



GLOSSARY

A

- AAA** Authentication, authorization, and accounting. Usually pronounced as triple-A.
- AAA client** Devices added to ACS Server through which the AAA service access is attempted. The CiscoWorks Server and devices managed in CiscoWorks should be added as AAA clients in ACS.
- AAA mode** Authentication Authorization and Accounting mode. By default, CiscoWorks Server authentication (CiscoWorks Local) is used to authenticate users and authorize them to access CiscoWorks applications.
- CiscoWorks Server can be integrated with Cisco Secure Access Control Server (ACS) to provide improved access control using authentication, authorization, and accounting. See also [ACS](#).
- Access Control Server** See [ACS](#).
- access port** Switch port that is either connected or not connected to a Layer 2 device, or is connected to a non-Layer 2 device (such as a router). In Campus Manager, this is a switch port that is connected to an End host or IP Phone.
- acknowledging discrepancy** Removing a discrepancy from the Unacknowledged Discrepancies report.
- acknowledging discrepancy** Process that discovers End Hosts and IP Phones connected in the network.
- ACS** Cisco Secure Access Control Server (ACS). Cisco Secure ACS provides authentication, authorization, and accounting services to network devices that function as AAA clients. In ACS mode, you can create custom roles to suit your business workflow. See also [AAA mode](#).
- Active Directory** Microsoft Active Directory. A pluggable authentication module that provides AAA services to CiscoWorks Server when integrated.
- Active end host** End hosts that are currently connected to the network.
- Active State** In CiscoWorks HUM, Active State indicates that HUM is currently polling for the device MIB instance.
- Active Switch** After converting two VSS-enabled Standalone Switches into a Virtual Switching System, one switch becomes the Active Switch and other the Standby Switch.

activity trace	Lists activity on the server running CiscoView (for example, launching the Ethernet Statistics dialog box).
adapter	Program that links a DFM domain manager to its environment. DFM 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. CiscoWorks Assistant 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 Target Device	External target devices that are added to IPM.
aggregate device	Device that contains more than one intelligent management agent, each with its own IP address. CiscoWorks 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 DFM that indicates an abnormal condition in the network. An alert consists of related events. A finite set of alerts are displayed on the DFM Alerts and Activities display.
Alias Devices	Devices in Resource Manager Essentials (RME) with different hostnames or IP addresses. When a new device is added to RME, it may already exist in RME, with another hostname or IP address. This device will be in the Alias state.
Allocate devices	Sub-step in the Server Set up workflow. This helps you to allocate devices to be managed by the applications installed in the CiscoWorks Server. See also Server Setup .
ANIServer	Process that performs Data Collection. See also Data Collection .
Apache	Web server used in CiscoWorks Server on both UNIX and Windows systems. This hosts the base CiscoWorks 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 Registration	<ol style="list-style-type: none">1. Process of registering the CiscoWorks applications with CiscoWorks Home Page on the local or remote servers.2. Process of moving the information from CiscoWorks Server to ACS Server. Only when the applications are registered, can CiscoWorks use the AAA services from the integrated ACS server for user authentication and authorization.
Application Service Adapter	See ASA .

Application specific groups	Groups based on device types or states specific to CiscoWorks applications. The application-specific groups appear in the device selector of the respective applications.
Application View	Views that are displayed in CiscoWorks LMS Portal. These views are based on the installed applications. For instance, CS View (Common Services View).
Approver	Predefined role in CiscoWorks applications. Users assigned with this role can approve all CiscoWorks tasks.
Archive Management	<p>Major application in Resource Manager Essentials (RME). It maintains an active archive of the configuration of devices managed by RME.</p> <p>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.</p>
archived report	A report is archived when a scheduled report job is completed successfully.
ARP	<p>One of the Discovery protocols supported by Common Services Device Discovery. This Discovery module depends on the Routing Table Discovery module.</p> <p>See also ARP in Cisco's Internetworking Terms and Acronyms.</p>
AS	Single Sign-On Master server providing authentication services to other CiscoWorks Server configured in the same domain.
ASA	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. For Common Services, Device and Credential Repository (DCR) acts as the ASA.
ASCII	American Standard Code for Information Interchange. 8-bit code for character representation.
Assertion error	<p>Sybase Assertion error that occurs when the Common Services databases do not run.</p> <p>This error appears if any anti-virus software or third-party backup software is used in the CiscoWorks Server.</p>
Audit Trail	Module of Resource Manager Essentials (RME). It tracks and reports changes that the RME administrator makes on the RME server.
AUS	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.
Auth password	SNMPv3 authentication password used to operate the devices in AuthNoPriv and AuthPriv modes.

Auth protocol	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.
Authentication mode	Mode selected to authenticate the CiscoWorks users when logging into the CiscoWorks Server. Either the ACS server or the CiscoWorks Server can provide the authentication services, based on the AAA mode set up in CiscoWorks.
Authentication Server	See ACS .
AuthNoPriv	One of the security levels within SNMPv3 providing message integrity and authentication security features.
Authorization mode	Mode selected to authorize the user after authentication. The Authorization services can be provided by the ACS or the CiscoWorks Server.
AuthPriv	One of the security levels within SNMPv3 providing message integrity, authentication, and data encryption features.
Auto mode	Mode in which devices are managed in Campus Manager. In this mode, all devices in DCR are automatically managed in Campus Manager. Filter policies can be set to manage certain devices/set of devices.
Auto Update Server	See AUS .
Auto Update Server	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.
Availability	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.

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. You can use Baseline templates through Resource Manager Essentials (RME).

Best Practice Deviation	Best practices that are recommended by Cisco but not implemented in the network.
BGP	<p>One of the discovery protocols supported by Common Services Device Discovery.</p> <p>This discovery module uses Border Gateway Peer Table to identify its BGP peer.</p> <p>See also BGP in Cisco's Internetworking Terms and Acronyms.</p>
Border Gateway Protocol	See BGP.
broker	DFM software that communicates between a domain manager and its clients.
Browser server security	<p>A security feature that Common Services provides for secure access between the client browser and the management server.</p> <p>Common Services uses SSL to provide browser server security.</p>
Bug Toolkit	Application in Resource Manager Essentials that helps you identify the bugs filed against devices in their network. It also helps you to check the status of the bugs.

C

CA	<p>Authority in a network that issues and manages security credentials and public keys for message encryption.</p> <p>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.</p>
called number	Destination telephone number of the call.
calling number	Telephone number from which the call originated.
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	CiscoWorks component that manages the seamless installation, upgrade, patching and uninstallation of Multiple Device Controller modules, and the Core module.

CDP	<p>Cisco Discovery Protocol. 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.</p> <p>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.</p>
certificate	See security certificate .
Certificate Authority	See CA .
Change ACS Settings	<p>Sub-step in the Server Setup workflow. CiscoWorks Assistant helps you to change the login module to use Cisco Secure ACS to provide improved access control.</p> <p>If you have a multi-server setup, CiscoWorks Assistant helps you change the login module of all the servers that are part of the multi-server setup, to ACS mode. See also AAA mode and Access Control Server.</p>
Change Audit	<p>Module in Resource Manager Essentials (RME). It tracks and reports changes made in the network. Change Audit allows other RME applications to log change information to a central repository.</p> <p>Device Configuration, Inventory, and Software Management changes can be logged and viewed using Change Audit.</p>
Change Audit reports	<p>Contains all change information provided by RME applications, based on filter criteria. You can generate a Change Audit report for selected devices.</p> <p>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.</p>
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 Interface Processor. 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 IOS software	<p>Cisco Internetwork Operating System software. Cisco system software provides common functionality, scalability, and security for many Cisco products.</p> <p>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.</p>
Cisco TAC	Cisco Technical Assistance Center. There are four TACs worldwide.

Cisco.com Fetch Interval	<p>RME Administration allows you to configure the interval at which PSIRT and End of Sale or End of Life information is retrieved from Cisco.com.</p> <p>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.</p>
CiscoView Planner page	Page from which you can download the latest CiscoView device packages.
CiscoWorks Home Page	Default home page that appears if you log into a CiscoWorks Server that has only Common Services. If you have installed LMS Portal on the same CiscoWorks Server, LMS Portal will be the default home page.
CiscoWorks Local mode	One of the AAA modes. In the CiscoWorks 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	<p>One of the discovery protocols supported by Common Services Device Discovery.</p> <p>This module discovers the devices in a DSBU cluster and queries the Cluster MIB to discover all members of the cluster.</p>
cluster managed device	One of the device management types in DCR Administration. The Cisco clusters and their member devices are managed using this device management type.
CM View	Campus Manager View.
CMF	Predecessor version of CiscoWorks Common Services. See also CS .
CN	Certificate Common Name.
CNS managed devices	One of the device management types in DCR Administration. Refers to the devices managed by Cisco Networking Services.
collector	Entity that encompasses a source router, a target device, an operation, and collector schedule details.
collector groups	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.
collector schedule duration	<p>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.</p> <p>The polling period is set from 00:00:00 hours to 23:59:59 hours on a daily basis.</p>
Command Line Interface	See CLI .

Common Management Foundation	See CMF .
Common Name	See CN .
Common Object Request Broker Architecture	See CORBA .
Common Services	See CS .
community string	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.
Compliance Management	Option in RME 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.
composite device	See aggregate device .
Config Editor	Option in the Configuration tab of Resource Manager Essentials 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.
Configuration Management	Stores the current, and a user-specified number of previous versions, of the configuration files for all supported Cisco devices maintained in the RME. It tracks changes to configuration files and updates the database if there are any changes.
Configure Range	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.
conflicting device	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.
Connectivity Status	Table in CiscoWorks Assistant that provides information on device connectivity. It displays the Ping, Trace route, Telnet statuses of the device, along with other related information.
contained device	Subordinate device that resides inside an aggregate (or containing) device. For example, an MSFC in a switch).
container group	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.
containing device	See aggregate device .

context menu	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.
Contract Connections	<p>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.</p> <p>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 Resource Manager Essentials (RME).</p>
CORBA	<p>Common Object Request Broker Architecture. CORBA is an industry standard middleware architecture developed and maintained by the Object Management Group.</p> <p>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.</p>
Core Client Registry	See CCR .
core file	<p>File created by the Operating System in CiscoWorks Server when a program is abnormally terminated.</p> <p>The core file is created in the <i>NMSROOT</i>\bin directory on CiscoWorks Server and stores important data about processes.</p>
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 CiscoWorks applications. This provides a foundation for CiscoWorks applications to share a common model for data storage, login, user role definitions, access privileges, security protocols, as well as navigation.
CS View	Common Services View.
CSR	Certificate Signing Request file.
CSV	Comma Separated Values. An 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 Reports (HUM)	CiscoWorks HUM allows you to create reports of MIB variables that are common to all Pollers or specific to a Poller polled by HUM. These reports are called Custom Reports.
Custom Report Template	Option available under RME Inventory Reports that allows you to create new report templates customized according to their requirements. You can edit, or delete existing custom templates.
cwcli	CiscoWorks Command Line Framework (CWCLI) is the interface or framework through which application functionality is provided. This framework is used by Resource Manager Essentials (RME).
cwcli config	CiscoWorks configuration command-line tool of Resource Manager Essentials (RME). It allows you to update devices and archive configurations, delete configurations and compare configurations.
cwcli export	CiscoWorks export command-line tool of Resource Manager Essentials (RME). This command-line tool provides servlet access to Inventory, Configuration and Change Audit data.
cwcli inventory	CiscoWorks Device Management application command-line tool of Resource Manager Essentials (RME). You can use this tool to check the device credentials, export the device credentials, view or delete the RME devices.
cwcli invreport	CiscoWorks Inventory command-line tool of Resource Manager Essentials (RME). 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	CiscoWorks netconfig command-line tool of Resource Manager Essentials (RME). It allows you to use NetConfig from the command line.
cwcli netshow	CiscoWorks 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	A 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.
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 Campus Manager 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.
database restore	Restoring the data that you had backed up earlier on the CiscoWorks Server.
data-link switching	See DLSw .
DCR	Common repository of devices, their attributes, and credentials that are used by various network management applications.
DCR Administration	Interface to administer the common repository of devices, their attributes, and credentials used by CiscoWorks applications.
DCR 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 modes	<p>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.</p> <p>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.</p>
DCR Slave	DCR mode that runs as a Slave to a Master server in the same management domain and shares the device list from the Master.
DCR Standalone	DCR mode that maintains an independent repository of the device list and the credential data.
dcrccli	Utility provided with CiscoWorks to perform the device management tasks through CLI.
debugging	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.
default credentials	Default credentials are stored in DCR and are not associated with any device. You can configure the default credentials and add or import a set of devices in DCR with default credentials. Later, you can edit the value of the credentials and add another set of values with the edited default credentials.
delete interval	Time interval at which records from End host table, IP Phone table, Wireless end hosts table, and the History table are deleted.
Detailed Device report	<p>One of the Inventory reports. It displays detailed hardware, software characteristics and physical containment information for one or more selected devices.</p> <p>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.</p>

Device and Credential Repository	See DCR .
device attributes	Unique identifiers of a device such as domain name, hostname, device identity and management IP Address.
device based acquisition	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.
Device Center	Provides a device-centric view for CiscoWorks applications and device-oriented navigation paradigm. This provides device-centric features and information from a single location.
Device Credentials	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.
Device Diagnostic Tools	Portlet from where you can launch Device Troubleshooting workflow and Device Center. See also Device Troubleshooting .
Device Discovery	Discovers the devices available in the network, starting from the seed device and updates the information to DCR. See also seed device .
Device Fault Manager	See DFM .
Device Management	<p>Starting point for all RME applications. Device Management refers to adding, editing and deleting devices in RME. In other words, it refers to managing devices in RME.</p> <p>In addition to these tasks, Device Management also verifies the device credentials. Device Management also consists of Inventory Management and RME Group Administration.</p>
Device Management mode	Mode in which the devices are managed in CiscoWorks application. It can be either Auto mode or Manual mode. CiscoWorks Assistant helps you to determine whether the new devices are automatically managed by CiscoWorks applications.
Device Map	List of all supported devices on a CiscoWorks Server maintained by Software Center.
device package	Software update that enables CiscoView to support new features for a particular device.
Device Poller	Process that polls the devices in the network. Polling checks if the devices managed by Campus Manager are SNMP reachable, and if the interfaces in the devices are up or down.

Device Report	<p>In CiscoWorks HUM, this report displays all performance parameters of a device, such as memory utilization, CPU utilization, interface utilization, environmental temperature, Poller failures and so on.</p> <p>The Device Report also displays the polled data for MIB variables added in the user-defined templates.</p> <p>CiscoWorks HUM generates Device Report based only on the data for the last 24 hours.</p>
Device Selector	<p>Device Selector allows you to search the devices in DCR. It helps to locate the devices and quickly perform the various device management tasks.</p>
device state	<p>Management state of a device. Can also pertain to the device discovery state. See also management state and Discovery state device.</p>
Device Troubleshooting	<p>One of the CiscoWorks Assistant workflows. Device Troubleshooting workflow helps you identify why a device is unreachable.</p> <p>The generated Device Troubleshooting report contains details on device topology, network inconsistencies, misconfiguration, and Alerts and Syslog Messages for the selected device.</p>
DFM	<p>CiscoWorks product that monitors and displays the operational health of the network. It analyzes events that occur in these environments and determine when a probable fault has occurred. It also notifies you of alert conditions through an online display and other notification services.</p>
DFM Server	<p>Process running DFM software that monitors network elements, uses analysis technology to find the root cause of failures, and diagnoses the effects of the failures on related elements. Also known as DFM Server or domain server.</p>
DFM View	<p>Device Fault Manager View.</p>
DHCP	<p>Dynamic Host Configuration Protocol. Allows you to allocate IP addresses dynamically so that addresses can be reused when hosts no longer need them.</p>
DiscoveryCli	<p>A command line utility used to start, stop and view the current status of Common Services Device Discovery.</p>
Discovery, device	<p>In DFM, this is the process of probing to analyze a network element. Also referred to as collection.</p>
Discovery Filters	<p>Allows Common Services Device Discovery to exclude or include devices from the network, based on some rules.</p>
Discovery Modules	<p>Various protocols used by Common Services Device Discovery to discover the devices from a network.</p>
Discovery state	<p>Condition that a device passes through while being probed. After Discovery, the device information is added to the DFM inventory. DFM Device Discovery states include Known, Learning, Questioned, Pending and Unknown.</p>
discrepancy	<p>Network inconsistencies or anomalies or misconfigurations in the discovered network. They have a severe impact on the network connectivity.</p>

Diskwatcher	Back-end process that monitors disk space availability on the CiscoWorks Server. This process calculates the disk space information of a drive (on Windows) or a file system (on Solaris) where CiscoWorks applications, are installed and stores them in diskWatcher.log file.
Distinguished Name	See DN .
DLSw	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. DLSw uses SSP instead of SRB, eliminating the timeouts, lack of flow control, and lack of prioritization schemes. See also SRB and SSP .
DN	Unique name used by authentication servers when you integrate CiscoWorks Server with external MS Active Directory or IBM SecureWay Directory servers. Distinguished Name is usually composed of the three parts: prefix, usersroot and login.
DNS	Domain Name System. System used in the Internet for translating names of network nodes into addresses.
domain manager	See DFM Server .
Domain Name System	See DNS .
domain server	See domain manager .
Dormant MAC	MAC Addresses that are inactive for the specified number of days.
DSBU	Desktop Switching Business Unit. One of the business units of Cisco.
DSBU cluster	See cluster managed device .
duration	Number of minutes that a collector actively collects network performance statistics at the source router. The default value is Forever.
dynamic group	Group for which the membership list is automatically recomputed whenever it is invoked and is always current.
Dynamic Host Configuration Protocol	See DHCP .
Dynamic Updates	Same as Dynamic User Tracking .
Dynamic User Tracking	Asynchronous updates based on SNMP MAC notifications traps. These updates are used by Campus Manager to track real time changes in the end hosts connected to the network.

E

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	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.
End Host/IP Phone Down	One of the CiscoWorks Assistant 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-	Inventory report, 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.
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 IP SLA Operation. IPM 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.
ethernetJitterAutoIPSLA	Ethernet Jitter Auto IP SLA is an Auto IP SLA Operation. IPM allows you to create, modify, or delete your own Ethernet Jitter Auto IP SLA operations from the List of Operations page for measuring performance between a source and MEP.
ethernetPing	Ethernet Ping is an IP SLA Operation. IPM 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.

ethernetPingAutoIPSLA	Ethernet Ping Auto IP SLA is an Auto IP SLA Operation. IPM allows you to create, modify, or delete your own Ethernet Ping Auto IP SLA operations from the List of Operations page for measuring performance between a source and MEP
event	Indicator that is generated in DFM when a fault occurs on a network. Related events are “rolled up” into alerts. A finite set of events is displayed on the DFM Alerts and Activities Detail page.
Event Distribution System	See EDS .
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.
FAT	A file system table used by the FAT file systems.
File Allocation Table	See FAT .
firewall	One or more routers or access servers designated as a buffer between any connected public networks and a private network to ensure security.
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 CiscoWorks 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 CiscoWorks Server.

G

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

GOLD	GOLD (Generic OnLine Diagnostics) is a device-specific IOS feature with fault detection capabilities. It defines a common framework for diagnostic operations across Cisco platforms running Cisco IOS Software.
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 CiscoWorks. 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.
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.
Historical reports and graphs	IPM 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.
Hostname change script	CLI utility to update the new hostname information in the CiscoWorks directories and files, registry entries, and databases. This occurs after you have changed your hostname in the CiscoWorks machine.
Hot Standby Router Protocol	See HSRP.
HPOV	Hewlett Packard OpenView. A third party software used as network management systems for CiscoWorks Applications.
HSRP	One of the Discovery protocols supported by Common Services 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. See also HSRP in Cisco's Internetworking Terms and Acronyms.
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 .

I

ICMP	Network Layer Internet protocol that reports errors and provides other information relevant to IP packet processing.
ICMP Jitter	Allows you to generate a stream of ICMP packets between a Cisco IOS device (source) and any other IP device (destination) to gather network performance-related statistics.

IDU	Incremental Device Update. Provides software updates and device updates for the earlier releases of a product.
IGMP	Internet Group Management Protocol. Used by IP hosts to report their multicast group memberships to an adjacent multicast router.
IIS	Component of the Windows Operating System that makes it easy to publish information and bring business applications to the Web.
Inactive State	In CiscoWorks HUM, this state indicates that HUM has stopped polling for the device MIB variable instance.
Install Mode - Software Distribution	Method of software distribution used by RME Software Management. According to this mode, the IOS Software Modularity image is extracted or uncompressed to a compact flash with a well defined directory structure. This mode can accommodate the point fix capabilities of Software Modularity.
instance	DFM object or element that belongs to a given device or device group.
Integration Utility	Depending on the specific NMS, this utility can launch Cisco network management applications, browse Cisco MIBs, integrate traps, and add Cisco device icons to NMS topology maps. It also allows remote integration between CiscoWorks applications residing on one server and an SNMP management platform residing on another server.
Internet Control Message Protocol	See ICMP
Internet Control Message Protocol Jitter	See ICMP Jitter .
Internet Information Services	See IIS .
Internet Protocol	See IP .
Internet Protocol Version 6	See IPv6 .
Internetwork Performance Monitor	See IPM .
interval	See duration .
inventory	<ol style="list-style-type: none"> List of all of the network elements in the repository of a DFM domain manager, and the relationships between those elements. The DFM inventory includes devices and their components. In-memory, object-oriented data structure of DFM that stores information about the managed elements currently in a network, and the relationships between these elements.

Inventory Management	<p>Inventory, or the Inventory Collection Service (ICS) and Poller software component of RME, collects inventory data from the network devices and updates the inventory.</p> <p>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.</p>
IP	<p>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.</p>
IP address	<p>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.</p> <p>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.</p> <p>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.</p>
IP Phone Acquisition	<p>Process that collects information about the IP Phones connected in the network.</p>
IP SLA	<p>Internet Protocol Service Level Agreement. This was formerly known as SAA.</p>
IP SLA Responder	<p>Component embedded in a target Cisco device running version 12.1 or later of the Cisco IOS software. It responds to IP SLA request packets from a source device and provides accurate results.</p>
IPM	<p>Internetwork Performance Monitor (IPM) is a network management application that allows you to monitor the performance of multi-protocol networks.</p> <p>IPM monitors the network performance by configuring collectors on IP SLA (IP Service Level Agreement) capable source devices (routers) and collects the performance-related statistics from these devices.</p>
IPM administrative password	<p>To protect the integrity of your IPM database, IPM provides client security, which enables you to define an IPM administrative password.</p> <p>IPM prompts you to enter this administrative password to access the client functions, such as opening the seed files, launching the Secure Web clients, using the <code>ipm tshoot</code> troubleshooting command, and downloading the IPM client software from the IPM Server home page.</p>

IPM View	Internetwork Performance Monitor View.
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).
<hr/>	
J	
JacORB	Object Broker Services provided and used by Common Services.
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	<p>Jobs can be scheduled by the various RME 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.</p> <p>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.</p> <p>Job Approval is also referred to as Maker Checker.</p>
Job browser	<p>A central place to manage all jobs in Common Services.</p> <p>The job management tasks include view the list of jobs, view the details of a selected job, stop a job and delete a job.</p>
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

KDC	Kerberos Key Distribution Center. A centralized server used to authenticate CiscoWorks users and applications when integrated, using the secret key cryptography.
------------	---

Kerberos	Developing standard for authenticating network users. Kerberos offers two key benefits. It functions in a multivendor network, and it does not transmit passwords over the network.
Kerberos Login	One of the non-ACS login modules in CiscoWorks. See also Kerberos .
KeyStore	See TrustStore .

L

LAN Management Solution	See LMS .
last configuration change	<p>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.</p> <p>CiscoWorks Assistant depends on RME to provide these details. See also Device Troubleshooting.</p>
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 Campus Manager.
link ports	Ports connected to Cisco devices (Switch or Router) are link ports. See also trunk port .
Link Registration	Adding additional links to CiscoWorks 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.
LMS	Software solution bundle that provides applications to configure, administer, monitor, and troubleshoot a campus network. It enables network administrators to effectively manage their LAN and campus networks.
LMS Portal	<p>CiscoWorks 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.</p> <p>You can view the important statistics and details of the LMS applications installed on your CiscoWorks Server, in a single page instead of navigating through several pages to view the required data.</p>
Local NMS	Network Management System on the local CiscoWorks Server. See also NMS .

local server	Identifies the CiscoWorks Server on which the Server Setup workflow is run.
local upgrade	Process of upgrading to a newer version of CiscoWorks software on the same machine.
local user setup policy	Username and password policies for CiscoWorks local users in Common Services. 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 CiscoWorks assistant log level settings. You can set the log level to Error, Fatal, Warn (Default), Info, or Debug. The log file, CWAlog, is stored at <code>/var/adm/CSCOpX/log</code> on Solaris, and <code>NMSROOT/log</code> on Windows.
Logrot	Log rotation program in CiscoWorks. Rotates log when CiscoWorks is running or when the logs have reached a particular size. Optionally archives and compresses the rotated logs.
Lookup Analyzer	Utility in Campus Manager 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).

M

MACUHC	MAC User-Host Information Collector. Tracks wired end users dynamically. It receives MAC notification traps from the switches, either directly or through DFM or HPOV. If the traps are from valid sources, it updates the Campus Manager database, accordingly.
major acquisition	Process that discovers all the End hosts and IP Phones that are connected to the devices managed by Campus Manager.
manage servers	Sub-step in the Server Set up workflow. CiscoWorks Assistant 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 Campus Manager 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 DFM domain manager.
Managed Sourced Interface	Configures the source router with appropriate IP address to send or receive the IP SLA (Internet Protocol Service Level Agreement) operation packets.
Management Information Base	See MIB .

management state	Indicates whether a device is currently being monitored by DFM. If a device management state is set to True, it will be discovered and monitored by DFM. 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.
ManagementIP Address	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 Common Services 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 CiscoWorks applications. This package contains new device types, new device type definitions, new device icons, and solutions to some problems in earlier MDF packages.
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	IPM generates these reports and graphs that contain statistical data for a single or a group of collectors on a minute basis.
Missed Cycles	In CiscoWorks HUM, 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.

N

name 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. CiscoWorks 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 RME IP Address	<p>Outcome of Network Address Translation (NAT) support in Resource Manager Essentials (RME). When the RME server is assigned an IP address that is within a NAT boundary, all the devices that are outside this boundary, cannot reach the RME server using the inside address of the RME server.</p> <p>For such devices, RME must use the correct outside address of its server for these transfers. To do this, RME allows the configuration of this outside address of its server (called Natted RME IP Address) for each device.</p>
NDG	Collection of AAA clients such as servers and network devices. When integrating CiscoWorks Server with ACS Server, you should add the CiscoWorks Server and the devices managed in CiscoWorks under a network device group.
NetConfig	<p>Part of Resource Manager Essentials (RME) Configuration Management applications. It allows you to make configuration changes to your network devices, whose configurations are archived in the Configuration Archive.</p> <p>It also provides easy access to the configuration files for all RME supported devices.</p>
Netscape Directory	One of the non-ACS login modules in CiscoWorks. Implements Lightweight Directory Access Protocol.
NetShow	<p>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).</p> <p>These are primarily, show commands that you can run on devices that are managed in RME. RME ships system-defined NetShow Command Sets. You cannot edit or delete any of these Command Sets.</p>
NetView	Third party Network Management System to which CiscoWorks applications, icons, MIBs, and traps can be integrated.
Network Access Restrictions	See NAR .
Network Access Server	See NAS
Network Administrator	Predefined role in CiscoWorks applications. Can perform all Network Operators tasks. Can perform tasks that result in a network configuration change.
Network Device Group	See NDG .

network device grouping	<p>Advanced feature in ACS view and administer a collection of network devices as a single logical group. You must specify the Network Device Group Name value when you configure ACS mode using CiscoWorks Assistant. The Network Device Group name should be in the ACS.</p> <p>The workflow converts the servers part of the Multi-server set up to ACS mode and also adds missing devices to the NDG that you specify. See also Access Control Server.</p>
Network Management Integration Module	See NMIM (Also known as Integration Utility).
network management system	See NMS .
Network Operator	Predefined role in CiscoWorks applications. Can perform tasks related to network data collection. Cannot perform any task that requires write access on the network.
Network View	Contains network-based portlets from CM, RME, IPM, and DFM applications.
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 portlet	Displays a N-hop view from a specified device. This is much faster than the regular Campus Manger 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 CiscoWorks LMS is installed.
Non Installed Mode - Software Distribution	<p>Method of software distribution used by RME 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.</p> <p>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.</p>
non-link trunk ports	Trunk ports connected to End hosts or IP Phones. See also trunk port .
Not Reachable	In CiscoWorks HUM, Not Reachable status indicates that the device may be down or not reachable.

notifications	Configurable messages sent by DFM 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

Object Finder portlet	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.
ODBC	Generic vendor independent API for accessing relational databases.
OGS	Object Grouping Service. A service provided by Common Services to group objects such as devices, collectors.
OID	Object identifier. Uniquely identifies a device, module, interface, or power supply. Values are defined in specific MIB modules.
Open Database Connectivity	See ODBC .
Open Shortest Path First Protocol	See OSPF .
operation	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.
OpsxmldbEngine	Database engine for the CiscoWorks Assistant workflow engine.
OpsXMLRuntime	Cisco Works Assistant workflow engine.
osagent	Process that allows CORBA servers to register their objects and assists CiscoWorks applications in the location of objects.
OSPF	One of the Discovery protocols supported by Common Services Device Discovery. The OSPF Discovery Module uses ospfNbrTable and ospfVirtNbrTable MIB to find its neighbor's IP addresses. See also OSPF in Cisco's Internetworking Terms and Acronyms.

- Out-of-Sync report** 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.
- Overlay graph** Comparative view of the latency of one or more collectors.

P

- Package Map** List of all device packages installed on a CiscoWorks Server 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 CiscoWorks Server 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 CiscoWorks Server, such as Active Directory, Kerberos 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 in a CiscoWorks Server. This account can enable communication among multiple CiscoWorks Servers. This can also authenticate processes running on a remote CiscoWorks Server.
- Peer Server Certificate** Certificate of peer CiscoWorks Servers. This is required to communicate with another CiscoWorks Server in a domain. When you add a server using Server Setup workflow, CiscoWorks Assistant fetches the certificate information of the server you are adding, and prompts you to accept the peer certificate. See also [Trust creation](#).
- PERL** Unix based scripting language. Perl scripts ends with an extension.pl

Permanent	In CiscoWorks HUM, Permanent status is displayed if the polled MIB variables or instances are not available in the device.
Permissions Report	A report in Common Services 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 CiscoWorks Server.
ping	Device diagnostic tool used by CiscoWorks. Use the Ping tool to test whether the device is reachable. A ping tests an ICMP echo message and its reply.
ping sweep	Basic network scanning technique used to determine which range of IP addresses map to live end hosts.
PKCS	Set of standards for public-key cryptography developed by RSA Laboratories. These standards are designed for binary and ASCII data.
PKI	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.
poll interval	Periodicity for polling the network using Device Poller. See also Device Poller .
Poller	In CiscoWorks HUM, this is a collection of devices and template MIB instances.
Poller Reports	In CiscoWorks HUM, these are reports created, based on the template added in a given Poller
polling frequency	Indicates how often CiscoView sends SNMP queries to a managed device.
Polling Interval	Frequency at which the IPM server polls the source router to retrieve the statistics and update the IPM database. IPM 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.
Polling Interval (HUM)	<p>The duration after which CiscoWorks HUM queries the MIB variable on the device.</p> <p>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.</p>
port attributes	Information about the ports in a device such as, Type of port, Administrative Status.
Portal Log Settings portlet	Sets the level of details you will find in the log based on the settings you configure.
portlets	Enables you to organize information inside a view. These are user interface components that are managed and displayed in a view.

Primary ACS server	Primary server providing authentication services to CiscoWorks Server after integration. If the primary server is down, authentication services are provided by secondary servers, if they are configured.
Primary credentials	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.
Privacy password	SNMPv3 privacy password of the device in AuthPriv mode.
Privacy protocol	SNMPv3 privacy algorithm used in AuthPriv mode. Can be DES, 3DES, AES128, AES192, and AES256.
Private	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 CiscoWorks LMS Portal and select Private at the top right corner.
Product Instance Device Mapping	Registry that stores mapping information between devices and applications. Also, known as PIDM. Each CiscoWorks application should register the information about the devices with PIDM.
Proxy server	Intermediate server that connects the clients to the external server.
PSIRT	Cisco's Product Security Incident Response Team.
PSIRT Summary report	<p>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.</p> <p>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.</p>
PSU	Central location within the CiscoWorks application to check for software updates and device updates, download and install the updates, and schedule downloading updates.
PSUCLI	CLI version of Package Support Updater.
PTT	Performance Tuning Tool. Command Line Interface (CLI) utility that enables you to apply and list various profiles available in CiscoWorks Server. Profiles consists of configuration files in the form of XML files whose values are based on the recommendations for various Resource Manager Essentials (RME) applications.
Public Key Cryptography Standards	See PKCS .

Public Key Infrastructure	See PKI .
Public mode	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.

Q

QoS	Measure of performance for a transmission system that reflects its transmission quality and service availability.
Quality of Service	See QoS .
Quick Reports	<p>CiscoWorks HUM contains a set of predefined system generated reports called Quick Reports.</p> <p>Quick Reports provide detailed information on the top 10 and bottom 10 devices polled by HUM. These are devices that have the highest or lowest utilization or availability value.</p>

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 CiscoWorks Server.
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	Remote Copy Protocol. 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	Remote Copy Protocol or Routing Control Processor.
Reachable	In CiscoWorks HUM, this indicates that the device is available and reachable in the network.
Reachable devices	Devices that are discovered by Common Services Device Discovery.
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 NMS	Network Management System on the remote CiscoWorks Server. See also NMS .
Remote upgrade	Process of installing a newer version of CiscoWorks software on a different machine and restoring the data backed up from the older version to the newer version.
report archives	A 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	<p>In CiscoWorks HUM, 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.</p> <p>System jobs are not shown in the Report Job Browser.</p>
Reports	CiscoWorks HUM 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 .
Resource Manager Essentials	See RME .
restore data	See database restore .
resume	Setting a device management state to True so that DFM will monitor the device. This is normally done from the DFM 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.

RME	<p>Powerful suite of Web-based applications offering network management solutions for Cisco switches, access servers, and routers. RME is bundled with LAN Management Solutions (LMS).</p> <p>This suite is part of the CiscoWorks family of products. It is an Enterprise solution to network management.</p>
RME system-defined groups	<p>Default grouping of devices in RME. This is a read only group. You cannot create new groups under system-defined groups. The system-defined device groups available in RME are All Devices, Normal devices, Pre-deployed, Previous selection and Saved device list.</p>
RME user-defined groups	<p>Device groups that can be created to reflect the way a network is managed. New user-defined groups created in Resource Manager Essentials (RME). You cannot create user-defined groups for Common Services (CS) in RME.</p> <p>The user-defined groups can be either dynamic or static groups with private or public access privileges. See also user defined group.</p>
RME View	<p>Resource Manager Essentials view.</p>
RMON	<p>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.</p> <p>Download the CiscoView Mini-RMON Manager device package to enable RMON functionality within CiscoView.</p>
Rogue MAC	<p>MAC Addresses that are not authorized to exist in your network.</p>
root device	<p>Device from which the N-Hop portlet starts drawing the Topology map.</p>
round-trip time	<p>See RTT.</p>
route	<p>Path through an internetwork between a specific source and target.</p>
router	<p>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.</p>
RP	<p>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.</p>
RS	<p>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.</p>
rsh	<p>Remote Shell Protocol. Protocol that allows a user to execute commands on a remote system without having to log in to the system.</p>
RSS	<p>Really Simple Syndication. Really Simple Syndication (RSS) is an 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.</p>

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 IPM and SA Agent are round-trip time latency measurements.
RTTMON MIB	<p>Round-trip time monitor management information base. 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.</p> <p>The IPM application obtains the round-trip time statistics from this MIB. You can access additional information about this MIB, on the Internet at ftp://ftp.cisco.com/pub/mibs/v2/CISCO-RTTMON-MIB.my.</p> <p>This MIB has been extended to monitor network performance statistics in addition to round-trip time statistics.</p>
RU	Request and response messages exchanged between NAUs in an SNA network.
<hr/>	
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	<p>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.</p> <p>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.</p>
Sample Interval	Frequency with which the IPM source device polls the target device to retrieve the statistics based on the IP SLA operations configured by you. IPM retrieves the statistics from the target device every 60 seconds, by default.
scheduled report	See job .
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 CiscoWorks Server only when the primary ACS server is down. You should configure the hostname or IP Address, and the port number on the CiscoWorks Server.
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.
seed device	Starting point for Device Discovery. See also Device Discovery .
seed file	DFM 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. DFM can use seed files to initiate device discovery.
Self-Signed certificate	<p>Security certificates created on the CiscoWorks Server that enable SSL communication between the client browser and management server. Self-signed certificates are valid for five years from the date of creation.</p> <p>When the certificate expires, the browser prompts you to install the certificate again from the server where you have installed CiscoWorks.</p>
server	Node or software program that provides services to clients.
Server Setup	One of the CiscoWorks Assistant 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.
Simple Network Management Protocol	See SNMP .
Single Sign On	See SSO .
SIU	<p>Communication between multiple CiscoWorks Servers 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.</p> <p>This trust user is called System Identity User. The System Identity User is also used for inter-process communication. See also Trust creation.</p>

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 Resource Manager Essentials (RME) 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.
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 IPM SNMP server to perform all IPM-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 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 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.
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 Management CLI	Command-line Interface of Resource Manage Essentials. You can use this tool to invoke the Software Management features from the command-line.
source router	Originating router or switch running IOS from which IPM measures network performance. The source router or switch must be running a version of Cisco IOS software version that supports IP SLA.
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.
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. CiscoWorks 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 CiscoWorks Servers 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 CiscoWorks Server 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 .
stale groups	Groups that belongs to users groups who are removed from CiscoWorks.
Standby Switch	After converting two VSS-enabled Standalone Switches into a Virtual Switching System, one switch becomes the Standby Switch and other the Active Switch.
static group	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.
static route	Explicitly configured route entered into the routing table. Static routes take precedence over routes chosen by dynamic routing protocols.
Structured Query Language	See SQL .
subnet based acquisition	Runs only on those subnets that are configured in Campus Manager. Campus Manager discovers End Hosts and IP Phones on all VLANs in the configured subnets.

- subnet groups** A system defined device group in device selector that contains the devices managed in Campus Manager.
- These subnet based groups help you work on smaller subsets of devices that are logically grouped.
- subscription** See [notifications](#).
- Super Admin** User in ACS created after the CiscoWorks Server is integrated to ACS. The Super Admin user has all privileges assigned in all applications. See also [Access Control Server](#).
- suspend** To set a device's management state to False so that DFM will not monitor the device. This is normally done from the DFM Detailed Device View. See also [resume](#).
- SWIM** SoftWare Image Management or Software Management is an application in Resource Manager Essentials (RME). The Software Management application 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 execute software image upgrades to multiple devices on the network at the same time.
- Switch Check** You can select this while running the End Host Down/IP Phone Down workflow. If you select this option, CiscoWorks Assistant 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](#).
- Switch-to-Switch Protocol** See [SSP](#).
- Syslog Analyzer/Collector** 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.
- Syslog messages** Messages that originate from a device in response to some activity that affects it. The devices that are connected to the RME server, are configured to send Syslog messages to the RME Syslog server whenever there are changes.
- The RME 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.

syslogConf.pl Utility	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 RME server, and Change Syslog File Location. You can run this script in the RME server as well as in the RSAC server. You can perform all these tasks in a RME server by running the syslogConf.pl script from the command prompt.
System Administrator	Predefined role in CiscoWorks. Can perform all CiscoWorks system administration tasks.
system defined group	Top-level container for standard groups that are accessible to and used by most Campus Manager users. It is available by default.
System Identity User	See SIU .
System Services Control Point	See SSCP .
System Status	Details about Campus Manager processes—Device Discovery, Data Collection and User Tracking Acquisition.
System View	View that contains all system related portlets, such as Job Information Status portlet, DCR and AAA, Log Space Usage, and Process Status.
System-defined Template	In CiscoWorks HUM, 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.

T

TAC	Cisco's Technical Assistance Center.
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	<p>Device to which the packets are sent by the IP SLA source devices. Target devices are the destination devices for which you want to gather network performance statistics.</p> <p>The target devices can be any IP-addressable device or a Cisco device running the IP SLA Responder on which the source router performs IP SLA operations.</p>
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 .
Template	In CiscoWorks HUM, 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).
Terminal Access Controller Access Control System	See TACACS .
Tertiary ACS Server	ACS server that provides authentication services to CiscoWorks Server 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 CiscoWorks Server.
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 CiscoWorks HUM, this is an optimal value for a MIB variable set by the user or the system.
Threshold Violation Reports	In CiscoWorks HUM, these are reports created, based on the threshold configured for the MIB variable.
Time Domain Reflectometry reports	Detects faults in a cable. Campus Manager supports TDR Cable Diagnostic Test and generates a report listing the results of the test on Cisco Catalyst 6000 switches.
timeout	<p>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.</p> <p>In CiscoView, this is the length of time that elapses before an SNMP request sent by the application to a managed device times out.</p>
TOC	Table of Contents.
Tomcat	Java servlet engine used on Windows and Solaris systems that hosts applications on the CiscoWorks desktop.

Topology and Neighbor information	Campus Manager 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.
Traceroute	Device diagnostic tool used to detect routing errors between the management station and the target device.
Transient	In CiscoWorks HUM, 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	Campus Manager server port that listens to SNMP MAC Notification traps sent from devices.
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 the VLANs that exist on the switch and carry traffic for all those VLANs between the switches.
Trust creation	Creation of trust is required to enable communication between CiscoWorks Servers part of a multi server set up. Communication among multiple CiscoWorks Servers 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 CiscoWorks maintains the list of certificates that it trusts.

U

UDF	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.
------------	--

UDP	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.
UDP Jitter	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.
UE	User Experience.
UI	User Interface.
unacknowledging discrepancy	Returns an acknowledged discrepancy into the Discrepancies report. See also acknowledging discrepancy .
Uniform Resource Locator	See URL .
Uniform Resource Name	See URN .
unreachable devices	Devices that are not reachable by Common Services Device Discovery.
UPN	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.
URL	Type of formatted identifier that describes the access method and the location of an information resource object on the Internet.
URN	<ol style="list-style-type: none">1. Uniform Resource Name. An Internet addressing scheme.2. Refers to the URL of a AUS Managed Device in CiscoWorks.
User Datagram Protocol	See UDP .
User Datagram Protocol jitter	See UDP Jitter .
User Defined Fields	See UDF .
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	Campus Manager application that 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	<p>CiscoWorks HUM 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.</p> <p>You can add or delete MIB variables in a user-defined template.</p>
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 .

V

view	<ol style="list-style-type: none"> 1. Selected set of device groups that you want to observe on the DFM Alerts and Activities display. 2. In LMS Portal, a view is a page that displays a set of relevant information. LMS Portal comes with four default views such as Functional, System, Network and CS (Common Services). <p>You can also create your own views and add content of your choice. The views are displayed as tabs at the top of the page.</p>
Virtual Switching System	<p>Technology that combines two standalone distribution switches found in the local distribution layer into a single management point.</p> <p>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.</p>
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 RME is used to convert the two VSS-enabled Standalone Switches into a Virtual Switching System.
Virtual Switching System Configuration tool	<p>The Virtual Switching technology is implemented in Lan Management Solutions (LMS) by providing a Virtual Switching System Configuration Tool under Resource Manager Essentials (RME).</p> <p>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.</p>

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.
VMware	Virtualization system on which CiscoWorks 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.
VSS Configuration	See Virtual Switching System Configuration.
VSS Mode	See Virtual Switching System Mode.

W

WLSE UHIC	Process that updates the Campus Manager 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.
workflows	<p>CiscoWorks Assistant workflows help you to deploy and manage the CiscoWorks Servers and troubleshoot your network. The workflows take you through the different steps required to achieve these tasks in a simplified manner.</p> <p>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.</p> <p>See also End Host/IP Phone Down, Device Troubleshooting and Server Setup.</p>

X

XML	Standard maintained by the World Wide Web Consortium (W3C). It defines a syntax that lets you create markup languages to specify information structures. CiscoWorks maintains application configuration, roles, tasks and other information in XML format.
XSL	XML Stylesheets.

Notices

The following notices pertain to this software license.

OpenSSL/Open SSL Project

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

License Issues

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License:

Copyright © 1998-2007 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)”.
4. The names “OpenSSL Toolkit” and “OpenSSL Project” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called “OpenSSL” nor may “OpenSSL” appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:
 “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)”.

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT “AS IS” AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License:

Copyright © 1995-1998 Eric Young (eay@cryptsoft.com). All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:
"This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)".

The word 'cryptographic' can be left out if the routines from the library being used are not cryptography-related.

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)".

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License].

