protocol (FTP) operation allows you to measure the network response time between a Cisco device and an FTP server to retrieve a file.

Functional View
Default view when you log into LMS for the first time. For subsequent logins, you can set any view as the default view. Contains portlets that help you to launch the applications installed in the LMS.

G
Generic OnLine Diagnostics
See GOLD.

Getting Started workflow
Getting Started workflow in LMS assists you in performing the following basic tasks required to get your Cisco Prime LMS running:

- Understanding the Procedure to Migrate Data
- Configuring E-mail, Cisco.com and Proxy Settings
- Checking Protocol, Security, Backup and Authentication Settings
- Managing Devices and Credentials
- Managing User Roles and Users in LMS
- Updating Software and Device Packages
- Advanced Configurations and Settings

You can configure these tasks step-by-step or configure them separately at different intervals. You can select the task using the Getting Started assistant pane.

Global seed devices
Seed devices that are common to all Discovery modules selected for a Device Discovery process.

GOLD
Device-specific IOS feature with fault detection capabilities. It defines a common framework for diagnostic operations across Cisco platforms running Cisco IOS Software.
GOLD Health Monitoring Task

Task that allows you to configure GOLD Health Monitoring tests on Cisco Catalyst 6500 IOS switches device categories.

This task is available only for the Module-based netconfig job wizard. See also GOLD.

Graphical User Interface

See GUI.

group

Named aggregate entity comprising a set of devices belonging to a single class or a set of classes, with a common superclass. Groups can be shared among users or applications, subject to access-control restrictions. The membership of a group is determined by a rule.

Group Admin

Allows you to interact with the Groups Server to create and manipulate groups using Group Admin.

Group Hierarchy

Hierarchical fashion of groups and subgroups.

Group Membership

Allows you to assign objects to a group or exclude objects from a group.

Group Rule

Consists of one or more rule expressions combined by operators. These operators can be AND, OR or EXCLUDE. A rule always evaluates to objects of a particular class defined in an application schema.

Group Selector

List-tree that displays all device groups. Allows you to add a device to the tree and modify, view or refresh the group details. You can also add the groups to the group selector or remove them from the list-tree.

Group Server

Manages groups of devices. It helps you to create, edit, delete, and refresh groups to be shared by the application. It interfaces with an application service adapter to evaluate group rules and retrieve devices of a particular group.

GUI

User environment with textual and graphical representation of the application. Conventions such as buttons, icons, and windows are typical, and many actions are performed using a pointing device (such as a mouse). Microsoft Windows and the Apple Macintosh are examples of platforms using a GUI.

H

Help Desk

Predefined role in LMS. Users with this role can access network status information only. Can access persisted data on the system and cannot perform any action on a device or schedule a job that will reach the network.

Hewlett Packard OpenView

See HPOV.

Hierarchical maps

Topology views that display the devices listed under Topology Groups in a hierarchical way. Each map displays the selected group as a cloud of devices. If there are parent and sub-groups, the sub-group is displayed inside the corresponding parent group as a cloud icon.
**High Security Mode**
High Security Mode ensures the highest security level of LAN-based access, where access is not granted unless authentication succeeds.

**Histo Graph-It**
Portlet that enables you to query the information of a particular MIB variable in a device for a specified period of time and generate a graph.

**Historical reports and graphs**
LMS generates these reports and graphs that contain statistical data for a single or group of collectors based on the granularity, such as hourly, daily, monthly, or weekly.

**History report**
Tracks the log in and log out information about the End Hosts and the users in your network.

**hop**
Passage of a data packet between two network nodes. For example, between two routers. See also hop count.

**hop count**
Number of hops till which the network topology is drawn in N-Hop view portlet. See also hop.

**host**
Computer system on a network. Similar to the term node, except that host usually implies a computer system, whereas node generally applies to any network system, including access servers and routers.

**Host Mode**
Host mode determines the number of hosts that can be authenticated on a given port.

**Hostname change script**
CLI utility to update the new hostname information in the Cisco Prime directories and files, registry entries, and databases. This occurs after you have changed your hostname in the Cisco Prime machine.

**Hot Standby Router Protocol**
See HSRP.

**HPOV**
Hewlett Packard OpenView. A third party software used as network management systems for LMS.

**HSRP**
One of the Discovery protocols supported by Device Discovery.

This module discovers the devices from the HSRP group which consists of an active router and Standby routers. If the active router fails, one of the Standby router will server as an active router.

The HSRP Discovery Module uses cHsrpGrpTable in CISCO-HSRP-MIB to find active or standby routers.

**HTTP**
Protocol used by Web browsers and Web servers to transfer files, such as text and graphic files.

**HTTPS**
HTTP Over SSL.

**Hypertext Transfer Protocol**
See HTTP.
<table>
<thead>
<tr>
<th><strong>I</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ICMP</strong></td>
</tr>
<tr>
<td><strong>ICMP Jitter</strong></td>
</tr>
<tr>
<td><strong>Identity</strong></td>
</tr>
<tr>
<td><strong>IDU</strong></td>
</tr>
<tr>
<td><strong>IGMP</strong></td>
</tr>
<tr>
<td><strong>IIS</strong></td>
</tr>
<tr>
<td><strong>Inactive State</strong></td>
</tr>
<tr>
<td><strong>Incremental Device Update</strong></td>
</tr>
<tr>
<td><strong>In Service Software Upgrade</strong></td>
</tr>
<tr>
<td><strong>Install Mode - Software Distribution</strong></td>
</tr>
<tr>
<td><strong>instance</strong></td>
</tr>
<tr>
<td><strong>Integration Utility</strong></td>
</tr>
<tr>
<td><strong>Internet Control Message Protocol</strong></td>
</tr>
<tr>
<td><strong>Internet Control Message Protocol Jitter</strong></td>
</tr>
<tr>
<td>Term</td>
</tr>
<tr>
<td>------</td>
</tr>
<tr>
<td>Internet Group Management Protocol</td>
</tr>
<tr>
<td>Internet Information Services</td>
</tr>
<tr>
<td>Internet Protocol</td>
</tr>
<tr>
<td>interval</td>
</tr>
</tbody>
</table>
| inventory | 1. List of all of the network elements in the repository of a domain manager, and the relationships between those elements. The inventory includes devices and their components.  
2. In-memory, object-oriented data structure of LMS that stores information about the managed elements currently in a network, and the relationships between these elements. |
| Inventory Management | Inventory, or the Inventory Collection Service (ICS) and Poller software component of LMS, collects inventory data from the network devices and updates the inventory.  
If any changes are detected in hardware or software components, the inventory database is updated and a change audit record is created to inform the network manager of the change, and to document the event. This ensures that the information displayed in the Inventory reports reflects the current state of network devices. |
| IP | Internet Protocol. Network layer protocol in the TCP/IP stack offering a connectionless internetwork service. IP allows you to address type-of-service specification, fragmentation and reassembly, and security. |
| IP Address | 32-bit address assigned to hosts using TCP/IP. An IP Address belongs to one of five classes (A, B, C, D, or E) and is written as 4 octets separated by periods (dotted decimal format). Each address consists of a network number, an optional subnetwork number, and a host number.  
The network and subnetwork numbers together are used for routing, while the host number is used to address an individual host within the network or subnetwork.  
A subnet mask is used to extract network and subnetwork information from the IP Address. CIDR provides a new way of representing IP Addresses and subnet masks. See also IP. |
| IP Phone Acquisition | Process that collects information about the IP Phones connected in the network. |
**IPSLA**
Internet Protocol Service Level Agreement. This was formerly known as SAa. A portfolio of technology embedded in most devices that run Cisco IOS software. This allows you to analyze IP service levels for IP applications and services, to increase productivity, to lower operational costs, and to reduce the frequency of network outages.

**IPSLA Availability**
A dashboard which displays information such as Operation Types, Number of Collectors and Availability percentage ranges.

**IPSLA Responder**
Component embedded in a target Cisco device running version 12.1 or later of the Cisco IOS software. It responds to IPSLA request packets from a source device and provides accurate results.

**IPv6**
Replaces the IP version 4. IPv6 includes support for flow ID in the packet header, which can be used to identify flows. Formerly called IPng (next generation).

**ISSU**
LMS supports In Service Software Upgrade process that allows Cisco IOS software images to be updated without rebooting the device. This increases network availability and reduces downtime caused by planned software upgrades.

**J**

**JacORB**
Object Broker Services provided and used by LMS.

**Java Runtime Environment**
See JRE.

**Jitter**
Inter-packet delay between any two consecutive data packets sent between the source and target router.

**job**
Reports that are scheduled to run at a later time.

**Job Approval**
Jobs can be scheduled by the various LMS applications such as NetConfig, Config Editor, Archive Management, and Software Management. Job Approval allows you to designate one person in a group of users as a Job Approver who will approve each job before it runs.

When Job Approval is enabled, applications that use it, require a job to be scheduled to run in the future, instead of immediately. Job approval cannot be enabled for jobs that run immediately.

Job Approval is also referred to as Maker Checker.

**Job browser**
Central place to manage all jobs in LMS.

The job management tasks include view the list of jobs, view the details of a selected job, stop a job and delete a job.

**Jobs and Resources Manager**
See JRM.
Join Window  
Join window is the period during which DHCP requests are processed by the SI director.

JRE  
Also known as Java Runtime, consists of the Java virtual machine, the Java platform core classes, and supporting files. It is the runtime part of the Java Development Kit that does not have a compiler, debugger, or tools. It is the smallest set of executables and files that constitute the standard Java platform.

JRM  
Jobs and Resources Manager. Allow applications to schedule an activity, track job instances, lock or unlock resources, and send notifications.

K  
KeyStore  
See TrustStore.

L  
LAN Management Solution  
See LMS.

last configuration change  
Device Troubleshooting report displays the time when the running configuration was archived in the Configuration Archive and the differences between the two archived running configurations in the Configuration Archive, under this head.

latency  
Time taken for a packet to travel from the source to target and back. It is also referred to as RTT (Round-Trip Time).

layouts  
Manner in which the portlets are arranged in a view.

LDAP  
Lightweight Directory Access Protocol. Protocol that allows access to management and browser applications that provide read/write interactive access to the X.500 Directory.

legend  
Explains the use of icons and colors in network views. Legends are available for Topology Services and Path Analysis in LMS.

Lightweight Directory Access Protocol  
See LDAP.

Link Layer Discovery Protocol (LLDP)  
Link Layer Discovery Protocol module uses entPhysicalTable MIB to find its neighbor’s IP Address.

link ports  
Ports connected to Cisco devices (Switch or Router) are link ports. See also trunk port.

Link Registration  
Adding additional links to LMS homepage for Custom tools and home grown tools, and third party applications such as HPOV. The links appear under the Third Party or Custom Tools, as you specify them.
Glossary

Live Graph-It
Portlet that enables you to do real-time monitoring for any MIB variable that belongs to a device that is managed by DCR.

LMS
Software solution bundle that provides applications to configure, administer, monitor, and troubleshoot a network. It enables network administrators to effectively manage their LAN and campus networks.

LMS Portal
Cisco Prime LMS Portal is the first page that appears when you launch the LMS application. It serves as an interface, launch point and top-level navigation for the frequently used functions in the application.

You can view the important statistics and details of the LMS applications installed on your LMS, in a single page instead of navigating through several pages to view the required data.

Local NMS
Network Management System on the local LMS. See also NMS.

local server
Identifies the LMS on which the Server Setup workflow is run.

local upgrade
Process of upgrading to a newer version of Cisco Prime software on the same machine.

local user setup policy
Username and password policies for local users in LMS.

This policy allows to start the local username with a number, include special characters in local username, and specify the length of the local username and the local user password.

log level settings
You can set the LMS log level settings. You can set the log level to Error, Fatal, Warn (Default), Info, or Debug. The log file, LMS log, is stored at /var/adm/CSCOpx/log on Solaris, and NMSROOT/log on Windows.

Logrot
Log rotation program in LMS. Rotates log when LMS is running or when the logs have reached a particular size. Optionally archives and compresses the rotated logs.

Lookup Analyzer
Utility in LMS to calculate efficiency of the DNS server.

loose source routing
IP source routing in which the IP address of the next router can be one or more routers away (multiple hops). The alternative is strict source routing, in which the next router must be adjacent (single-hop).

Low Impact Mode
Low Impact Mode enables differentiated access through policy-driven downloadable access control lists (DACLs), based on user identity information.

M

MAC Move/Replace
MAC Move allows movement of non-Cisco phones or other intermediary devices that cannot signal a link-down event.

MAC Replace is a corrective action for the security violation that is triggered when one host replaces another authenticated host.
MACUHIC  
MAC User-Host Information Collector. Tracks wired end users dynamically. It receives MAC notification traps from the switches. If the traps are from valid sources, it updates the LMS database, accordingly.

major acquisition  
Process that discovers all the End hosts and IP Phones that are connected to the devices managed by LMS.

manage Auto Smartports  
In LMS, you can use this task to enable or disable auto smartports functionality on a port.

manage servers  
Sub-step in the Server Set up workflow. LMS allows you to add servers. You can add servers, create System Identity Users, and modify the Device Management mode. See also Server Setup.

managed device  
Devices are managed in LMS when they are a part of Data Collection and are shown in Topology maps. See also Data Collection.

managed object  
Network element that is monitored by a domain manager.

Managed Sourced Interface  
Configures the source router with appropriate IP address to send or receive the IPSLA (Internet Protocol Service Level Agreement) operation packets.

Management Information Base  
See MIB.

management state  
Indicates whether a device is currently being monitored.

If a device management state is set to True, it will be discovered and monitored. If its discovery state is set to False, it will not be monitored. See also suspend and resume.

Management Station to Device  
Device diagnostic tool that helps you to diagnose the connectivity problems of un-managed or non-responding devices in the network.

Management IPAddress  
IP Address to access the device. One of the variables used to create and edit a group rule and a device search rule.

MD5  
Message digest algorithm. MD5 is a secure hashing function that converts an arbitrarily long data stream into a digest of fixed size (16 bytes).

MDC Support Utility  
Multi Domain Controller Support Utility. A diagnostic tool provided by LMS to collect the information such as database files, core client registry files, schema files, webserver configuration files, event logs, host environment information, and installation logs for debugging.

MDF Package  
Meta Data Framework Package. This package defines device types in a uniform way across LMS. This package contains new device types, new device type definitions, new device icons, and solutions to some problems in earlier MDF packages.
Medianet

- Media-aware: Detects and optimizes different media and application types to deliver the best experience.
- Endpoint-aware: Detects and configures media endpoints automatically.
- Network-aware: Detects and responds to changes in device, connection, and service availability

MIB

Database of network management information that is used and maintained by a network management protocol such as SNMP. The value of a MIB object can be changed or retrieved using SNMP commands. This is usually through a GUI network management system.

MIB objects are organized in a tree structure that includes public (standard) and private (proprietary) branches.

Minor acquisition

Minor acquisition happens on a device if there are changes in port state, VLAN information, End hosts/IP Phones connected to the device.

Minute reports and graphs

LMS generates these reports and graphs that contain statistical data for a single or a group of collectors on a minute basis.

Missed cycles

In LMS, Missed cycles is the number of polling interval cycles missed during polling.

For example, if the Polling Interval for a Poller is set as 15 minutes and the first polling cycle starts at 10:00 a.m., the next polling cycle is scheduled to start at 10:15 a.m.

If the polling cycle that started at 10.00 a.m. does not complete before 10:15 a.m., then the next polling cycle will start only at 10:30 a.m. The polling cycle missed at 10:15 is called Missed Cycle.

Monitoring dashboards

Provides summarized information about the health of the network.

Monitor Mode

Monitor Mode enables authentication without enforcing any kind of authorization.

MPIDS

Maintenance End Point ID's

MPLS interface

Interface on which MPLS traffic is enabled.
MPLS VPN

IP network infrastructure that provides private network services over a public infrastructure. It does this by using a Layer 3 backbone.

If you use MPLS VPNs in a Cisco IOS network you can deploy and administer scalable Layer 3 VPN backbone services including applications, data hosting network commerce, and telephony services to business customers.

For an MPLS VPN solution, an MPLS VPN is a set of provider edge routers that are connected by a common backbone network to supply private IP interconnectivity between two or more customer sites for a given customer.

Each VPN has a set of provisioning templates and policies and can span multiple provider administrative domains (PADs).

Multiple Authentication (Multi-auth) Mode

Multi-auth host mode allows only one client in the voice VLAN and multiple authenticated clients in the data VLAN.

Multiple Domain Authentication (Multi-domain)

Multi-domain authentication mode allows an IP Phone (Cisco or non-Cisco) and a PC to authenticate on the same switch port while it places them on appropriate voice and data VLANs.

Multiple Host Mode

Multiple host mode supports multiple hosts to authenticate on the same port in a single domain.

Multiprotocol Label Switching Virtual Private Network

See MPLS VPN.

N

NAM

A network traffic data source.

ame resolution

Process of associating a name with a network location.

name server

Server connected to a network that resolves network names into network addresses.

NAR

Definition created by ACS Administrative Users in ACS. LMS must meet the conditions in the definition to access the network.

NAS

Network Access Server. A Cisco platform that interfaces with the packets and the circuit (PSTN).

Natted LMS IP Address

Outcome of Network Address Translation (NAT) support in LMS. When the LMS server is assigned an IP Address that is within a NAT boundary, all the devices that are outside this boundary, cannot reach the LMS server using the inside address of the LMS server.

For such devices, LMS must use the correct outside address of its server for these transfers. To do this, LMS allows the configuration of this outside address of its server (called Natted LMS IP Address) for each device.
**NDG**
Collection of AAA clients such as servers and network devices. When integrating LMS with ACS Server, you should add the LMS and the devices managed in LMS under a network device group.

**NetConfig**
NetConfig allows you to make configuration changes to your network devices, whose configurations are archived in the Configuration Archive.

It also provides easy access to the configuration files for all LMS supported devices.

**Netscape Directory**

**NetShow**
Commands that represent a set of read-only commands. They can either be run from the Graphical User Interface (GUI) or from the Command Line Interface (CLI).

These are primarily, `show` commands that you can run on devices that are managed in LMS. LMS ships system-defined NetShow Command Sets. You cannot edit or delete any of these Command Sets.

**NetView**
Third party Network Management System to which LMS, icons, MIBs, and traps can be integrated.

**Network Access Restrictions**
See NAR.

**Network Access Server**
See NAS

**Network Administrator**
Predefined role in LMS. Can perform all Network Operators tasks. Can perform tasks that result in a network configuration change.

**Network Device Group**
See NDG.

**Network File System**
See NFS.

**Network Management Integration Module**
See NMIM (Also known as Integration Utility).

**Network Management System**
See NMS.

**Network Operator**
Predefined role in LMS. Can perform tasks related to network data collection. Cannot perform any task that requires write access on the network.

**New Technology File System**
See NTFS.

**NFS**
Network File System. It is a distributed file system protocol suite developed by Sun Microsystems that allows remote file access across a network.
### N-Hop view
Displays a N-hop view from a specified device. This is much faster than the regular Campus Manager Topology services and should be used to view a limited set of devices.

### NMIM
See Integration Utility.

### NMS
System responsible for managing at least part of a network. Typically, an NMS is a reasonably powerful and well-equipped computer such as an engineering workstation. NMSs communicate with agents to track network statistics and resources.

### NMSROOT
Directory where Cisco Prime LMS is installed.

### Non Installed Mode - Software Distribution
Method of software distribution used by Software Management. This process involves distributing images by copying the IOS Software Modularity images to the hard disk of the device, updating the boot commands, and rebooting the OS on the device.

You can run the Cisco IOS Software Modularity Images in this mode and so it is also called IOS Software Modularity non-install mode. It is also known as binary mode.

### non-link trunk ports
Trunk ports connected to End hosts or IP Phones. See also trunk port.

### Not Reachable
In LMS, Not Reachable status indicates that the device may be down or not reachable.

### notifications
Configurable messages sent by LMS to certain recipients. Notifications are configured by type (e-mail, syslog, SNMP trap) and group (certain events, devices, alerts, severity, status, etc.) A notification subscription consists of a notification type, a notification group, and a set of recipients.

### NTFS
Windows NT file system used to organize and keep track of files.

### NV RAM
Non-Volatile Memory where the start-up configuration in a device is stored.

### O

<table>
<thead>
<tr>
<th><strong>Object identifier</strong></th>
<th>See OID.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Object Finder portlet</strong></td>
<td>Helps you to extensively search, sort, and filter functions and to query the managed entities. You can view the device details, the job details, the End Host details, (MAC, IP address, host name, and device names, user name). You can also view the online help details.</td>
</tr>
<tr>
<td><strong>Object Grouping Service</strong></td>
<td>See OGS.</td>
</tr>
<tr>
<td><strong>Object Grouping Service Command Line Interface</strong></td>
<td>See OGSCLI.</td>
</tr>
<tr>
<td><strong>ODBC</strong></td>
<td>Generic vendor independent API for accessing relational databases.</td>
</tr>
<tr>
<td>-------------</td>
<td>---------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>OGS</strong></td>
<td>Service provided by LMS to group objects such as devices and collectors.</td>
</tr>
<tr>
<td><strong>OGSCLI</strong></td>
<td>Interface used to export groups information to a file and import groups information from a file to server.</td>
</tr>
<tr>
<td><strong>OID</strong></td>
<td>Object identifier. Uniquely identifies a device, module, interface, or power supply. Values are defined in specific MIB modules.</td>
</tr>
<tr>
<td><strong>Open Database Connectivity</strong></td>
<td>See ODBC.</td>
</tr>
<tr>
<td><strong>Open Shortest Path First Protocol</strong></td>
<td>See OSPF.</td>
</tr>
<tr>
<td><strong>operation</strong></td>
<td>Set of parameters used to measure network performance statistics. The parameters specify the type of measurement to be performed and many other parameters specific to the type of measurement being taken.</td>
</tr>
<tr>
<td><strong>OpsxmlDbEngine</strong></td>
<td>Database engine for the LMS workflow engine.</td>
</tr>
<tr>
<td><strong>OpsXMLRuntime</strong></td>
<td>Cisco Prime Assistant workflow engine.</td>
</tr>
<tr>
<td><strong>osagent</strong></td>
<td>Process that allows CORBA servers to register their objects and assists LMS in the location of objects.</td>
</tr>
<tr>
<td><strong>OSPF</strong></td>
<td>One of the Discovery protocols supported by Device Discovery. The OSPF Discovery Module uses ospfNbrTable and ospfVirtNbrTable MIB to find its neighbor's IP addresses.</td>
</tr>
<tr>
<td><strong>Out-of-Sync report</strong></td>
<td>Depicts the startup configuration, running configuration and the diff (difference) between the two configurations for selected group of devices. It summarizes the configuration details of the devices whose running and startup configurations are not synchronized.</td>
</tr>
<tr>
<td><strong>Overlay graph</strong></td>
<td>Comparative view of the latency of one or more collectors.</td>
</tr>
</tbody>
</table>

**P**

| **Package Map** | List of all device packages installed on a LMS maintained by Software Center. |
| **Package Support Updater** | See PSU. |
| **Packet Capture** | Device diagnostic tool that can be used to capture the live data from the LMS and troubleshoot the problems in the server. |
| **Packet Loss** | Measures the total number of packets lost while moving from source to target and back. |
PAK  Product Authorization Key. A key printed on the label of LMS Bundle product box. You should use this key to register your software and obtain a product license.

PAM  Pluggable Authentication Module for LMS, such as Active Directory Login and so on.

panner  Displays a compact view of the entire Network Topology view.

Parent group  Container groups and the groups that have sub-groups.

Path Analysis  Diagnostic application that traces the connectivity between two specified devices in the network, including the physical and logical paths taken by packets flowing between those points.

path echo  Measures end-to-end and hop-by-hop network response time between a Cisco device and other devices using IP. Path Echo is available only for the IP protocol.

Peer Server Account  User accounts set up on a LMS. This account can enable communication among multiple LMS. This can also authenticate processes running on a remote LMS.

Peer Server Certificate  Certificate of peer LMS. This is required to communicate with another LMS in a domain.

When you add a server using Server Setup workflow, LMS fetches the certificate information of the server you are adding, and prompts you to accept the peer certificate. See also Trust creation.

Performance Monitoring  Performance Monitoring templates allow you to configure a flow record and specify how the collected data is aggregated and presented. You can configure the following for endpoints like CUVA, Movi, Tandberg, and Webex Servers.

Performance Routing (PFR) template  PFR template is available in Template Center (Configuration > Tools > Template Center). It provides best path optimization and advanced load balancing of traffic over the WAN and to the Internet for enterprise networks with multiple paths.

Performance Tuning Tool  See PTT.

PERL  Unix based scripting language. Perl scripts ends with an extension.pl

Permanent  In LMS, Permanent status is displayed if the polled MIB variables or instances are not available in the device.

Permissions report  Report in LMS that provides information on roles, and privileges associated with the roles. It specifies the tasks that a user in a particular role can perform.

PID  Process ID. A unique number by which the operating system identifies each running program on a LMS.

PIN  Place of the device in the network layer (Edge, Core, Access, Distribution)

Ping  Device diagnostic tool used by LMS. Use the Ping tool to test whether the device is reachable. A Ping tests an ICMP echo message and its reply.
<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ping sweep</td>
<td>Basic network scanning technique used to determine which range of IP addresses map to live end hosts.</td>
</tr>
<tr>
<td>Ping Sweep Module</td>
<td>Ping Sweep Module supports both CIDR notation and subnet mask to find the range of IP Addresses.</td>
</tr>
<tr>
<td>PKCS</td>
<td>Set of standards for public-key cryptography developed by RSA Laboratories. These standards are designed for binary and ASCII data.</td>
</tr>
<tr>
<td>PKI</td>
<td>System of certificate authorities, registration authorities and other supporting agents. These authorities perform some set of certificate management, archive management, key management, and token management functions for a community of users in an application of asymmetric cryptography.</td>
</tr>
<tr>
<td>Pluggable Authentication Module</td>
<td>See PAM.</td>
</tr>
<tr>
<td>PMCOGSServer</td>
<td>Process that is required for administering Port and Module Groups in LMS.</td>
</tr>
<tr>
<td></td>
<td>You can start this process using Admin &gt; System &gt; Server Monitoring &gt; Processes. In the Process Management page, select the PMCOGSServer and click Start.</td>
</tr>
<tr>
<td>PoE</td>
<td>Power over Ethernet or technology is a system to transfer electrical power, along with data, to remote devices over standard twisted-pair cables in an Ethernet network. The terms power over Ethernet (PoE), power over LAN (PoL), and inline power are synonymous terms used to describe the powering of attached devices through Ethernet ports.</td>
</tr>
<tr>
<td>POE Port Level report</td>
<td>In LMS, this report displays information such as power consumption, power available and power remaining at the port level for devices. See also Power Policing.</td>
</tr>
<tr>
<td>PoE Port Utilization report</td>
<td>In LMS, this report displays the power utilization for each device polled for the Power Over Ethernet Port Utilization template. See also Power Policing.</td>
</tr>
<tr>
<td>PoE PSE Consumption report</td>
<td>In LMS, this report displays the power utilization for each device polled for the Power Over Ethernet PSE Consumption template. See also Power Policing.</td>
</tr>
<tr>
<td>POE report</td>
<td>Power over Ethernet (POE) is the ability of the LAN switching infrastructure to provide power over a copper Ethernet cable to an endpoint (Powered device). You can generate the POE report in LMS. See also Power Policing.</td>
</tr>
<tr>
<td>poll interval</td>
<td>Periodicity for polling the network using Device Poller. See also Device Poller.</td>
</tr>
<tr>
<td>Poller</td>
<td>Collection of devices and template MIB instances.</td>
</tr>
<tr>
<td>Poller reports</td>
<td>In LMS, these are reports created, based on the template added in a given Poller</td>
</tr>
<tr>
<td>polling frequency</td>
<td>Indicates how often CiscoView sends SNMP queries to a managed device.</td>
</tr>
<tr>
<td>Glossary Term</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Polling interval</strong></td>
<td>Frequency at which the server polls the source router to retrieve the statistics and update the database. LMS retrieves the data from source router every hour by default. The polling interval (such as 1, 5, 15, 30, or 60 minutes) is specified while creating collectors. The default polling interval is 60 minutes.</td>
</tr>
<tr>
<td><strong>Polling parameter</strong></td>
<td>Displays the edited parameters for the selected device group.</td>
</tr>
<tr>
<td><strong>Port and Module Configuration</strong></td>
<td>LMS allows you to create groups based on ports and modules for a selected set of devices or device groups. You can do this using Port and Module Group Administration.</td>
</tr>
<tr>
<td><strong>port attributes</strong></td>
<td>Information about the ports in a device such as, Type of port, Administrative Status.</td>
</tr>
<tr>
<td><strong>Portal Log Settings portlet</strong></td>
<td>Sets the level of details you will find in the log based on the settings you configure.</td>
</tr>
<tr>
<td><strong>portlets</strong></td>
<td>Enables you to organize information inside a view. These are user interface components that are managed and displayed in a view.</td>
</tr>
<tr>
<td><strong>Power over Ethernet</strong></td>
<td>See Power Policing</td>
</tr>
<tr>
<td><strong>Power Policing</strong></td>
<td>Task that allows you to configure Power and Power Policing in ports. Power Policing allows you to turn off power while generating Syslogs. This is needed if the real-time power consumption exceeds the maximum power allocation on the port. Power policing and PoE is supported only on Catalyst 3750-E and Catalyst 3560-E switches with PoE ports. This task is available only in the Port based flow of a NetConfig job.</td>
</tr>
<tr>
<td><strong>Power Sourcing Equipment</strong></td>
<td>See PSE.</td>
</tr>
<tr>
<td><strong>Preferred DCR Device Name</strong></td>
<td>You can set the name of the discovered devices in DCR as any one of the following: Sysname, DNS Resolvable Host Name</td>
</tr>
<tr>
<td><strong>Primary ACS server</strong></td>
<td>Primary server providing authentication services to LMS after integration. If the primary server is down, authentication services are provided by secondary servers, if they are configured.</td>
</tr>
<tr>
<td><strong>Primary credentials</strong></td>
<td>Primary values used to access the devices in the network. Primary credentials are stored in DCR. You can use secondary credentials to access the devices if you cannot access them using primary credentials.</td>
</tr>
<tr>
<td><strong>Privacy password</strong></td>
<td>SNMPv3 privacy password of the device in AuthPriv mode.</td>
</tr>
<tr>
<td><strong>Privacy protocol</strong></td>
<td>SNMPv3 privacy algorithm used in AuthPriv mode. Can be DES, 3DES, AES128, AES192, and AES256.</td>
</tr>
<tr>
<td><strong>Private</strong></td>
<td>LMS Portal can be a public portal or private portal. In the Private mode you can customize and configure the Views and Portlets. To select Private Portal, go to Cisco Prime LMS Portal and select <strong>Private</strong> at the top right corner.</td>
</tr>
<tr>
<td><strong>Product Authorization Key</strong></td>
<td>See <strong>PAK</strong>.</td>
</tr>
<tr>
<td><strong>Product Instance Device Mapping</strong></td>
<td>Registry that stores mapping information between devices and applications. Also, known as PIDM. Each LMS application should register the information about the devices with PIDM.</td>
</tr>
<tr>
<td><strong>Provider Edge router</strong></td>
<td>Router on the border between a VPN provider and a VPN customer that belongs to the provider</td>
</tr>
<tr>
<td><strong>Proxy server</strong></td>
<td>Intermediate server that connects the clients to the external server.</td>
</tr>
<tr>
<td><strong>PSE</strong></td>
<td>Power Sourcing Equipment refers to network devices (switches or hubs for instance), that will provide power in a Power over Ethernet (PoE) setup. See also <strong>PoE</strong>.</td>
</tr>
<tr>
<td><strong>PSIRT</strong></td>
<td>Cisco’s Product Security Incident Response Team.</td>
</tr>
<tr>
<td><strong>PSIRT Summary report</strong></td>
<td>Inventory report, generated based on the PSIRT information retrieved from Cisco.com at regular intervals. This report helps you to ascertain the security vulnerabilities that affect the devices in your network. It provides a summary of the possible security alerts based on the selected devices. It also recommends upgrade to the IOS image version that has the fix for the security vulnerability.</td>
</tr>
<tr>
<td><strong>PSU</strong></td>
<td>Central location within the LMS application to check for software updates and device updates, download and install the updates, and schedule downloading updates.</td>
</tr>
<tr>
<td><strong>PSUCLI</strong></td>
<td>CLI version of Package Support Updater.</td>
</tr>
<tr>
<td><strong>PTT</strong></td>
<td>Performance Tuning Tool. Command Line Interface (CLI) utility that enables you to apply and list various profiles available in LMS. Profiles consists of configuration files in the form of XML files whose values are based on the recommendations for various applications.</td>
</tr>
<tr>
<td><strong>Public Key Cryptography Standards</strong></td>
<td>See <strong>PKCS</strong>.</td>
</tr>
<tr>
<td><strong>Public Key Infrastructure</strong></td>
<td>See <strong>PKI</strong>.</td>
</tr>
<tr>
<td><strong>Public mode</strong></td>
<td>LMS Portal can be a Public or a Private portal. In the Public mode you can view all the portlets added by the Administrator. You can select the portal as Public to view only the portlets added into the Public portal by the administrator.</td>
</tr>
</tbody>
</table>
Q

QoS
Measure of performance for a transmission system that reflects its transmission quality and service availability.

Quality of Service
See QoS.

Quality of Service (QoS) template
QoS template is available in Template Center (Configuration > Tools > Template Center). This template provides QoS macros to switch ports upon detection of a Medianet endpoint.

Quick reports
LMS contains a set of predefined system generated reports called Quick reports.

Quick reports provide detailed information on the top 10 and bottom 10 devices polled by LMS. These are devices that have the highest or lowest utilization or availability value.

R

RA
Authority in a network that verifies the digital certificate submitted by a requestor.

RADIUS
Remote Authentication Dial-In User Service. Database for authenticating modem and ISDN connections and for tracking connection time. One of the non-ACS login modules available in the LMS.

Range operator
Operator for group rule or search rule expressions. Enables you to group the devices of the specified range of IP Addresses. You can select the range operator only for the ManagementIpAddress variable. You should enter the range of IP Addresses in the Value field.

RCP
Protocol that allows you to copy files to and from a file system residing on a remote host or server on the network. The rcp protocol uses TCP to ensure the reliable delivery of data.

RCP user
Name used by network device when it connects to LMS to run RCP.

User account must exist on UNIX systems, and should also be configured on devices as local user in the ip rcmd configuration command

Readiness report
Provides information about the VRF readiness of the devices. The Readiness report enables administrators to identify VRF Capable, VRF Supported and other devices on a network.

Reachable
In LMS, this indicates that the device is available and reachable in the network.

Reachable devices
Devices that are discovered by Device Discovery.

Really Simple Syndication
See RSS.

Real-time graph
Allows you to monitor the statistics of a collector on a real-time basis.
**refresh rate**

Indicates how often a monitoring dialog box is updated by CiscoView. The default value is 30 seconds.

**Registration Authority**

See RA.

**Regular Server**

See RS.

**Remote Authentication Dial-In User Service**

See RADIUS.

**Remote Copy Protocol**

See RCP.

**Remote Monitoring**

See RMON.

**Remote NMS**

Network Management System on the remote LMS. See also NMS.

**Remote upgrade**

Process of installing a newer version of Cisco Prime software on a different machine and restoring the data backed up from the older version to the newer version.

**report archives**

Report is archived when a scheduled report job has completed successfully and stored in archive for future reference.

**report granularity**

Level of detail in a report that you want to view from the archived statistics. The various levels available are Minute, Hourly, Daily, Weekly, and Monthly.

**report job**

Jobs for which reports are scheduled to run at the specified date and time.

**Report Job Browser**

In LMS, Report Job Browser allows you to view the list of report jobs scheduled to generate reports. From the Report Job Browser, you can perform report job management activities such as viewing the details of a report job, deleting a report job, suspending a report job, resuming a report job and viewing a report.

System jobs are not shown in the Report Job Browser.

**Reports**

LMS offers comprehensive reporting on the data collected by polling the device and presents this data using tables and graphs. These reports help network administrators analyze the utilization and availability of devices connected to the network. Reports also provide the historical trending information of a device.

**Request/Response Unit**

See RU.

**restore data**

See database restore.

**resume**

Setting a device management state to True so that LMS will monitor the device. This is normally done from the Detailed Device view. See also suspend.

**retry**

Number of times CiscoView will send an SNMP request to a managed device before the request times out.
System-defined groups

Default grouping of devices. This is a read only group. You cannot create new groups under system-defined groups. The system-defined device groups available in LMS are All Devices, Normal devices, Pre-deployed, Previous selection and Saved device list.

RMON

Remote monitoring. MIB agent specification described in RFC 1271 that defines functions for remote monitoring networked devices. The RMON specification provides monitoring, problem detection, and reporting capabilities.

Download the CiscoView Mini-RMON Manager device package to enable RMON functionality within CiscoView.

Rogue MAC

MAC Addresses that are not authorized to exist in your network.

root device

Device from which the N-Hop portlet starts drawing the Topology map.

round-trip time

See RTT.

Round-trip time monitor management information base

See RTTMON MIB.

route

Path through an internetwork between a specific source and target.

Route Processor

See RP.

router

Network layer device that uses one or more metrics to determine the optimal path along which network traffic should be forwarded. Routers forward packets from one network to another, based on network layer information.

Route Distinguisher

Number that identifies VPNs in the provider’s (MPLS) network and it supports overlapping address in a network.

Route distinguisher is prefixed to private IPv4 addresses to make the IPv4 addresses globally unique. The value is used by the edge router to identify the VPNs to which packets belongs to.

For example: A PE router can distinguish between the IP address 10.10.10.1 of one customer from the 10.10.10.1 of another customer, the network administrator must add a unique route distinguisher to each.

Routing Control Processor

See RCP.

RP

Route Processor. Processor module in the Cisco 7000 series routers that contains the CPU, system software, and most of the memory components that are used in the router. Sometimes called a supervisory processor.

RS

Single Sign-On Slave server using the authentication services from the Master. The regular server should be configured in the same domain as the Master server.

rsh

Remote Shell Protocol. Protocol that allows you to run commands on a remote system without logging into the system.
RSS
Really Simple Syndication. XML-based format used to distribute Web content (such as news headlines). By using RSS, web content publishers can easily create and disseminate current news headlines and URLs.

RSVP template
Resource Reservation Protocol (RSVP) signals the QoS needs of an application's traffic along the devices, in the end-to-end path through the network.

RTT
Time required for a network packet to travel from the source to the destination and back. RTT includes the time required for the destination to process the message from the source and generate a reply. The latency measurements taken by LMS and SA Agent are round-trip time latency measurements.

RTTMON MIB
Proprietary MIB created by Cisco to obtain and store round-trip time statistics. The MIB is implemented by the Cisco IOS software in the source router.

LMS obtains the round-trip time statistics from this MIB. This MIB has been extended to monitor network performance statistics in addition to round-trip time statistics.

RU
Request and response messages exchanged between NAUs in an SNA network.

S
SAA
Feature of Cisco IOS software that allows you to measure and monitor network performance between a Cisco router and a remote device.

SA Agent Responder
Component embedded in a target Cisco router running version 12.1 or later of the Cisco IOS software. It responds to SA Agent request packets from a source router running the SA Agent software.

The Responder can listen on any user-defined port for UDP and TCP protocols. The SA Agent Responder is required only for specific collector types, such as Enhanced UDP for monitoring jitter in Voice-over-IP networks.

Sample Interval
Frequency with which the source device polls the target device to retrieve the statistics based on the IPSLA operations configured by you. LMS retrieves the statistics from the target device every 60 seconds, by default.

scheduled report
See job.

SCP user
Name used by network device when it connects to LMS to run SCP.

The username you have entered here is used for authorization while the device transfers software images, using SCP protocol.

search rule
Consists of one or more rule expressions combined by logical operators. Used to filter and display only the devices that satisfy the rule conditions, in the device selector.

Secondary ACS Server
ACS server that provides authentication services to LMS only when the primary ACS server is down. You should configure the hostname or IP Address, and the port number on the LMS.
secondary credentials  
Credentials that you can use as a fallback if you cannot access the network devices using primary credentials. Secondary credentials comprise a username, a password, and a console-enabled password for the devices.

secret key  
Text string (usually passwords) used in a multi-server domain to maintain the confidentiality and provide authenticity among the servers.

Secure Hash Algorithm  
See SHA.

Secure Shell  
See SSH.

Secure Socket Layer  
See SSL.

security certificate  
Similar to digital ID cards. They prove the identity of the server to clients. Certificates are issued by Certificate Authorities (CAs) such as VeriSign or Thawte.

Security mode  
In Identity, you can choose the level of security you wish to implement in the selected switches.

seed device  
Starting point for Device Discovery. See also Device Discovery.

seed file  
A text file that lists top-level network devices (for example, hosts, routers, and switches) by name or IP address, and the read community strings of the devices. LMS can use seed files to initiate device discovery.

selective backup  
Saving only the selected data and configuration files to maintain a safe copy. See also database backup.

Self-Signed certificate  
Security certificates created on the LMS that enable SSL communication between the client browser and management server. Self-signed certificates are valid for five years from the date of creation.

When the certificate expires, the browser prompts you to install the certificate again from the server where you have installed LMS.

server  
Node or software program that provides services to clients.

Server Setup  
One of the LMS workflows. It helps you to simplify the deployment and setting up of single or multiple LMS servers.

Service Assurance Agent  
See SAA.

Setup Center  
Centralized area that displays the LMS System configurations and allows you to configure the necessary server settings, immediately after installing LMS Software.

SHA  
Algorithm that accepts a message of less than 264 bits in length and produces a 160-bit message digest.

Show Map  
Shows the connectivity details of the devices on which VRF is to be configured. Using Show Map, you can view the connectivity details of up to 30 devices.
| **Glossary** |
|-----------------|--------------------------------------------------|
| **Simple Mail Transfer Protocol** | See SMTP. |
| **Simple Network Management Protocol** | See SNMP. |
| **Single Host Mode** | Single Host mode allows only one user to authenticate per port. |
| **Single Sign On** | See SSO. |
| **SIU** | Communication between multiple LMS is enabled by a trust model addressed by certificates and shared secrets. Use the System Identity setup to create a trust user on Slave servers to facilitate communication in Multi-server scenarios. This trust user is called System Identity User. The System Identity User is also used for inter-process communication. See also Trust creation. |
| **Smart Call Home** | Smart Call Home is a new, secure connected service that is currently available on the Cisco Catalyst 6500 devices. It offers proactive diagnostics and real-time alerts on select Cisco devices and provides higher network availability and increased operational efficiency. |
| **SmartCase** | Lets you access Cisco.com from LMS to open a Cisco.com case or to query and update an existing case. It allows you to submit, review, and update problems or questions about Cisco products. |
| **Smart Install** | Smart Install (SI) is a plug-and-play configuration and image management feature that provides zero-touch deployment for new switches. |
| **Smart Install Groups** | You must define a minimum of one Smart Install group to configure an SI director. |
| **Smartports** | In LMS, you can use this task to apply smartports on a port by selecting the predefined smartports macros. |
| **SMTP** | Simple Mail Transfer Protocol. Internet protocol providing e-mail services. |
| **SNMP** | Simple Network Management Protocol. It is used almost exclusively in TCP/IP networks. SNMP allows you to monitor and control network devices, and to manage configurations, statistics collection, performance, and security. CiscoView supports SNMP versions 1, 2, and 3. |
| **SNMP agent** | Simple Network Management Protocol agent. Resides in the source router and is provided as part of Cisco IOS software. The SNMP agent receives requests from the SNMP server to perform all LMS-related functions. |
| **SNMP community string** | Text strings that act as passwords to authenticate messages sent between the network management station and devices containing an SNMP agent. Community strings allow you to limit access to network devices. |
| **SNMP MAC notification** | MAC address notification enables you to track users on a network. Whenever the switch learns about or removes a MAC address, an SNMP notification can be generated and sent. |
SNMP retries  Number of attempts made to query the device.
SNMP Set  Device diagnostic tool that allows you to set an SNMP object or multiple objects on a device for controlling the device.
SNMP timeout  Time period after which the SNMP query times out.
SNMP trace  Displays information on SNMP requests sent by CiscoView to managed devices.
SNMP Traps Forwarding  Forwards SNMP traps from devices in the LMS inventory. LMS will forward the raw trap in the format in which it was received from the device. All traps are forwarded in V1 (SNMP Version) format.
SNMP Traps Receiving  Receives SNMP traps on port 162 (or, if port 162 is occupied, port 9000).
SNMP walk  Device diagnostic tool that allows you to trace the MIB tree of a device starting from a given OID for troubleshooting or to gather information about a certain device.
SNMPv3  Version 3 of SNMP.
Soft Appliance  LMS is available for customers on a Soft Appliance platform. The soft appliance is built on Cisco standard CARS platform Version 2.0 with Redhat 5.4 (64 bit) as the underlying Soft Appliance distribution.
Software Center  Helps you to check for software and device support updates, download them to their server file system along with the related dependent packages, and install the device updates. Also known as PSU.
SoftWare Image Management  See SWIM.
Software Management CLI  Command-line Interface of LMS. You can use this tool to invoke the Software Management features from the command-line.
source device  Devices which support IPSLA and which performs the operations by generating packets at the predefined intervals and storing the measured values.
source router  Originating router or switch running IOS from which LMS measures network performance. The source router or switch must be running a version of Cisco IOS software version that supports IPSLA.
source-route bridging  See SRB.
SQL  International standard language to define and access relational databases.
SRB  Method of bridging originated by IBM and popular in Token Ring networks. In an SRB network, the entire route to a destination is predetermined, in real time, before the data is transmitted to its destination.
SRE Operation

In LMS, you can use the SRE Operation task to perform the following operations in the service modules of SRE supported devices:

- Install application in service modules
- Uninstall application from service modules
- Understand:
  - Status of the service module
  - Application that is running on the module
  - Status of the current installation in the service module
  - Status of uninstallation in the service module
- Stop the installation on a set of service modules in a SRE device
- Reset service modules in a SRE device
- Shutdown the set of service modules in a SRE device

SSCP

Focal point within an SNA network to manage network configuration, coordinate network operator and problem determination requests, and provide directory services and other session services for network end users.

SSCP-PU session

Session used by SNA to allow an SSCP to manage the resources of a node through the PU. SSCPs can send requests to, and receive replies from, individual nodes to control the network configuration.

SSH

Protocol that provides a secure remote connection to devices. There are currently two versions of SSH available: SSH Version 1 and SSH Version 2. Only SSH Version 1 is implemented in the Cisco IOS software.

SSL

Encryption technology for the Web used to provide secure transactions. LMS uses SSL to provide secure access between the client browser and the management server.

SSO

Single Sign On enables you to use your browser session to transparently navigate to multiple LMS without authenticating to each of them.

SSO mode

The SSO authentication server is called the Master, and the SSO regular server is called the Slave. Authentication always takes place from the SSO Master server (Authentication Server-AS).

Authorization happens at the respective servers. The LMS can also be configured to be in the Standalone mode (Normal mode, without SSO). See also SSO.

SSP

Protocol specified in the DLSw standard, used by routers establish DLSw connections, locate resources, forward data, and handle flow control and error recovery. See also DLSw.

Stack Group

This is a custom group which is used to set up the image and configuration file for all client switches that match stack number for switches in a stack.

stale groups

Groups that belongs to users groups who are removed from LMS.
<table>
<thead>
<tr>
<th><strong>Standby Switch</strong></th>
<th>After converting two VSS-enabled Standalone Switches into a Virtual Switching System, one switch becomes the Standby Switch and other the Active Switch.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>static group</strong></td>
<td>Group whose membership is refreshed only when you explicitly request it. Between re-evaluations, the Group Server stores the membership list and group definition of the static group. Whenever you view a Static group, you can see the membership list that the ASA created the last time the group rule was evaluated.</td>
</tr>
<tr>
<td><strong>static route</strong></td>
<td>Explicitly configured route entered into the routing table. Static routes take precedence over routes chosen by dynamic routing protocols.</td>
</tr>
<tr>
<td><strong>Structured Query Language</strong></td>
<td>See SQL.</td>
</tr>
<tr>
<td><strong>Sub Interface</strong></td>
<td>Logical interfaces derived from a physical interface.</td>
</tr>
<tr>
<td><strong>subnet based acquisition</strong></td>
<td>Runs only on those subnets that are configured in LMS.</td>
</tr>
<tr>
<td><strong>subnet groups</strong></td>
<td>System defined device group in device selector that contains the devices managed in LMS. These subnet based groups help you work on smaller subsets of devices that are logically grouped.</td>
</tr>
<tr>
<td><strong>subscription</strong></td>
<td>See notifications.</td>
</tr>
<tr>
<td><strong>Super Admin</strong></td>
<td>User in LMS created after the LMS is integrated. Cperform all LMS operations including the administration and approval tasks. By default, this role has full privileges.</td>
</tr>
<tr>
<td><strong>suspend</strong></td>
<td>To set a device’s management state to False so that LMS will not monitor the device. This is normally done from the Detailed Device View. See also resume.</td>
</tr>
<tr>
<td><strong>SWIM</strong></td>
<td>Software Image Management or Software Management in LMS automates the steps associated with upgrade planning, scheduling, downloading software images, and monitoring your network. It provides tools that make it easier to store backup copies of all Cisco software images running on network devices. It also helps to store any additional software images if required, and to plan and run software image upgrades to multiple devices on the network at the same time.</td>
</tr>
<tr>
<td><strong>Switch Check</strong></td>
<td>You can select this while running the End Host Down/IP Phone Down workflow. If you select this option, LMS will check the reachability status for the selected device to which the End Host is connected. Otherwise, it will check the reachability status for the Cisco Call Manager (CCM) to which the IP Phone is connected. See also End Host/IP Phone Down.</td>
</tr>
<tr>
<td><strong>Switch-to-Switch Protocol</strong></td>
<td>See SSP.</td>
</tr>
<tr>
<td>Term</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Syslog Analyzer/Collector</td>
<td>Allows you to centrally log and track syslog messages (error, exception, information etc.) sent by devices in the network. You can use the logged message data to analyze network device performance. You can also customize this application to store and produce important information.</td>
</tr>
<tr>
<td>Syslog messages</td>
<td>Messages that originate from a device in response to some activity that affects it. The devices that are connected to the LMS server, are configured to send Syslog messages to the LMS Syslog server whenever there are changes. The LMS server receives these messages either directly from the devices in the network or through a Remote Syslog Collector installed in the network. You can use these logged Syslog messages to analyze network device performance.</td>
</tr>
<tr>
<td>Syslog Receiver Group</td>
<td>Group of hosts that receives Syslog messages when any TrendWatch or Threshold violation occurs in LMS. LMS allows you to create Syslog Receiver Groups using the Syslog Receiver Groups option.</td>
</tr>
<tr>
<td>syslogConf.pl Utility</td>
<td>Perl Script CLI utility. You can use this to Change Syslog Analyzer Port, Change Syslog Collector Port, Configure Remote Syslog Collector (RSAC) Address and Port in LMS server, and Change Syslog File Location. You can perform all these tasks on a LMS server by running the syslogConf.pl script from the command prompt.</td>
</tr>
<tr>
<td>System Administrator</td>
<td>Predefined role in LMS. Can perform all LMS system administration tasks.</td>
</tr>
<tr>
<td>System-defined group</td>
<td>Top-level container for standard groups that are accessible to and used by most LMS users. It is available by default.</td>
</tr>
<tr>
<td>System Identity User</td>
<td>See SIU.</td>
</tr>
<tr>
<td>System Services Control Point</td>
<td>See SSCP.</td>
</tr>
<tr>
<td>System status</td>
<td>Details about LMS processes—Device Discovery, Data Collection and User Tracking Acquisition.</td>
</tr>
<tr>
<td>System view</td>
<td>View that contains all system related portlets, such as Job Information Status portlet, DCR and AAA, Log Space Usage, and Process Status.</td>
</tr>
<tr>
<td>System-defined template</td>
<td>In LMS, System-defined MIB templates provide most of the common network parameters that you need to monitor a device connected to the network. These templates cannot be deleted or modified.</td>
</tr>
</tbody>
</table>
TACACS Authentication protocol, developed by the DDN community, that provides remote access authentication and related services, such as event logging.

User passwords are administered in a central database instead of in individual routers, providing an easily scalable network security solution. See also TACACS+ in the Cisco Systems Terms and Acronyms section.

TACACS+ Terminal Access Controller Access Control System Plus. Proprietary Cisco enhancement to Terminal Access Controller Access Control System (TACACS). Provides additional support for authentication, authorization, and accounting. See also TACACS in main glossary.

target device Device to which the packets are sent by the IPSLA source devices. Target devices are the destination devices for which you want to gather network performance statistics.

The target devices can be any IP-addressable device or a Cisco device running the IPSLA Responder on which the source router performs IPSLA operations.

TCP Connection-oriented transport layer protocol that provides reliable full-duplex data transmission. TCP is part of the TCP/IP protocol stack. See also TCP/IP.

TCP/IP Common name for the suite of protocols developed by the U.S. DoD in the 1970s to support the construction of worldwide internetworks. TCP and IP are the two best-known protocols in the suite. See also TCP and IP.

TDR Time Domain Reflectometry (TDR) is used to detect faults in a cable. TDR checks and locates open circuits, short circuits, sharp bends, crimps, kinks, impedance mismatches, and other such defects.

Template In LMS, this is a collection of MIB variables logically grouped by the user or the system to monitor the utilization and availability levels of a device (such as CPU, memory, interface).

Template Center Template Center in LMS provides you with a list of both system-defined templates and user-defined templates. These templates contain configuration commands that can be deployed on the devices in your network. These templates are deployed using Deploy Template jobs in LMS.

You can modify the system-defined templates and save them as user-defined templates. You can also import templates from a client machine and these templates are stored as user-defined templates in LMS.

Template management Allows you to create a user-defined template, modify the configuration of a user-defined template, export and import a user-defined template, delete a user-defined template, and so on.
| **Terminal Access Controller Access Control System** | See TACACS. |
| **Tertiary ACS Server** | ACS server that provides authentication services to LMS only when both the primary ACS server and the secondary ACS server are down. You should configure the hostname or IP Address, and the port number in LMS. |
| **TFTP** | Simplified version of FTP that allows files to be transferred from one computer to another over a network, usually without the use of client authentication. For example, username and password. |
| **Threshold** | In LMS, this is an optimal value for a MIB variable set by the user or the system. |
| **Threshold setup** | Threshold rule can be set for only one MIB variable at a time and you can set many thresholds for each MIB variable. You can set threshold rules for all the MIB variables on a device selected for polling. |
| **Threshold Violation reports** | In LMS, these are reports created based on the threshold configured for the MIB variable. |
| **Time Domain Reflectometry reports** | Detects faults in a cable. LMS supports TDR Cable Diagnostic Test and generates a report listing the results of the test on Cisco Catalyst 6000 switches. |
| **timeout** | Event that occurs when one network device expects to hear from another network device within a specified period of time, but does not. Typically, a timeout results in a retransmission of information, or the cancellation of the session between the two devices. In CiscoView, this is the length of time that elapses before an SNMP request sent by the application to a managed device times out. |
| **TOC** | Table of Contents. |
| **Tomcat** | Java servlet engine used on Windows and Solaris systems that hosts applications on the LMS desktop. |
| **Topology and Neighbor information** | LMS features that let you manage, view, and monitor the physical and logical services on your network. You can also get information on neighbor devices. |
| **Topology filters** | Filters devices, links, and networking services. Locates these items on the Network Topology Views. |
| **Topology groups** | Customized views, of the network in which devices are grouped according to various criteria. A view may be considered as a group of devices or device elements. |
| **Topology Services** | Messages about the status of Topology Services that appear on the left side of the status bar. These messages typically are displayed at the start and end of a task that is performed within Topology Services. |
Traceroute

Device diagnostic tool used to detect routing errors between the management station and the target device. Helps you understand why ping fails or why applications time out.

Transient

In LMS, this status is displayed if the device is down or the SNMP credentials are incorrect.

Transmission Control Protocol

See TCP.

Transmission Control Protocol/Internet Protocol

See TCP/IP.

trap

Message sent by an SNMP agent to an NMS, console, or terminal indicating that a significant event has occurred. This could be a specifically defined condition or a threshold that has been reached.

Trap listener

LMS server port that listens to SNMP MAC Notification traps sent from devices.

Trap Receiver group

Group of hosts that receives specified trap notifications, when any TrendWatch or Threshold violation occurs in LMS. LMS allows you to create SNMP Trap Receiver Groups using the Trap Receiver Groups option.

TrendWatch

Allows you to continuously monitor a value over time, sampling the value at periodic intervals to view the trends.

TrendWatch report

LMS report that is created based on the TrendWatch configured for the MIB variable. You can create, edit, copy, and view these reports for specific TrendWatch MIB variables.

Trivial File Transfer Protocol

See TFTP.

trunk port

Switch port that is connected to another Layer 2 device (such as a switch or bridge). This is by default, a member of all VLANs that exist on the switch and carry traffic for all VLANs, among the switches.

Trust creation

Creation of trust is required to enable communication between LMS part of a multi server set up. Communication among multiple LMS is enabled by a trust model addressed by Certificates and shared secrets. See also Peer Server Certificate and System Identity User.

TrustStore

Also known as KeyStore. The location where Cisco Prime maintains the list of certificates that it trusts.
### Glossary

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>UDF</strong></td>
<td>Stores additional information about a device in DCR. DCR supports a maximum of ten UDFs. By default, the DCR Administration user interface provides four UDFs.</td>
</tr>
<tr>
<td><strong>UDP</strong></td>
<td>Connectionless transport layer protocol in the TCP/IP protocol stack. UDP is a simple protocol that exchanges datagrams without acknowledgments or guaranteed delivery, requiring that error processing and retransmission be handled by other protocols.</td>
</tr>
<tr>
<td><strong>UDP jitter</strong></td>
<td>User Datagram Protocol jitter. It allows you to measure round-trip delay, one-way delay, one-way jitter, one-way packet loss, and connectivity in networks that carry UDP traffic.</td>
</tr>
<tr>
<td><strong>UDM</strong></td>
<td>Unified Device Manager (UDM) provides centralized device management using a centralized policy configuration. You have to configure a single policy to manage the devices. UDM identifies managed devices after verifying the configured policy and the license count.</td>
</tr>
<tr>
<td><strong>UE</strong></td>
<td>User Experience.</td>
</tr>
<tr>
<td><strong>UI</strong></td>
<td>User Interface.</td>
</tr>
<tr>
<td><strong>unacknowledging discrepancy</strong></td>
<td>Returns an acknowledged discrepancy into the Discrepancies report. See also acknowledging discrepancy.</td>
</tr>
<tr>
<td><strong>Uniform Resource Locator</strong></td>
<td>See URL.</td>
</tr>
<tr>
<td><strong>Uniform Resource Name</strong></td>
<td>See URN.</td>
</tr>
<tr>
<td><strong>unreachable devices</strong></td>
<td>Devices that are not reachable by LMS Device Discovery.</td>
</tr>
<tr>
<td><strong>UPN</strong></td>
<td>User Principal Name. It is composed of two parts, User login and UPN suffix. You should enter the User login name and UPN suffix for a UPN-based authentication to MS Active Directory Server.</td>
</tr>
<tr>
<td><strong>URL</strong></td>
<td>Type of formatted identifier that describes the access method and the location of an information resource object on the Internet.</td>
</tr>
<tr>
<td><strong>URN</strong></td>
<td>1. Uniform Resource Name. An Internet addressing scheme. &lt;br&gt;2. Refers to the URL of a AUS Managed Device in Cisco Prime.</td>
</tr>
<tr>
<td><strong>User Datagram Protocol</strong></td>
<td>See UDP.</td>
</tr>
<tr>
<td><strong>User Datagram Protocol jitter</strong></td>
<td>See UDP jitter.</td>
</tr>
<tr>
<td><strong>User-defined fields</strong></td>
<td>See UDF.</td>
</tr>
</tbody>
</table>
User-defined group

Top-level container where individual application users can create their own groups. Typically, the groups under User Defined Groups are used and accessible to the user who created the group, and perhaps a small group of additional users. Groups created by you, based on the device attributes in DCR

User Principal Name

See UPN.

User Tracking

Allows you to track End Hosts and IP Phones connected to the network.

User Tracking utility

Allows you to search for users or hosts discovered by User Tracking application. Comprises a server-side component and a client utility.

User-defined template

LMS allows you to create your own templates. You can do this by grouping new MIB variables or by leveraging MIB variables from an existing System-defined template to suit your requirements. These templates are called user-defined templates.

You can add or delete MIB variables in a user-defined template.

UT major acquisition

See major acquisition.

utilization

Percentage of a particular resource, such as CPU or memory, currently in use by a device, card, or port, as indicated by a CiscoView monitoring dialog box.

UTLite

Process that collects user names from Primary Domain Controllers, Active Directory, and Novell servers. It runs only on Windows clients.

UTManager

Process that receives information from MACUHIC about newly added end hosts in the network. This information is completed using updates from DHCP or UTLite or from both. See also MACUHIC.

Video Conferencing

Video Conferencing template is available in Template Center (Configuration > Tools > Template Center). You can configure different video endpoints for video conferences. You can configure three types of video profiles:

- Homogeneous conferences (video switching)
- Heterogeneous conferences (video mixing)
- Guaranteed audio conferences (best-effort video)

Video Transcoding

Video Transcoding template is available in Template Center (Configuration > Tools > Template Center). Video can be converted from one format to another. You can configure video transcoding when the bit rate, frame rate, resolution, or codec is different between two endpoints.

Virtual Local Area Network

See VLAN.

Virtual Routing and Forwarding

See VRF-Lite.
**Virtual Switching System**

Technology that combines two standalone distribution switches found in the local distribution layer into a single management point.

The Virtual Switching System functions and appears as a single switch to the wiring closet and the core layer. You can also create Virtual Switching Systems with a pair of standalone switches available in the core layer.

**Virtual Switching System Configuration**

Process of converting two VSS-enabled Standalone distribution switches into a Virtual Switching System. Virtual Switching System Configuration Tool available in LMS is used to convert the two VSS-enabled Standalone Switches into a Virtual Switching System.

**Virtual Switching System Configuration Tool**

The Virtual Switching technology is implemented in LMS by providing a Virtual Switching System Configuration Tool. This GUI based conversion tool allows you to select two compatible standalone switches and guides you to convert those standalone switches into one Virtual Switching System.

**Virtual Switching System Mode**

When two Standby switches are converted to a Virtual Switching System, they are considered to be in Virtual Switching System Mode.

**virtualization**

Allows you to run multiple virtual machines with same or different Operating Systems independently on the same physical machine.

**VLAN**

Virtual Local Area Network. This is a group of devices on one or more LANs that are configured (using management software) so that they can communicate as if they were attached to the same wire. This is although they are located on a number of different LAN segments.

VLANs are based on logical instead of physical connection. This makes them extremely flexible.

**VMware**

Virtualization system on which Cisco Prime LMS can be installed and run.

**voice trace**

Specifies Voice over IP (VoIP) traffic trace between telephone number.

**VoIP Call Setup Post Dial Delay**

Measures network response time for setting up a VoIP call.

**VoIP Gatekeeper Registration Delay**

Allows you to measure the average, median, or aggregated network response time of registration attempts from a VoIP gateway to a VoIP gatekeeper device.

**VoIP RTP**

Real-Time Transport Protocol (RTP)-based Voice over IP (VoIP) operation allows you to set up and schedule a test call and use Voice gateway digital signal processors (DSPs) to gather network performance-related statistics for the call.

**VRF**

VPN routing or forwarding instance. A VRF includes the routing information that defines a VPN site that is attached to a PE router.

This can be an IP routing table, a derived forwarding table, a set of interfaces that use the forwarding table, and a set of routing protocols that determine what goes into the forwarding table.

**VRF Based report**

Displays the VRF details specific to the VRFs selected while generating the report. See also VRF-Lite.
VRF Capable Devices

Represents the devices with necessary hardware support. To configure VRF on these devices, you need to update the software of the device.

VRF Collection

Fetches the complete information about the VRFs from the network. See also VRF-Lite.

VRF-Lite

One of the simplest form of implementing virtualization technology in an Enterprise network. A Virtual Routing and Forwarding is defined as VPN routing/forwarding instance. A VRF consists of an IP Routing table, a derived forwarding table, a set of interfaces that use the forwarding table and set of routing protocols that determine what goes into the forwarding table.

VRF Supported Devices

Represents the devices with necessary hardware and software support to configure VRF.

VSS Configuration

See Virtual Switching System Configuration.

VSS Mode

See Virtual Switching System Mode.

W

WLSE UHIC

Process that updates the LMS database with the information on wireless clients. WLSE UHIC polls the Wireless LAN Solution Engines (WLSE) periodically and receives details on the changes occurring in the wireless host associations.

Work Centers

Work Centers in LMS 4.2 provides complete lifecycle management of TrustSec, EnergyWise, Auto Smartports, and Smart Install from Day 1 to Day N operations in a workflow-oriented approach.

This includes readiness assessment, configuration, monitoring, and reporting capabilities.

workflows

LMS workflows help you to deploy and manage the LMS and troubleshoot your network. The workflows take you through the different steps required to achieve these tasks.

You can perform the steps required to set up a multi-server set up, in a single flow. Also, you can generate device troubleshooting reports that use features from the different installed applications, without having to go to each of them to run the tasks.

See also End Host/IP Phone Down, Device Troubleshooting and Server Setup.
<table>
<thead>
<tr>
<th><strong>X</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>XML</strong></td>
</tr>
<tr>
<td><strong>XSL</strong></td>
</tr>
</tbody>
</table>