



CiscoWorks LAN Management Solution 3.2

Large-Scale

Deployment Guide



Contents

Overview	3
CiscoWorks LAN Management Solution 3.2	3
Related Reading	5
Licensing Options	5
Licensing and Scalability of CiscoWorks HUM	6
Application Scaling Numbers	7
General Rule Regarding Number of Servers Needed for CiscoWorks LMS Bundle	7
Deployment Scenarios	8
Device Credentials Repository	8
Device Discovery	9
Device Groups	10
Integration with Cisco Secure Access Control Server for Authentication and Authorization	10
Secure Views	11
Single Sign-On	11
Registering Applications with the CiscoWorks LMS Portal Homepage	11
Single Server: All CiscoWorks LMS Applications Installed on the Same Server	11
Managing 1500 Devices on the Same Server	12
Managing 5000 Devices on the Same Server	12
Multi-server Setup	13
Applications on Separate Servers Managing a Single Domain	14
Multiple Instances of CiscoWorks LMS Bundle (Multiple Management Domains)	15
Multiple Instances of CiscoWorks LMS Bundle (Single Domain)	17
Centralized CiscoWorks RME Server	17
Dividing Large Networks into Smaller Management Domains	19
Redundant-Server Scenario	19
Device Discovery	20
CiscoWorks Campus Data Collection	20
User Tracking Discovery	20
CiscoWorks DFM Polling Parameters and Threshold	20
CiscoWorks RME	21
General Observations	21
Extracting Data from CiscoWorks LMS Servers for Centralized Reporting	22
CiscoWorks RME Data Extracting Engine	22
CiscoWorks Campus Manager Data Extracting Engine	23
Open Database Schema Support in CiscoWorks LMS 3.2	23
Application Performance Numbers	24
CiscoWorks Common Services Performance Data and Recommendations	24
CiscoWorks Campus Manager Performance Data and Recommendations	24
CiscoWorks RME Performance Data and Recommendations	25
Multi-server Configuration Example	26
CiscoWorks LMS Portal	28
Summary	31

Overview

Today's network managers are often faced with the task of managing very large and complicated networks. As networks continue to grow in size and complexity, the number of network management tools and products are increasing as well. In such a situation, it is a challenge for administrators to effectively manage networks.

Cisco offers a number of CiscoWorks product bundles for effective network management. Each of these product bundles typically has a documented system recommendation and size limitation (for a single-server installation). However, customers often need additional information about how to manage networks larger than the recommended limit for a single CiscoWorks installation. This paper provides information and recommendations for resolving issues related to managing networks larger than the recommended limit for a single CiscoWorks installation.

It is important to understand that dealing with concerns related to a large network is a complex problem, with a number of factors affecting the end result. Even a simple question such as "What is the size of the server required for CiscoWorks LAN Management Solution (LMS) to manage x number of devices?" can be difficult to answer in a meaningful way. The number of devices is, at best, a vague indicator for estimating the required system resources--different devices can have vastly differing numbers and types of managed objects. In addition to the number of devices, the following points must be considered before providing an answer:

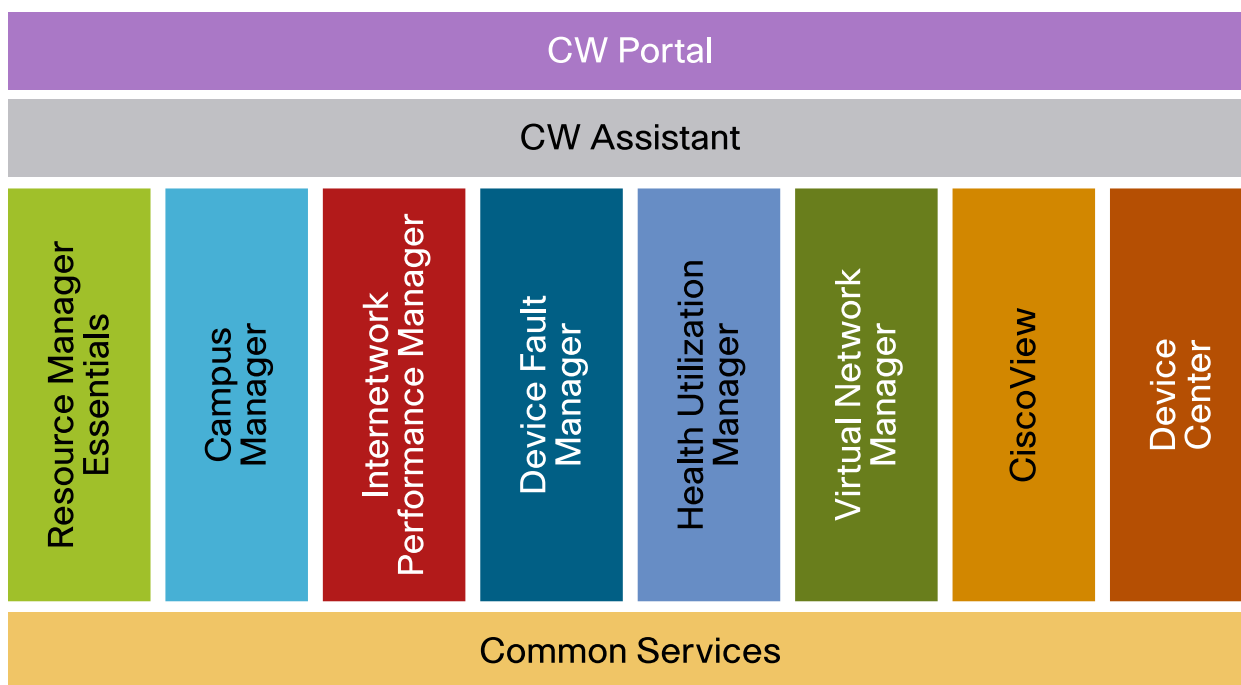
- The components and functions of the products that are most important to the network managers
- The number of users possessing network management tools and the number using the tools simultaneously
- The administrative groupings of the network devices and network management users, in the case of very large networks

These points, along with the information contained in this paper, will help enable users to make informed decisions about deploying CiscoWorks LMS for managing their networks.

CiscoWorks LAN Management Solution 3.2

CiscoWorks LAN Management Solution 3.2 is the current version offered by Cisco and includes the components shown in Figure 1.

Figure 1. CiscoWorks LMS 3.2 Applications



* Note: Health Utilization Monitor (HUM) is an add-on product to LMS.

- **CiscoWorks Common Services 3.2**

Common Services provides a set of shared application services that are used by all LMS applications. It runs the database server, the web server, the job scheduler, and other backend processes to support other applications.

CiscoWorks Common Services 3.2 includes CiscoView 6.1.9, Integration Utility 1.9, LMS Portal 1.2, and CiscoWorks Assistant (CWA) 1.2.

- LMS Portal is the GUI front of the CiscoWorks server. It gives the user ability to customize information regardless of applications and view frequently used information in a common place. With LMS Portal, users do not need to navigate through several pages to obtain the information they need--instead, users can display application-related information as portlets and customize the homepage to have all information on a single screen from all applications.
- CiscoView provides a “front panel” graphical display of Cisco® devices, allowing users to easily interact with device components to change configuration parameters and monitor statistics.
- Integration Utility is an integration module that supports third-party network management systems, such as HP OpenView NNM (Network Node Manager).
- CiscoWorks Assistant (CWA) 1.2 has the following features:
 - Workflows to improve usability of CiscoWorks LMS applications
 - Help to solve real business problems and overcome network inconsistencies

- **CiscoWorks Resource Manager Essentials (RME) 4.3**

To support lifecycle management, CiscoWorks RME provides the ability to manage device inventory and audit changes, configuration files, software images--as well as syslog analysis.

- **CiscoWorks Campus Manager (CM) 5.2**

CiscoWorks Campus Manager provides the ability to visualize network topology, manage VLANs, detect/fix network discrepancies, and track end-host/IP phone/user information.

- **CiscoWorks Device Fault Manager (DFM) 3.2**

CiscoWorks Device Fault Manager provides the ability to monitor device faults in real time and determine the root cause by correlating device-level fault conditions. CiscoWorks DFM can issue notifications of critical network conditions by email or pager. Fault History lets the user store and access historical information about alerts and faults that are detected and processed by CiscoWorks DFM.

- **CiscoWorks Internetwork Performance Monitor (IPM) 4.2**

CiscoWorks Internetwork Performance Monitor measures network performance based on the synthetic traffic generation technology within the Cisco IOS[®], which is known as Cisco IOS IP SLA (Service Level Agreement). Using synthetic traffic by IPM gives the network manager a high degree of flexibility in selecting the endpoints in a network between which network performance will be measured. This flexibility makes IPM a highly effective performance-troubleshooting tool.

- **CiscoWorks Virtual Network Manager (VNM)**

CiscoWorks VNM is an enterprise solution that allows administrators to carry out end-to-end VRF configuration and edit, extend, and delete VRF configuration details. It also collects VRF details of the VRF configured in devices and generates reports to help you analyze VRF configurations on your network.

There is a separate whitepaper for VNM at

http://www.cisco.com/en/US/products/sw/cscowork/ps2425/prod_white_papers_list.html.

Add-on application:

- **CiscoWorks Health Utilization Monitor (HUM) 1.2**

CiscoWorks Health and Utilization Monitor (HUM) is an add-on application pre-integrated into CiscoWorks LMS. It is a Simple Network Management Protocol (SNMP)-based MIB polling application that monitors network elements (such as CPU, memory, interfaces/ports, and links) for their availability and utilization levels and provides historical reporting.

Related Reading

Refer to the *CiscoWorks LMS 3.2 Deployment Guide* and *Installation and Configuration Guide* for an overview of CiscoWorks LMS 3.2. The *CiscoWorks LMS 3.2 Deployment Guide* focus on single-server installation, while this whitepaper is mostly dedicated to multi-server setup where the applications are distributed across multiple servers for better scalability and performance.

CiscoWorks LMS 3.2 Deployment Guide can be found at the whitepapers section at <http://www.cisco.com/go/lms>.

Licensing Options

The licenses in CiscoWorks LMS 3.2 are device-based for all applications except CiscoWorks IPM, where the license is based on the number of configured collectors.

You can select any one of the following five SKUs for CiscoWorks LMS 3.2:

- CWLMS-3.2-100-K9

Allows you to manage the following in each application:

- CiscoWorks RME: 100 devices
- CiscoWorks Campus Manager: 100 devices
- CiscoWorks DFM: 100 devices
- CiscoWorks IPM: 100 devices and 300 collectors

- CWLMS-3.2-300-K9
Allows you to manage the following in each application:
 - CiscoWorks RME: 300 devices
 - CiscoWorks Campus Manager: 300 devices
 - CiscoWorks DFM: 300 devices
 - CiscoWorks IPM: 300 devices and 1000 collectors
- CWLMS-3.2-1.5K-K9
Allows you to manage the following in each application:
 - CiscoWorks RME: 1500 devices
 - CiscoWorks Campus Manager : 1500 devices
 - CiscoWorks DFM: 1500 devices
 - CiscoWorks IPM: 1500 devices and 1500 collectors
- CWLMS-3.2-5K-K9
Allows you to manage the following in each application:
 - CiscoWorks RME: 5000 devices
 - CiscoWorks Campus Manager: 5000 devices
 - CiscoWorks DFM: 5000 devices
 - CiscoWorks IPM: 5000 devices and 5000 collectors, or 10,000 collectors (1 hour polling interval)
- CWLMS-3.2-10K-K9
Allows you to manage the following in each application:
 - CiscoWorks RME : 10,000 devices
 - CiscoWorks Campus Manager: 5000 devices
 - CiscoWorks DFM: 5000 devices
 - CiscoWorks IPM: 5000 device and 5000 collectors, or 10,000 collectors (1 hour polling interval)

Note: The 10K SKU have not been tested at bundle level, that is, 10k for RME and 5K devices in all other applications on a single server. It can be only in a multi-server deployment, with RME on a dedicated server and other applications managing 5K devices on more servers.

Licensing and Scalability of CiscoWorks HUM

Consistent with the CiscoWorks LMS bundle, CiscoWorks HUM is licensed based on the number of devices managed (Table 1).

Table 1. CiscoWorks HUM SKUs

SKU	License Parameter (Device Count)
CWHUM-1.2-S-K9	50
CWHUM-1.2-M-K9	300
CWHUM-1.2-L-K9	1000

- Today the maximum SKU that is offered for CiscoWorks HUM is 1000 devices (licensing restriction). Adding licenses to increase the number to 10,000 devices is not supported, even though the LMS bundle supports up to 10,000 devices. In future releases users will be able to add licenses to accommodate up to a maximum of 5000 devices total.

- The device count restricts the license options. One CiscoWorks HUM server can support up to 1000 devices. Actually the scalability of HUM depends on how many MIB objects are being managed. The maximum number of MIB objects supported is 100,000, with 40,000 on 1 minute and 60,000 on 5 minute polling intervals.

Application Scaling Numbers

This section describes the specific scaling numbers and concerns for each of the CiscoWorks LMS applications. This information will help users decide the server size and distribution that would best suit their needs and optimize performance. You need to purchase appropriate CiscoWorks LMS licenses to manage these numbers.

The tested numbers for each application in standalone mode are the following:

- CiscoWorks RME: 10,000 devices (You need to buy CWLMS-3.0-10K-K9 to manage 10,000 devices in a single server.)
- CiscoWorks Campus Manager: 5000 devices and 250,000 end stations
- CiscoWorks DFM: 5000 devices
- CiscoWorks IPM: 10,000 collectors
- CiscoWorks Common Services Device Credentials Repository (DCR): 50,000 devices and 100 user-defined groups

Note: Multiple, simultaneous users can affect system performance. Depending on the size of the server, the maximum number of users who can log in concurrently without the performance being affected is 20.

General Rule Regarding Number of Servers Needed for CiscoWorks LMS Bundle

Note: CiscoWorks LMS 3.2 can manage up to 5000 device per server (DFM excluded), meaning one server with adequate hardware configurations can manage up to 5000 devices with Common Services, RME, Campus Manager, and IPM, but an additional server will be needed to run DFM if DFM is used extensively to poll the devices.

Note: To have better performance and reliability, it is recommended to distribute the applications across multiple servers once there are more than 5000 managed devices. For example, many users dedicate a server to run RME on one server, with other applications running on one or more servers depending on how heavily they are used.

Note: On top of this, CiscoWorks HUM can be deployed either as a standalone application or in bundle environments.

- **Standalone:** CiscoWorks HUM with CiscoWorks Common Services, LMS Portal, and CiscoWorks Assistant
- **Bundle:** CiscoWorks HUM with CiscoWorks LMS

Table 2 lists the scalability numbers for the different SKUs in both standalone and bundle deployments.

Table 2. CiscoWorks HUM Scalability Limits for Standalone and Bundle Deployments

Devices	Environment Type	MIB Objects Polled
300 Devices	Standalone (300 HUM SKU)	30,000 MIB objects
	Bundle (300 HUM SKU + 1,500 LMS SKU)	20,000 MIB objects
1,000 Devices	Standalone (1,000 HUM SKU)	100,000 MIB objects
	Bundle	Not supported

Note: The scalability information is pending upon testing for the 50-license SKU. Generally the more powerful hardware will support more MIB objects.

Deployment Scenarios

When working with large-scale deployments, it is important to determine the required server size and to decide whether to deploy the network management tools across multiple network management servers. Beyond the point where a single server is adequate, there may be a need to use multiple servers for a single management domain (a single managed network) by distributing applications across multiple servers for better performance and scaling.

Larger networks have to be split into multiple management domains and multiple groups managed by individual management servers or groups of servers. When a network is split into multiple domains, the division can be made in many ways: by administrative groups, by geography, or any other parameter that fits the network's administrative needs.

Note: For a successful deployment of CiscoWorks LMS 3.0, you should understand some of the new functions introduced in this version, as well as the architectural changes associated with them. The key changes are briefly covered in the following sections. It is highly recommended that the corresponding user guides be consulted to get a better understanding of the individual CiscoWorks LMS bundle components.

New Features in CiscoWorks LMS 3.2

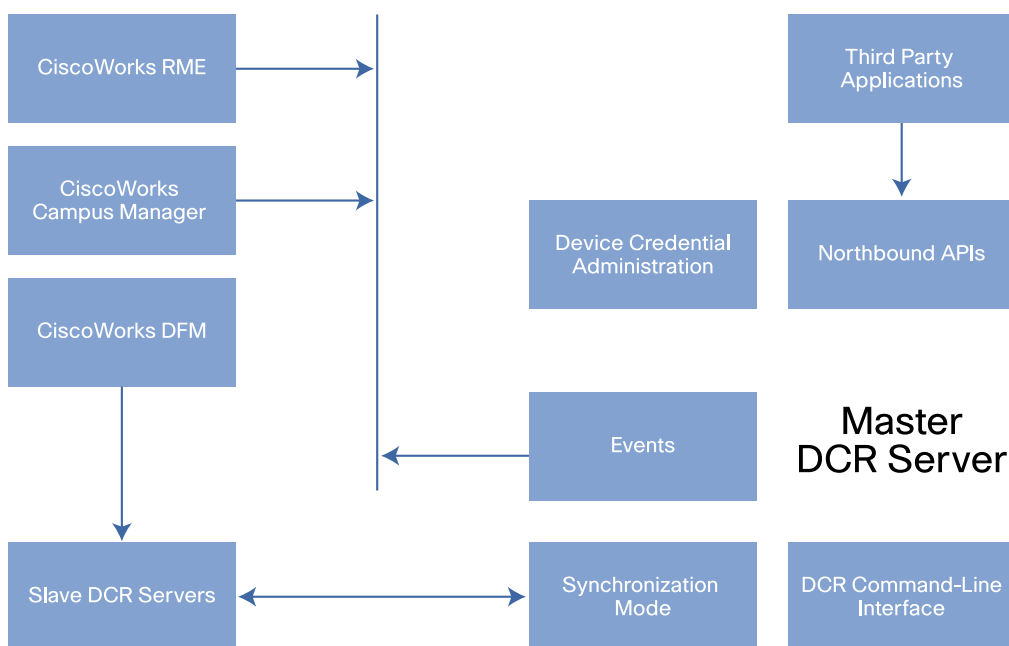
CiscoWorks LMS 3.2 supports high availability and disaster recovery based on Veritas clustering components.

For details about high availability and disaster recovery using Veritas, refer to the document published at <http://www.cisco.com/go/lms>.

Device Credentials Repository

Prior to CiscoWorks LMS 2.5, each application retained its own copy of device credentials (the information needed to access the device), and there was limited sharing of device credentials between applications. As a result, administrators spent significant time and resources reconciling the devices and credentials among applications. See Figure 2 for a typical Device Credentials Repository architecture.

Figure 2. DCR Architecture



The DCR, introduced in CiscoWorks LMS 2.5, allows the user to manage the device list and associated credentials and other user-defined device attributes in a management domain. In a multi-server setup, where each server could host one or more CiscoWorks LMS application instances, the DCR could serve as the single repository where the user could manage the device lists and related attributes for use by all the applications in the domain.

Some of the key benefits of DCR are:

- Secure storage in one place
- Single-point management of devices and attributes
- Automatic replication among servers (for continuous operation even in the case of interserver link failures)
- Changes to the store allowed only in the master server

In a single-server scenario, the DCR will be operating in a standalone mode (the default mode after installation). In a multi-server scenario, the user should designate one of the servers as the master and configure the other servers in a slave mode. The copy of the DCR data in the slave servers is always in sync with the master DCR.

Note: The only data replicated between the master and slave servers is the DCR. Replication of other application data such as RME configuration, syslog, and so on are not supported yet.

The master DCR server contains to the master repository of device list and credential data. There is only one master repository for each management domain, and it contains the most up-to-date device list and credentials. DCR slaves are slave instances of DCR on other servers and provide transparent access to applications installed on those servers. Any change to the repository data occurs first in the master with the changes being propagated to all the slaves. There can be more than one slave in a management domain, but any slave can become a master at any time.

In a standalone mode, the DCR maintains an independent repository of device list and credential data. It does not participate in a management domain, and its data is not shared with any other DCR. It does not communicate with or contain registration information about any other master, slave, or standalone DCR.

Devices newly added in the DCR can be managed by an application in the following ways:

- **Automanage mode:** In this mode, applications listen to the “Add Device” event and automatically start managing the device if it is relevant to the application. All the applications in the CiscoWorks LMS bundle are by default in automanage mode.
- **Manual-manage mode:** In this mode, the application keeps track of all newly added devices and shows the list to the user. The user chooses few or all devices from the list for the application to manage.

If the two servers are set up as master/slave, they will share the same copy of DCR. All changes to DCR must be done on the master first then replicate to the slave. In case of failure:

- If the slave fails permanently, the master will continue to work.
- If the master fails permanently, the slave will continue to work, but it cannot add or discover new devices. The slave needs to be changed back to “standalone” mode or promoted to be a master when joined by other slaves to be fully functional.
- If either the master or slave fails transiently, the servers automatically recover once they get back online.

Device Discovery

Prior to CiscoWorks LMS 3.2, it has been tested and certified that the discovery function (NGD: Next Generation Discovery, introduced in LMS 3.0.1), is able to discover 5000 devices from the network at a time. As far as discovery is concerned, there is no hard limit in discovering the number of devices. However, when users have a large number

of devices (greater than 5000) in a network, there might be performance-related issues related to the discovery process.

CiscoWorks LMS 3.2 will support discovery of 10,000 devices at a single instance. Discovery can be extended to discover still more devices by scheduling a couple of instances with appropriate and different network seed devices.

In the case of masters/slaves, each server should be capable of discovering 10,000 devices at an instance. Also note that a server cannot run more than one instance of discovery at a time.

Refer to the whitepaper on Next Generation Discovery at

http://www.cisco.com/en/US/prod/collateral/netmgtsw/ps6504/ps6528/ps2425/white_paper_c11-493921_ps3996_Products_White_Paper.html

Device Groups

Device groups are characterized by a set of properties such as associated rule, name, description, type, and access permission. The rule determines the membership of a group, which may change whenever the rule is evaluated. Groups are hierarchical, and they can be dynamic or static and private or public.

In CiscoWorks LMS, device groups can be created under CiscoWorks Common Services or other applications. Device groups created using CiscoWorks Common Services are visible in all applications that are in the same management domain, irrespective of whether they are installed on the same or separate servers. Application device groups created by each application group's administration service can be seen from CiscoWorks Common Services and the group user interface of other applications.

You cannot create groups in CiscoWorks Common Services if DCR is in slave mode. However, in the case of applications, you can create groups even if the server on which they are installed is in slave mode. Hence, in a cluster that has several slaves and a master, you need to create common device groups (under CiscoWorks Common Services) only on the master server. The common device group you create on the master will be synchronized across the slave servers. From the CiscoWorks Common Services group administrator UI, you cannot perform Create, Edit, or Delete operations on application groups.

Note: Prior to CiscoWorks LMS 3.2, there is a limit of 100 user-defined groups in Common Services. In CiscoWorks LMS 3.2, this is increased to 200 user-defined groups.

Integration with Cisco Secure Access Control Server for Authentication and Authorization

Cisco[®] Secure Access Control Server (ACS) provides authentication, authorization, and accounting (AAA) services for network devices that function as AAA clients. Cisco Secure ACS supports CiscoWorks LMS applications by providing command authorization and authentication for network users who use the management application to configure managed network devices.

When you change the CiscoWorks LMS login module to Cisco Secure ACS, make sure that:

- CiscoWorks server is added as an AAA client in the Cisco Secure ACS server along with the secret key, and the secret key is entered in the AAA Mode Setup dialog box.
- The username you enter while logging in to CiscoWorks is a valid Cisco Secure ACS username. In ACS mode, authentication takes place from the Cisco Secure ACS server.

Refer to the whitepaper for ACS integration at

http://www.cisco.com/en/US/prod/collateral/netmgtsw/ps6504/ps6528/ps2425/prod_white_paper0900aecd80613f62.html.

Secure Views

Secure Views allows access to a group of devices to be restricted. Secure Views allows filtering of group membership based on the user and the application task context in which a request is made. Filtering will be performed only when operating in ACS mode.

While operating in non-ACS mode, no filtering will be performed. Evaluating a group results in all devices of that group being returned.

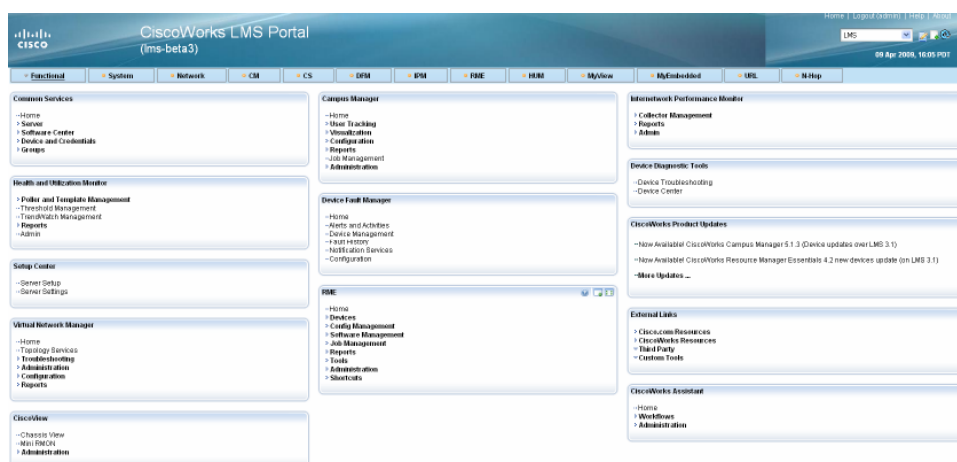
Single Sign-On

With single sign-on (SSO), you can use your browser session to transparently navigate to multiple CiscoWorks servers without performing an authentication with each of them. Communication between multiple CiscoWorks servers is enabled by a trust model. One of the CiscoWorks servers should be set up as the SSO authentication server. The SSO authentication server is called the master, and the SSO regular server is called the slave.

Registering Applications with the CiscoWorks LMS Portal Homepage

The CiscoWorks LMS Portal homepage (see Figure 3) provides a launch point for the applications installed on the server. You can customize it to provide a launch point for applications installed on the remote CiscoWorks LMS servers or other third-party applications. Apart from SSO, this feature provides seamless navigation across multiple servers.

Figure 3. CiscoWorks LMS Portal Homepage



Single Server: All CiscoWorks LMS Applications Installed on the Same Server

For successful deployment of CiscoWorks LMS, some basic configuration needs to be done on each CiscoWorks LMS application. The applications are configured to manage all devices in the DCR. If you do not want all devices in the DCR to be managed by CiscoWorks RME or CiscoWorks DFM, you could turn off the automanage feature of that application and add the devices manually. CiscoWorks Campus Manager is always in automanage mode, and you could limit the scope of device collection by using filters based on IP address or VLAN Trunking Protocol (VTP) domain.

You could use CiscoWorks Campus Manager device discovery to populate devices. The discovery process uses Cisco Discovery Protocol and SNMP to discover the network, so it is important that these two protocols are enabled on devices. You might need to use multiple seed devices to start the discovery process, depending on network configuration, the existence of non Cisco devices in the network, or the need for a faster discovery.

Managing 1500 Devices on the Same Server

License requirement: **CWLMS-3.2-1.5K-K9**

For a single server as a network management platform with all applications on one server, the general scaling recommendation for the CiscoWorks LMS bundle is to manage up to 1500 devices. See Tables 3 and 4 for detailed requirements.

Note: For more detailed hardware requirements, please refer to the LMS server sizing tool at http://www.cisco.com/en/US/products/sw/cscowork/ps2425/prod_presentation_list.html. Based on the number of devices managed and the application bundle chosen by the user, the server sizing tool gives detailed descriptions of the hardware needed for different configurations.

Table 3. Recommended Windows System Requirements

Windows	Recommended System Requirements
CPU	<ul style="list-style-type: none"> • Dual Intel Xeon processor, or • Dual AMD Opteron processor
RAM	4 GB
Disk space	35 GB or more free space for CiscoWorks LMS applications and data
Virtual memory (swap space)	8 GB
Software for Windows	<ul style="list-style-type: none"> • Windows Server 2003 Standard and Enterprise Editions (32bit or 64 bit) • Windows Server 2003 R2 Standard and Enterprise Editions (32bit or 64 bit) • Windows Server 2008 Standard and Enterprise Editions (32bit or 64 bit)

Table 4. Recommended Solaris System Requirements

Solaris	Recommended System Requirements
CPU	Dual Sun UltraSPARC T1/T2/T2+ with 1.3 GHz or above
RAM	4 GB
Disk space	35 GB or more free space for CiscoWorks LMS applications and data
Swap space	8 GB
Software	Solaris 9 and Solaris 10

Managing 5000 Devices on the Same Server

License requirement: **CWLMS-3.2-5K-K9**

For a single server as a network management platform with all applications on one server, you could manage up to 5000 devices (DFM excluded), and that is the highest tested and certified number in the single-server configuration. See Tables 5 and 6 for detailed requirements.

Table 5. Recommended Windows System Requirements

Windows	Recommended System Requirements
CPU	Four Intel Xeon processors, four AMD Opteron processors or equivalent configuration
RAM	8 GB
Disk space	72 GB or more free space for CiscoWorks LMS applications and data
Virtual memory (swap space)	16 GB
Software for Windows	Windows Server 2003 Standard and Enterprise Editions (32bit or 64 bit) Windows Server 2003 R2 Standard and Enterprise Editions (32bit or 64 bit) Windows Server 2008 Standard and Enterprise Editions (32bit or 64 bit)

Table 6. Recommended Solaris System Requirements

Solaris	Recommended System Requirements
CPU	Four Sun UltraSPARC T1/T2/T2+processor-based system
RAM	8 GB
Disk space	72 GB or more free space for CiscoWorks LMS applications and data
Swap space	16 GB
Software	Solaris 9 and Solaris 10

Multi-server Setup

For large deployments, it may be necessary to distribute network management applications across multiple servers for enhancing performance or to accommodate a larger number of network devices. If a single server for CiscoWorks applications cannot handle the load when multiple applications are required, one solution is to distribute the following applications across several servers:

- CiscoWorks Campus Manager
- CiscoWorks DFM
- CiscoWorks RME
- CiscoWorks IPM

CiscoWorks Assistant

The server setup workflow helps you to set up and manage CiscoWorks LMS servers. It helps you to simplify the deployment and setting up of multiple CiscoWorks LMS servers.

Setting up Multi-server Communication

The following terminology is related to multi-server setup:

- **Peer Server:** Remote CiscoWorks LMS server.
- **System Identity User:** Commonly known as a common trust user; used to communicate between peer servers.
- **Peer Server Account:** Used to log in programmatically (using code) and perform certain tasks. You cannot log in through the browser using the Peer Server Account username and password.
- Setup involves the following:
 - **Peer Server Certificate Setup**
CiscoWorks allows you to add the certificate of another CiscoWorks server into its trusted store. This will allow one CiscoWorks server to communicate with another using Secure Sockets Layer (SSL).¹
 - **System Identity User Setup**
Communication between multiple CiscoWorks servers is enabled by a trust model addressed by certificates and shared secrets. The system identity setup should be used to create a “trust” user on slave/regular servers to facilitate communication in multi-server scenarios.
 - **Peer Server Account Setup**
Peer Server Account setup helps you create users who can log in to CiscoWorks servers and perform certain tasks. These users should be set up to enable communication between multiple CiscoWorks servers.

¹ This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. For more details please visit <http://www.openssl.org/>.

A default System Identity User, admin, is created during installation. During the installation, the user should provide the password for the System Identity User. This password can be different from that of the usual administrator user.

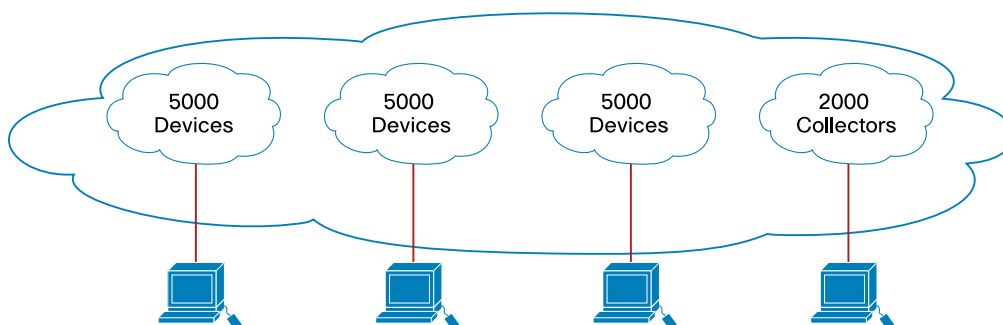
Note: It is recommended that the password be different for the usual administrator user and the System Identity User, admin. Alternatively, you can create another user called sysadmin with system administrator privileges and use that ID for multi-server communication. In the multi-server setup, the same username/password combination (System Identity User, Password, and Peer Server User) should be configured across all servers. If the CiscoWorks LMS server is in ACS AAA mode, this user should be present in the Cisco Secure ACS user database with all privileges.

Applications on Separate Servers Managing a Single Domain

License requirement: **CWLMS-3.2-5K-K9**

Figure 4 shows four management servers being used to manage a network of 5000 devices, with each application from the CiscoWorks LMS bundle distributed across a separate server. The distribution has been done based on the tested scaling limit for each application. The CiscoWorks DFM limit is based on number of ports and CiscoWorks IPM on number of collectors configured on the server. See Tables 7 and 8 for details.

Figure 4. Distributed Deployment Scenario: Single Management Domain



The hardware and software configuration recommendation for each server, namely, CiscoWorks RME, CiscoWorks Campus Manager, CiscoWorks DFM, and CiscoWorks IPM, is similar.

Table 7. Recommended Windows System Requirements

Windows	Recommended System Requirements
CPU	Dual Intel Xeon processor or Dual AMD Opteron processor
RAM	4 GB
Disk space	35 GB or more free space for CiscoWorks LMS applications and data
Virtual memory (swap space)	8 GB
Software for Windows	Windows Server 2003 Standard and Enterprise Editions (32bit or 64 bit) Windows Server 2003 R2 Standard and Enterprise Editions (32bit or 64 bit) Windows Server 2008 Standard and Enterprise Editions (32bit or 64 bit)

Table 8. Recommended Solaris System Requirements

Solaris	Recommended System Requirements
CPU	Dual Sun UltraSPARC T1/T2/T2+ with 1.3 GHz or above
RAM	4 GB
Disk space	35 GB or more free space for CiscoWorks LMS applications and data
Swap space	8 GB
Software	Solaris 9 and Solaris 10

In this deployment scenario, you will use and deploy the master-slave concept of DCR. You could install Server 1 with CiscoWorks Common Services and CiscoWorks RME where DCR could be configured as the master. Server 2 will have CiscoWorks Common Services and CiscoWorks Campus Manager installed, Server 3 will have CiscoWorks Common Services and CiscoWorks DFM installed, and Server 4 will have CiscoWorks Common Services and CiscoWorks IPM installed. In Servers 2, 3, and 4, DCR mode will be configured as slave to Server 1.

The following setup is recommended for the scenario shown in Figure 4:

- Import the Peer Server Certificate from Servers 2, 3, and 4 to Server 1.
- Set up a System Identity User on Server 1, and configure the same user as Peer Server Account on Servers 2, 3, and 4.
- Configure Server 1 DCR as master, and then configure Servers 2, 3, and 4 DCR as slaves of Server 1.
- Enable the default credential sets in DCR, and select the Default Credential Sets while configuring CiscoWorks Common Services device discovery.
- Configure CiscoWorks Common Services to run a complete discovery of the network, which in turn populates the master DCR server.
- Direct syslog messages to the CiscoWorks RME server and SNMP traps to the CiscoWorks DFM server, which could also forward SNMP traps to other trap listeners.
- Integrate all servers with Cisco Secure ACS server for authentication and application and device authorization.
- Configure one of the servers for the CiscoWorks homepage to register applications installed on remote servers.
- Configure SSO across all the servers to help ensure better navigation between applications installed on different servers.

Multiple Instances of CiscoWorks LMS Bundle (Multiple Management Domains)

License requirement: Three **CWLMS-3.2-5K-K9** (Number of licenses required equals number of servers, and in this scenario, three CiscoWorks LMS licenses are required.)

When the network contains more than 10,000 devices, it must be divided into multiple management domains, and multiple servers (or groups of servers) must be deployed. In specific instances, it may be preferable to do so for administrative reasons, even if the numbers do not warrant a division.

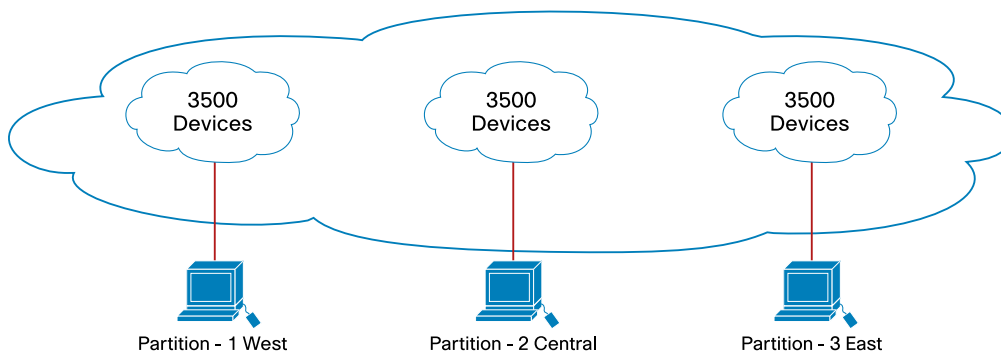
The network could be segmented based on:

- SYS location
- IP address ranges
- LAN and WAN boundaries

Look for administrative logic--separate management teams or regions, or administrative groupings. Make sure there is a clear demarcation of which management workstation is managing which device and vice versa and remember to account for future growth.

Consider the scenario shown in Figure 5, where a network of 10,000 devices is broken into three groups of up to 3500 devices with a separate CiscoWorks LMS server for each segment of the network.

Figure 5. Distributed Deployment Scenario--Multiple Management Domains



Configure each instance of CiscoWorks Common Services to discover the part of the network that it intends to manage. You can achieve this by limiting the discovery by IP range. In this scenario, there is no communication between servers and, thus, no sharing of information. See Tables 9 and 10 for the recommended system requirements.

Table 9. Recommended Windows System Requirements

Windows	Recommended System Requirements
CPU	Four Intel Xeon processors, four AMD Opteron processors, or equivalent configuration
RAM	8 GB
Disk space	72 GB or more free space for CiscoWorks LMS applications and data
Virtual memory (swap space)	16 GB
Software for Windows	Windows Server 2003 Standard and Enterprise Editions (32bit or 64 bit) Windows Server 2003 R2 Standard and Enterprise Editions (32bit or 64 bit) Windows Server 2008 Standard and Enterprise Editions (32bit or 64 bit)

Table 10. Recommended Solaris System Requirements

Solaris	Recommended System Requirements
CPU	Four Sun UltraSPARC T1/T2/T2+ processor based system
RAM	8 GB
Disk space	72 GB or more free space for CiscoWorks LMS applications and data
Swap space	16 GB
Software	Solaris 9 and Solaris 10

In the preceding setup, anyone requiring centralized access to the servers can get it by creating a CiscoWorks Portal private view. Install CiscoWorks Common Services on a server and then register all applications from all the servers in the CiscoWorks Common Services homepage. You can also create an SSO domain for all the servers to help ensure better navigability from the portal to any application. This works better if the same Cisco Secure ACS servers provide AAA services to the servers.

Multiple Instances of CiscoWorks LMS Bundle (Single Domain)

In this scenario, you may want to control the entire administration of servers by creating a single management domain. Multiple management servers (or groups of servers) running multiple applications manage part of the network.

In such a case, one DCR server will be configured as a master server, and all other servers will be slave servers. To set up the environment:

- Turn off automanage mode for CiscoWorks RME and CiscoWorks Campus Manager on each server. CiscoWorks Campus Manager discovers the network and populates the DCR.
- Configure each CiscoWorks Campus Manager application to collect data from part of the network. This can be achieved by implementing data collection filters based on IP address range or VTP domain or by selecting the Include Devices option and the list of devices to be managed from the DCR based on the common device groups.
- On the master server, create common device groups based on IP address range, SNMP Sys location, hostname, and so on, to partition the device list in DCR.
- For each CiscoWorks RME server, select the list of devices to be managed from the DCR based on the common device groups.
- For each CiscoWorks DFM server, select the autoimport filters and select the device groups to be managed in each of the servers.

Syslog messages and SNMP traps will be directed to the respective CiscoWorks RME and CiscoWorks DFM servers.

Centralized CiscoWorks RME Server

License requirement: One **CWLMS-3.0-10K-K9**

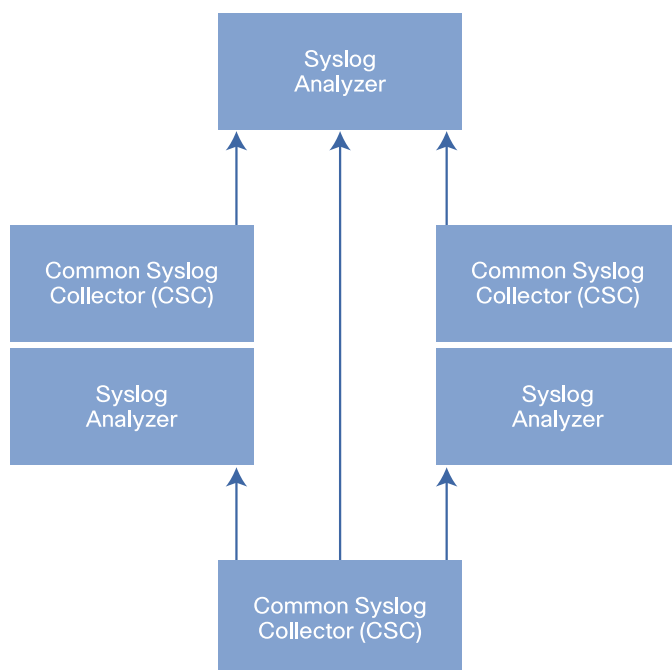
In this scenario, a centralized CiscoWorks RME server is used because of better scalability compared to other applications in CiscoWorks LMS. Assume that the customer has 10,000 devices and each server manages a set of devices. There is a centralized server that helps manage the entire set of devices and can be used as a backup server.

Before discussing details of the centralized server, it is important to understand the new concept of a distributed syslog collector and analyzer introduced in CiscoWorks RME.

Distributed Syslog Collection

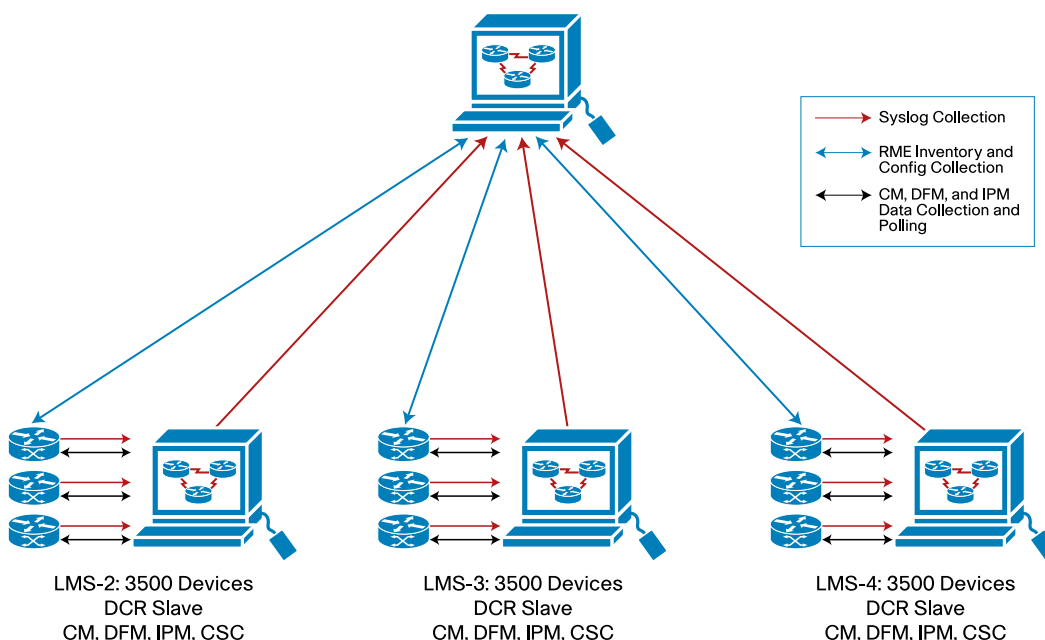
The syslog application has the following features (see Figure 6):

- **Common Syslog Collector (CSC):** Helps in receiving, validating, filtering, and forwarding syslogs.
- **Syslog Analyzer:** Responsible for receiving syslogs from the collector, invoking automated actions and storing them in the database, and generating reports.
- **Collectors and analyzers:** Help in balancing the syslog processing load by making syslog servers subscribe to syslog collectors.
- **Easy time zone support:** Supports any time zone by allowing you to edit the configuration file.
- **Drop/keep filtering:** Allows you to keep or drop syslogs. The enhanced filtering capabilities allow you to consider interfaces as well.
- **Import/export:** Helps in import and export of automated actions and message filters in syslogs.

Figure 6. Distributed Syslog Collection

This central CiscoWorks RME design provides a single reporting server for inventory, configurations, and syslogs. In this scenario, there will be multiple CiscoWorks LMS servers that will manage parts of the network, and there will be one CiscoWorks RME server that will manage the enterprise with customized policies. The policies will allow scalability up to the maximum permitted number of devices in the network.

A central CiscoWorks RME server could be populated with all the network devices by importing the device list from a central network management system (NMS), such as HP OpenView Network Node Manager, or export/import the device list from each local CiscoWorks LMS server. The inventory and configuration archive collection will be configured with multiple jobs, each containing a set of devices. Each device will be configured to send the syslog to the respective local CiscoWorks RME server where the device is managed. The syslog analyzer on the central CiscoWorks RME server will subscribe to the syslog collector of each of these CiscoWorks RME servers with central log filters. See Figure 7.

Figure 7. Centralized CiscoWorks RME Server

Dividing Large Networks into Smaller Management Domains

Customers may have multiple groups of network managers with responsibilities that may be totally different or may overlap. In addition, managed service providers may want to manage multiple client networks in a segregated manner from a single server.

You could logically achieve this segmentation by integrating the CiscoWorks LMS server with Cisco Secure ACS for authentication and authorization. With Cisco Secure ACS integration, users will be able to create custom roles and network device groups (NDGs) that only certain users have access to.

Note: Customer A can see devices and configurations for Network A but not for Customer B. Customer A will only be able to see Customer B group names (for example, an Object Grouping Services [OGS] group named Network B).

Redundant-Server Scenario

CiscoWorks LMS does not support high availability by design, but this could be achieved by either using the Veritas solution mentioned before or installing multiple identical servers. CiscoWorks LMS provides features that help optimize this scenario. In this scenario, one of the servers is designated as “hot” and will be used primarily for managing, and the other will be used as a standby server. Install all the applications on both servers and configure the hot server as DCR master and the standby server as DCR slave. This way, the device list gets synchronized between hot and standby. The hot server will be polling at each desired polling interval, while the standby server will be in either of the following states:

- No polling (keep prepared documents nearby as a reminder of what options need to be quickly turned on manually in the event of a failure)
- Polling at a lengthened interval (that is, four to five times the hot server interval; shorten the polling intervals upon failure)
- Polling intervals can be configured for the following parameters:
 - CiscoWorks Campus Manager data collection schedule
 - User tracking discovery schedule

- CiscoWorks RME system inventory polling and configuration archive polling
- CiscoWorks DFM device polling

Syslog analyzer administration supports exporting and importing of filter and automated action configuration. Export syslog filter data from the hot server to a flat file and import the same into the standby server. Perform the same tasks for syslog automated actions as well, but keep them in a suspend mode.

Another option is to shut down all the services on the standby server and regularly import CiscoWorks LMS backup data from the hot server. (Make sure that the active and standby servers have the same name.) When the hot server goes down, change the IP address of the standby server to that of the hot server, and start all the CiscoWorks LMS services.

Recommendations for Improved Usability and Performance

It is very important to find the baseline values for your environment before you set up the final configurations and polling intervals. Some application performance numbers have been documented later in this paper. The test results are based on testing against a simulated network of 5000 devices. Actual values in your environment could vary based on speed and latency of your network along with other factors. Even a Domain Name System (DNS) can vary the results.

Device Discovery

It is recommended that you set up the discovery schedule to a less frequent one and choose the time most appropriate to you. (This process is required to find the new devices added to your network.) Select the discovery parameters most suitable to your environment so that it could speed up the discovery process, and discover and populate correct values.

- Choose Use Loopback Address if loopback addresses are configured on the devices and you want those addresses to be the management IP address in CiscoWorks LMS.
- Choose Use Reverse DNS Lookup only if DNS is configured in your environment for network devices. Otherwise, deselect that option to speed up the discovery process.
- Choose Use Resolve by Sysname or Resolve by Name depending on the DNS configuration. If you have configured the management IP address of the device using any of the above settings, select the corresponding checkbox.

CiscoWorks Campus Data Collection

The data collection is configured to run every four hours starting at midnight. Run discovery manually once to determine an appropriate polling cycle. Four hours is enough for smaller networks, but larger networks can take long for the initial poll. The subsequent polls will be shorter in duration, but you should still give it a 20 percent buffer. For example, if it took four hours to poll the whole network the first time, you could set the frequency to five hours to make sure that there is no overlapping between the two consecutive data collection processes.

User Tracking Discovery

Configure the time so that two consecutive schedules do not overlap. Filter subnets for which you do not want to perform end-host discovery or subnets where no end hosts are present. Configure subnets that you want excluded from doing a ping sweep before the discovery process.

CiscoWorks DFM Polling Parameters and Threshold

Default CiscoWorks DFM polling and threshold parameters are configured for CiscoWorks DFM system-defined groups; however, you need to look at these configurations based on critical and noncritical devices in your network.

To accomplish this:

- Start by adding devices to the customizable groups under CiscoWorks DFM user-defined groups. By default, no device belongs to customizable groups.
- Set the priority of the customizable group. By default, customizable groups have a lower priority than system-defined groups. Change the priority based on group members (critical or noncritical).
- Change the polling parameters for the customizable device groups to larger or smaller values. You could even disable polling based on devices in that group.

CiscoWorks RME

During CiscoWorks RME installation, system jobs are created for inventory collection and polling, the default schedules being weekly and daily, respectively. In case of configuration archive management, system-level periodic configuration collection and polling are disabled by default.

In CiscoWorks RME, you can create user-defined jobs for inventory polling and collection, and configuration collection and polling on a set of devices selected as part of the job creation process. You should consider this option when servers manage a large number of devices. In this case, data collection and job creation will be much easier if you have created well-defined common device groups.

Note: One problem with this approach is that when new devices get added to the system, you have to modify the jobs to add the new devices. This modification helps update the job to include the new device list.

CiscoWorks RME can also be configured to periodically poll configuration MIB variables on devices that support MIBs. This will be carried out according to a specified schedule to determine whether the startup or running configuration file has changed. If it has, CiscoWorks RME will retrieve and archive the most current configuration file from the device. Polling uses fewer resources than full scheduled collection because configuration files are retrieved only if the configuration MIB variable is set.

Change the execution policy in default job policies for archive management and network configuration to parallel execution (choose **Resource Manager Essentials → Admin → Config Mgmt → Config Job Policies**). Remove protocols that are not used in your environment, and prioritize them.

General Observations

The UI performance of the application client can be improved by using device groups when executing application tasks, especially when a single server is managing a large number of devices.

When you configure systems to manage a large number of devices, consider the following:

Administrative Tips

- When CiscoWorks LMS is configured in ACS mode, the fallback user from Cisco Secure ACS to CiscoWorks local will have only Help Desk privileges. However, users can change the login mode to CiscoWorks local security by choosing **Server → Security → AAA Mode Setup → Non-ACS Change**.
- On the Windows platform, Terminal Server is supported only if Windows is configured for Remote Desktop Administration (Windows 2003).
- CiscoWorks and system log files could grow to an unmanageable size over a period of time. It is very important to trim or rotate these files periodically. You could use the Logrot utility (part of the CiscoWorks Common Services application) to manage these files. Following are some of the features of the Logrot utility:
 - Not limited to rotating only CiscoWorks log files but can be used to rotate any file
 - Can be run using the command **NMSROOT/bin/perl NMSRoot/bin/logrot.pl**

- Can be configured and scheduled from GUI at **Server → Admin → Log rotation**.
- Can rotate logs while CiscoWorks is running
- Can optionally archive and compress rotated logs
- Can be configured to rotate logs only when they have reached a certain size
- Has a built-in configuration that makes adding new files very easy
- Is typically run from UNIX cron or Windows AT. However, before automating Logrot, you should verify that it runs on demand.
- Command-line interface (CLI) commands:
 - **cmexport** is the CiscoWorks Campus Manager CLI for exporting user tracking, Layer 2 topology, and discrepancy data details into XML format.
 - Remote invocation through servlet-based **cmexport** and **utexport** can also be used in CiscoWorks Campus Manager, the former command for exporting Layer 2 topology details and discrepancy and the latter for user tracking.
 - **cwcli config** is the configuration command-line tool of CiscoWorks RME. The **cwcli netconfig** command allows you to use NetConfig from the command line.
 - **cwcli export** is a command-line tool that provides servlet access to inventory, configuration, and change audit data. This can be used for generating inventory, configuration archive, and change audit data for devices in CiscoWorks RME.

Extracting Data from CiscoWorks LMS Servers for Centralized Reporting

CiscoWorks Campus Manager and CiscoWorks RME support export of data in XML format. If you have multiple instances of any of these applications, you could use this facility to develop consolidated reports.

From this version, LMS 3.2, direct access to the LMS database is also supported, which offers users great flexibility in creating applications on their own. Initially only a limited set of table views is supported. More will be open in future releases.

CiscoWorks RME Data Extracting Engine

CiscoWorks RME Data Extracting Engine (DEE) is a utility that allows customers to extract data for devices managed by CiscoWorks RME from the inventory database, configuration archive, and change audit data. This tool supports the following features:

- Generating inventory data in XML format: The tool has servlet access and a command-line utility that can generate inventory data for devices managed by the CiscoWorks RME server.
- Generating configuration data in XML format: The tool generates the latest configuration data from the configuration archive in XML format. Elements in the XML file are created at the configlet level in the current configuration archive.
- Generating change audit data in XML format: The tool uses the existing change audit log data and generates the change audit log data in XML format.

The Data Extracting Engine offers a great opportunity for customers to take advantage of the information stored in CiscoWorks RME. The XML-based data along with web-based access to data allows CiscoWorks RME users to:

- Integrate their applications tightly with CiscoWorks RME
- Consolidate information from multiple CiscoWorks RME servers in a single location
- Maintain custom asset-management solutions

CiscoWorks Campus Manager Data Extracting Engine

CiscoWorks Campus Manager DEE is a utility that allows users to extract information available in CiscoWorks Campus Manager. CiscoWorks Campus Manager DEE provides servlet access and a command-line utility to extract information on devices discovered by the CiscoWorks Campus Manager Asynchronous Network Interface (ANI) server. The information that can be extracted using CiscoWorks Campus Manager DEE is:

- User tracking data in XML format: DEE generates user tracking data for devices discovered by CiscoWorks Campus Manager.
- Layer 2 topology data in XML format: Generates the latest Layer 2 topology data including information on neighbor devices.
- Discrepancy data in XML format: CiscoWorks Campus Manager discrepancy APIs are used to retrieve the latest discrepancy data from the CiscoWorks Campus Manager ANI server.

Open Database Schema Support in CiscoWorks LMS 3.2

CiscoWorks LMS uses a proprietary database based on Sybase. In previous versions, there is no support for direct database access. From LMS 3.2, database access is supported. Following is a list of exposed database views by applications:

- Common Services
 - Network_Devices
 - Job_Details
- Campus Manager
 - End_Hosts
- Device Fault Manager (DFM)
 - Fault_Alert_History
 - Fault_Event_History
 - Fault_Event_Details
- Resource Manager Essentials (RME)
 - Device_Inventory
 - Module_Inventory
 - Port_Inventory
 - Processor_Inventory
 - Memory_Inventory
 - Device_Credentials_Status
 - Device_Inventory_Collection_Status
 - Device_Config_Archive_Status
 - Change_Audit_History
 - Syslog
 - Internetwork Performance Monitor (IPM)

Refer to

http://www.cisco.com/en/US/docs/net_mgmt/cisoworks_internetwork_performance_monitor/4.1/user/guide/IPM_db_4.1.html

For how to setup Open Database Connectivity (ODBC) to the database and for details of the database schema, please refer to the document "Open Database Schema Support in LMS 3.2" included on the DVD.

Application Performance Numbers

CiscoWorks Common Services Performance Data and Recommendations

Device Discovery for 5000 Devices

- Time: ~15 minutes
- Average memory: 78 MB
- Average CPU usage: 12 percent
- Device Discovery
 - NMSROOT/conf/csdiscovery/CSDiscovery-config.xml
 - NMSROOT/campus/etc/cwsi/discoverysnmp.conf--for SNMP credentials, timeout, and retry values

CiscoWorks Campus Manager Performance Data and Recommendations

CiscoWorks Campus Manager Device Data Collection for 5000 Devices

- Time: ~4 hours
- Average memory: 670 MB
- Average CPU usage: 46 percent
- Occupied heap: ~933 MB

User Tracking Discovering 5000 Devices and 100,000 EndStations (Hosts)

- Time: ~1 hour 26 minutes
- Average memory: 520 MB
- Average CPU usage: 35 percent

CiscoWorks Campus Manager Property Files

- Data collection and user tracking
 - NMSROOT/campus/etc/cwsi/ANIServer.properties
 - NMSROOT/campus/etc/cwsi/datacollectionsnmp.conf--for SNMP timeout and retry values
- Increase the heap for the ANI server from -Xmx1024m to -Xmx1280m
- ANI.resolve is true by default, so DNS should be properly set up with both forward and reverse name lookups to reduce user tracking data collection time.

CiscoWorks RME Performance Data and Recommendations

Inventory Collection: Single Job with 5000 Devices

- Time: 1 hour 30 minutes
- System memory utilization: 1.6 GB
- CPU usage: 10–30 percent
- Recommended: Collection once a week; polling daily

Configuration Archive: 5000 Devices with 2 KB Configuration File Using Telnet Protocol (Both Startup and Running Configurations)

- Time: 5 hours
- System memory utilization: 1.6 GB
- CPU usage: 10–30 percent

Configuration Archive: 5000 Devices with 2 KB Configuration File Using TFTP Protocol (Both Startup and Running Configurations)

- Time: 3 hours
- System memory utilization: 1.6 GB
- CPU usage: 10–30 percent

For better performance, choose only supported protocols in the Fetch Protocol list. For example, if RCP, SCP, and HTTPS are not supported or configured, do not select those protocols.

NetConfig: Four Cisco IOS Software Commands and 5000 Devices in a Single Job

- Time: 5 hours
- System memory utilization: 1.6 GB
- CPU usage: 10–30 percent
- Download: Sequential and parallel; use the parallel option to update large number of devices in a single job
- Concurrent jobs

Syslog

- Can validate and filter 200 syslogs per second
- Can forward and store 50 syslogs per second
- Can take one action per second
- Can validate and filter 1000 syslogs per second burst for an hour

Recommendations:

- Define backup policy
 - To avoid losing syslog messages when they get purged from the database, specify the file to which syslogs should be copied before deletion.
- Define purge policy
 - To avoid the database growing to a large size, set the purge schedule and specify the age of the syslogs to be deleted.
 - Default value is seven days and there is no upper limit for number of days, but the syslog database has a limit of 1 million managed messages and 50,000 unexpected messages in the database.

- Purge immediately
 - Use the Force Purge option to instantly delete all the syslog records older than a certain number of days.

Multi-server Configuration Example

Scenario

Currently Customer X is managing about 5000 devices and wants to deploy CiscoWorks RME, CiscoWorks Campus Manager, CiscoWorks DFM, and CiscoWorks IPM for managing its network.

The servers that can be deployed in the customer network are:

Solaris

- SUN V240, 280R, V440, 480R, or V490, with two processors and 4 GB RAM. (Check out the details of hardware requirements using the LMS server sizing tool.)
- If there are two drives, try to put a swap on each disk and put /opt on one disk and /var on the other. That helps split up the load.
- ZFS is recommended to be a solution for scalable storage.
- Sample partition for a server with 72 GB hard drive:
 - / 4096 MB (4 GB; anything not allocated in the other partitions comes from /, so make it a little bigger than recommended)
 - /var 16384 MB (16 GB; syslog, device images, config files, and so on get stored here)
 - /opt 32768 MB (32 GB; application goes here /opt/CSCOPx)
 - swap 8192 MB (8 GB; conforms to the 8 GB swap rule)
 - /usr 8192 MB (8 GB; in case you get some data in /usr/local)
 - /export/home 4096 MB

Windows

- Intel Dual Xeon processor with 4 GB RAM (Check out the details of hardware requirements using the LMS server sizing tool.)

It is recommended to have CiscoWorks RME, CiscoWorks Campus Manager, CiscoWorks DFM, and CiscoWorks IPM applications deployed on separate servers. In this case, the customer must have four servers. Make sure that name resolution (DNS) is configured properly so that each server can access the other server by hostname rather than IP address. Install CiscoWorks Common Services and one of the applications on each server. During CiscoWorks Common Services installation, give the same password for System Identity User across all servers. In this case admin will be your System Identity User.

Note: If you do not want to use admin as the System Identity User, create a local user with system administrator privileges on all the servers and assign that user as a System Identity User. (Choose **Common Services** → **Server** → **Security** → **System Identity Setup**.)

Once the installation is completed, verify that the self-signed certificate has the hostname (name resolvable) that you are going to use in multi-server communication, and if not, re-create the certificate. In the CiscoWorks homepage, choose **Common Services** → **Server** → **Security** → **Certificate Setup**. See Figure 8.

Figure 8. Certificate Setup

Common Services

Home | Server | Software Center | Device and Credentials

Security | Reports | Admin | Home Page Admin

You Are Here > Server > Security > Single-Server Management > Certificate Setup

TOC

- Single-Server Management
 - Browser-Server Security Mode Setup
 - Local User Policy Setup
 - Local User Setup
 - Certificate Setup**
- Multi-Server Trust Management
 - Peer Server Account Setup
 - System Identity Setup
 - Peer Server Certificate Setup
 - Single Sign-On Setup
- AAA Mode Setup
- Cisco.com Connection Management
 - Cisco.com User Account Setup
 - Proxy Server Setup

Certificate Setup

Self Signed Certificate Setup

Country Name:

State or Province:

City (Eg: SJ):

Organization Name:

Organization Unit Name:

Server Name*:

Email Address:

Note: Server Name (Hostname or IP Address or FQDN) is the mandatory field. This is required to create the certificate. Ensure that the server name is same as the peer hostname that is used for setting up peer relations. Entering other fields are optional. However, it is desirable to provide all input fields for certificate regeneration.

Apply Cancel

The next step is to import the server certificate from other servers into its trust store. In the CiscoWorks homepage, choose **Common Services** → **Server** → **Security** → **Peer Server Certificate Setup**. Give the IP address or hostname of each server and import the servers into the trust store. Import certificates from each other so that later you could make any server as an SSO or DCR master server. See Figure 9.

Figure 9. Peer Server Certificate

Common Services

Home | Server | Software Center | Device and Credentials

Security | Reports | Admin | Home Page Admin

You Are Here > Server > Security > Multi-Server Trust Management > Peer Server Certificate Setup

TOC

- Single-Server Management
 - Browser-Server Security Mode Setup
 - Local User Policy Setup
 - Local User Setup
 - Certificate Setup
- Multi-Server Trust Management
 - Peer Server Account Setup
 - System Identity Setup
 - Peer Server Certificate Setup**
 - Single Sign-On Setup
- AAA Mode Setup
- Cisco.com Connection Management

Peer Server Certificate

Peer CiscoWorks Certificate

IP address/hostname of peer CiscoWorks Server:

SSL(HTTPS) Port of peer CiscoWorks Server:

OK Cancel

CiscoWorks LMS Portal

The CiscoWorks homepage will help cross-launch applications among multiple servers from a single homepage. If SSO is configured, users could launch applications on different servers from the same homepage without authenticating each server. To configure SSO:

1. Configure one of the servers as the SSO master server and the others as SSO slave servers.
2. In the CiscoWorks homepage, choose **Common Services → Server → Security → Single Sign-On**, change the mode of one server to master and of the other three to slave, and enter the master server's hostname in the dialog box. See Figure 10.

Figure 10. SSO Setup

Note: In non-ACS mode, SSO provides authentication across servers, and authorization is done through the local user database. If the user is not present in the local user database, only the Help Desk role is assigned. In such a situation, create users with a corresponding authorization role on all the servers. To avoid duplication of effort, you could manually synchronize the “cwpass” file from the server where you created the users and other servers.

To use Cisco Secure ACS for CiscoWorks LMS security:

1. In the CiscoWorks homepage, choose **Common Services → Server → Security → AAA Mode Setup**.
2. Enter the primary Cisco Secure ACS server IP address, Cisco Secure ACS administrator username and password, and shared secret key (which is the secret key used to communicate between the CiscoWorks LMS and Cisco Secure ACS servers; this needs to be defined while adding the AAA client in the Cisco Secure ACS server).
3. Select **Register all installed applications with Cisco Secure ACS** to register all the installed applications with the Cisco Secure ACS server. See Figure 11.

Figure 11. AAA Mode Setup

Repeat the same steps on all the servers, and once finished, restart the Daemon Manager.

On the Cisco Secure ACS server, add the CiscoWorks LMS servers as AAA clients and specify the same secret key. See Figure 12.

Figure 12. Cisco Secure ACS: Add AAA Client

Add a user in the Cisco Secure ACS server with the same username and password as that of the System Identity User and assign system administrator privileges to that user. Configure Cisco Secure ACS users with the necessary privileges to access the CiscoWorks LMS server. You could do this at the group level or user level.

For complete details on ACS integration, refer to the whitepaper “CiscoWorks LMS Integration with Cisco Secure ACS” at http://www.cisco.com/en/US/prod/collateral/netmgtsw/ps6504/ps6528/ps2425/prod_white_paper0900aecd80613f62.html.

Now you could register all applications installed on multiple servers to one of the servers and that becomes your CiscoWorks LMS portal. You could launch any application registered with the portal without authentication at each server where applications are installed. Select **Common Services** → **HomePage** → **Application Registrations**, choose **Import from Other** servers, and enter the remote server details. See Figure 13.

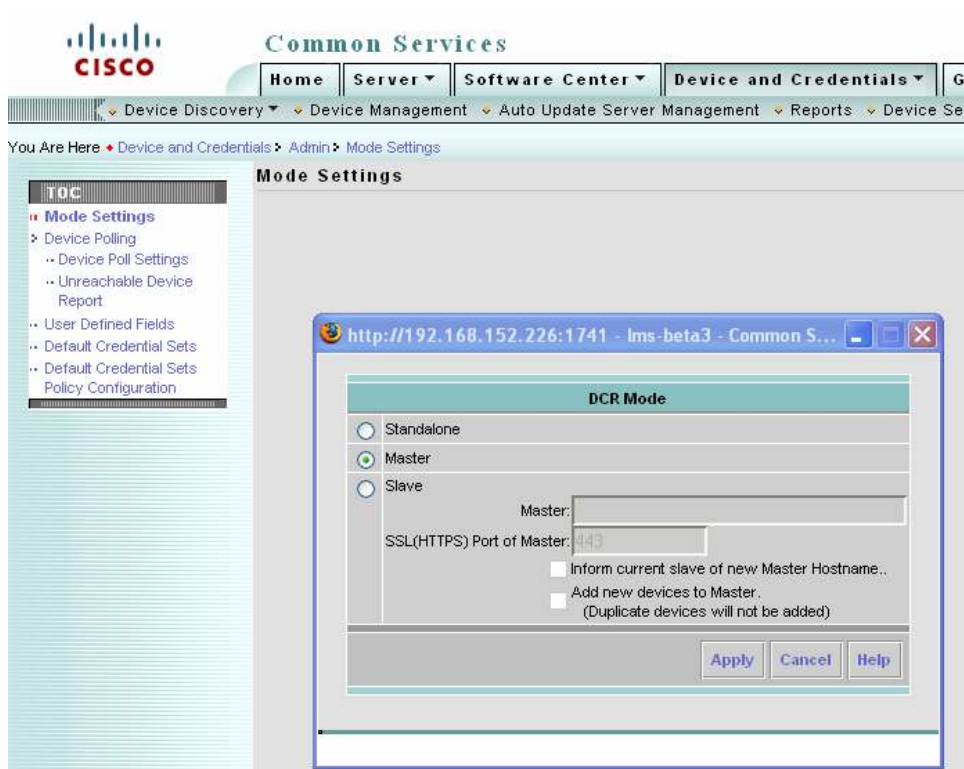
Figure 13. Import Registration

The screenshot displays the CiscoWorks LMS Administration interface. At the top, the Cisco logo is visible on the left, and the text 'Common Services' is centered. Below this is a navigation bar with tabs for 'Home', 'Server', 'Software Center', and 'Device and Credentials'. The 'Server' tab is active, and its sub-menu is expanded to show 'Security', 'Reports', 'Admin', and 'Home Page Admin'. The 'Home Page Admin' sub-menu is further expanded to show 'Application Registration'. The main content area is titled 'Import Registrations' and features a progress bar with four steps: 1. Choose Location (checked), 2. Import Registration from Server (selected), 3. Applications Imported, and 4. Import Registration Summary. Below the progress bar is a table titled 'Import Server's Attributes' with three rows: 'Server Name' with the value 'LMS-Server2', 'Server Display Name' with the value 'lms@SanJose', and 'SSL Port' with the value '443'.

Repeat the registration process for all the servers. Once you have finished, your CiscoWorks LMS Portal page appears, and the remote CiscoWorks LMS servers show up in the portal.

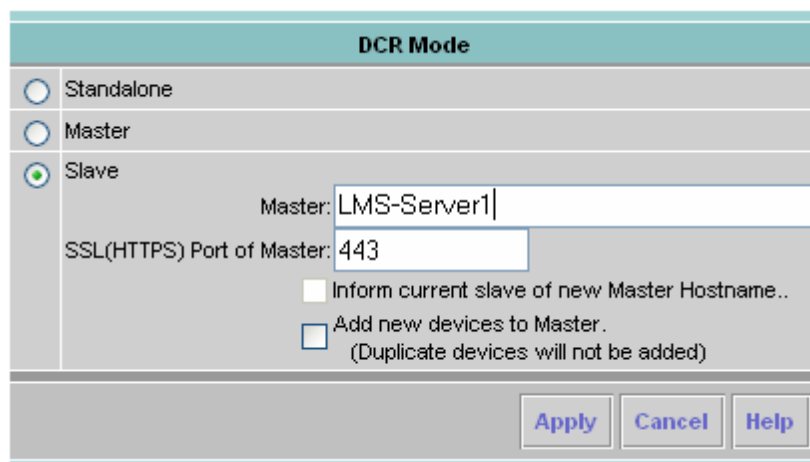
The next step is to configure DCR. Since you want a single device management domain, configure the server where CiscoWorks RME is installed as DCR master server and the rest of the servers as DCR slave servers. In the CiscoWorks homepage, choose **Common Services** → **Device and Credentials** → **Admin**, and change the mode setting on the CiscoWorks RME server to Master as shown in Figure 14.

Figure 14. DCR Mode



For other servers, change the DCR mode to Slave and enter the master CiscoWorks RME server's hostname as the master server's hostname. See Figure 15.

Figure 15. DCR Mode



Summary

This white paper provides an outline and recommendations for deploying CiscoWorks LMS server. It also tries to highlight some of the best practices related to the deployment of large-scale networks and makes the user aware of the scaling characteristics of the various individual CiscoWorks products. Your implementation may vary--watch system resource usage, and plan accordingly. Distribute products across multiple workstations as needed for optimum performance. Be aware of the means to maximize performance and usability that are already available in the tools.



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

CCDE, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks, and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0903R)