Release Notes for Cisco Wireless Control System 6.0.181.0 for Windows or Linux

February 2010

These release notes describe open caveats for the Cisco Wireless Control System 6.0.181.0 for Windows or Linux, which comprises part of the Cisco Unified Wireless Network Solution (Cisco UWN).

The Cisco Wireless Control System is hereafter referred to as *Cisco WCS*.

Contents

These release notes contain the following sections.

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2010 Cisco Systems, Inc. All rights reserved.

Cisco Unified Wireless Network Solution Components

The following components are part of the Cisco UWN Solution and are compatible in this release:

- Operating system (Wireless LAN Controller and Cisco Aironet Lightweight Access Point)
- Cisco Wireless Control System (Cisco WCS)
- Cisco Mobility Services Engine
- Cisco WCS Navigator
- Cisco 2700 Series Location Appliance
- Cisco 2000 Series Wireless LAN Controllers
- Cisco 2100 Series Wireless LAN Controllers
- Cisco 4400 Series Wireless LAN Controllers
- Cisco 5500 Series Wireless LAN Controllers
- Catalyst 3750G Wireless LAN Controller Switches
- Cisco Wireless Services Modules (WiSMs) for Cisco Catalyst 6500 Series Switches
- Cisco WLAN Controller Network Modules for Cisco Integrated Services Routers
- Cisco Aironet 1000, 1100, 1130, 1140, 1200, 1230, 1240, 1250, 1310, 1500, and 1524 Series Lightweight Access Points
- Cisco Aironet 1310 and 1410 Bridges
- Cisco Aironet Access Points running Lightweight Access Point Protocol (LWAPP) or Control and Provisioning of Wireless Access Points protocol (CAPWAP)

Requirements for Cisco WCS

The following server hardware and software is required to support Cisco WCS for Windows or Linux.

Hardware Requirements for Server

Cisco WCS can be run on a workstation or server, and access points can be distributed unevenly across controllers.

- High-end server—Supports up to 3,000 Cisco Aironet lightweight access points, 1,250 standalone access points, and 750 Cisco wireless LAN controllers.
  - 3.16-GHz Intel Xeon Quad processor.
  - 8-GB RAM.
  - 200 GB minimum free disk space is needed on your hard drive.
- Standard server—Supports up to 2,000 Cisco Aironet lightweight access points, 1,000 standalone access points, and 450 Cisco wireless LAN controllers.
  - 3.2-GHz Intel processor.
  - 2.13-GHz Intel Quad Core X3210 processor.
  - 2.16-GHz Intel Core2 processor.

  - 4-GB RAM.
  - 80 GB minimum free disk space is needed on your hard drive.
- Low-end server—Supports up to 500 Cisco Aironet lightweight access points, 200 standalone access points, and 125 Cisco wireless LAN controllers.
  - 3.06-GHz Intel processor.
  - 1.86-GHz Intel Dual core processor.
  - 2-GB RAM.
  - 50 GB minimum free disk space is needed on your hard drive.

Note For all server levels, AMD processors equivalent to the listed Intel processors are also supported.

Note The free disk space listed is a minimum requirement, but several variables (such as backups) impact the disk space.

Operating Systems Requirements

The following operating systems are supported:

- Windows 2003/SP2 and Windows 2003 R2/SP2 32-bit installations with all critical and security Windows updates installed.

  Windows 2003/SP2 64-bit installations are not supported. A 32-bit operating system running on a 64-bit capable hardware is supported.

  Windows 2003 32-bit installations provide support for up to 64 GB of RAM provided Physical Address Extension (PAE) is enabled. Refer to Windows documentation for instructions on enabling this mode.
- Red Hat Linux Enterprise Server 5.X 32-bit operating system installations.

  Red Hat Linux Enterprise Server 5.X 64-bit operating system installations are not supported. A 32-bit operating system running on a 64-bit capable hardware is supported.
- Windows 2003 and Redhat Linux version support on VmWare ESX version 3.0.1 and above with either local storage or SAN over fiber channel.

  Individual operating systems running WCS in VmWare must follow the specifications for the size of WCS you intend to use.

Client Requirements

The Cisco WCS user interface requires Internet Explorer 7.0 with the Flash plugin or Mozilla Firefox 3.

Note Cisco recommends Mozilla Firefox 3.0 for best performance.

Note Internet Explorer 6.0 is currently supported, but support will be removed in a future release.

Using a web browser running on Windows 2003 to access the WCS web GUI is not recommended because recommended Windows 2003 security settings may cause browsing problems.

The client running the browser must have a minimum of 1 GB of RAM and a 2-GHz processor. The client device should not be running any CPU or memory-intensive applications.

Note The minimum screen resolution that is recommended for both WCS and Navigator use is 1024 x 768 pixels.

Wireless LAN Controller Requirements

Cisco WCS 6.0.181.0 supports management for controllers running the following software releases:

- 4.2.61.0
- 4.2.99.0
- 4.2.112.0
- 4.2.130.0
- 4.2.176.0
- 4.2.205.0
- 4.2.207.0
- 5.1.151.0
- 5.1.163.0
- 5.2.157.0
- 5.2.178.0
- 5.2.193.0
- 6.0.182.0
- 6.0.188.0
- 6.0.196.0

Location Server, Mesh, and MSE

Cisco WCS 6.0.181.0 supports management for the following location server, mesh, and mobility service engine (MSE) software:

- MSE release and Context Aware Software 6.0.103.0

  Note Client and tag licenses are required in order to retrieve contextual (such as location) information within Context Aware Software. See the *Release Notes for Mobility Service Engine for Software Release 6.0* for more information.

- Location server 6.0.101.0

Note See the *Release Notes for Location Appliance Software Release 6.0.101.0* for more information.

- WLC running mesh release 4.1.192.35M and later.

WCS on WLSE Appliance

Cisco WCS on a WLSE appliance supports up to 1,500 Cisco Aironet lightweight access points and 161 Cisco wireless LAN controllers. The required processor is a 3.16 GHz Intel Xeon processor (or AMD equivalent) with 3 GB of RAM and 38 GB of free hard drive space.

The Windows operating system is not supported with the WCS on the WLSE appliance.

Finding the Software Release

To find the software release Cisco WCS is running, refer to the *Cisco Wireless Control System Configuration Guide*. If WCS is already installed and connected, verify the software release by choosing **Help > About the Software**.

Upgrading to a New Software Release

The Cisco WCS release must be the same or more recent than the controller software release. Upgrade the Cisco WCS first to prevent any unexpected problems. Cisco WCS supports database upgrades only from the following official Cisco WCS releases:

- 4.2.62.0
- 4.2.62.11
- 4.2.81.0
- 4.2.97.0
- 4.2.110.0
- 4.2.128.0
- 5.1.64.0
- 5.1.65.4
- 5.2.110.0
- 5.2.130.0
- 5.2.148.0
- 6.0.132.0
- 6.0.170.0

Note All 5.2.x releases posted after 5.2.148.0 will not be eligible for upgrade to release 6.0.181.0.

Upgrading WCS

This section provides instructions for upgrading WCS on either a Windows or Linux server. It handles the steps you would normally follow to accomplish a manual upgrade (shut down WCS, perform a backup, remove the old WCS version, install new version, restore the backup, and start WCS). If you choose to use the installer, it searches for any previous WCS versions.

Note You must have software release 4.1.91.0 before you can automatically upgrade to 4.2.

If you choose to use the easy upgrade process, it provides error checking at each step and gives an informative message if an error causing an exit occurs. An upgrade-*version*.log is also produced and provides corrective measures.

Note For steps on upgrading WCS in a high availability environment, refer to Chapter 14 of the *Cisco Wireless Control System Configuration Guide*.

Using the Installer to Upgrade WCS for Windows

Follow these steps to upgrade WCS (on a Windows platform) using the automated upgrade:

Step 1 Insert the Windows Cisco WCS CD into the CD-ROM drive and double click the WCS-STANDARD-K9-6.0.X.Y.exe file where 6.0.X.Y is the software build. If you downloaded the installer from Cisco.com, double click the WCS-STANDARD-WB-K9-6-0-X-Y.exe file that you downloaded to your local drive.

Step 2 The Install Anywhere window appears and prepares the system for installation. After a few seconds, the Introduction window appears, followed by the license agreement window. You must click the "I accept the terms of the License Agreement" option to continue.

Step 3 At this point, the install wizard detects whether a previous version of WCS is installed and specifies whether the current version is eligible for an automated upgrade. If your most recent WCS version cannot participate in the automated upgrade, you receive such a notice. You must then choose **Install** and must switch to the manual upgrade. (Refer to the *WCS Software Configuration Guide* for manual upgrade instructions.) If your WCS version is eligible for an automated upgrade and the previous qualifying version of WCS is detected, choose **Upgrade** and continue to Step 4. This method is preferred.

Step 4 Several of the values from the previous installation are retained as part of the upgrade. These include the following:

- the ports
- the root password
- the root FTP password
- the TFTP server file location
- the FTP server file location
- the multi-homed server interfaces

Step 5 Choose a folder in which to install the Cisco WCS at the Choose Install Folder window. It must be a different location than the previous installation. Click **Next** to continue.

Step 6 Choose a folder location in which to store the shortcuts. It must be a different location than the previous installation.

Step 7 Continue to follow the prompts that appear. You are notified when the system checks for required space, uninstalls previous versions, backs up files, restores, and so on. A prompt appears asking if you are ready to start WCS as a service. Click **Yes**.

Note The upgrade log is located in the standard log directory (\webnms\logs) if the automated upgrade completes. If the automated upgrade did not complete, the upgrade log is located in the user home directory.

Note If WCS is configured to use TACACS+ or RADIUS for external authentication, the custom vendor attribute list should be updated in the TACACS+ or RADIUS server with any new permissions. The attribute list for the appropriate UserGroup can be found at Administration > AAA > UserGroups. Click the **Export** link for the appropriate user group. Refer to Chapter 14 of the *Cisco Wireless Control System Configuration Guide* for additional information regarding upgrading.

Using the Installer to Upgrade WCS for Linux

Follow these steps to upgrade WCS (on a Linux platform) using the automated upgrade:

Step 1 Using the command line, perform one of the following:

a. If you are installing from a CD, switch to the /media/cdrom directory.

b. If you are installing from Cisco.com, switch to the directory in which the install file was downloaded. For example, if the install file was placed in /root/Desktop, enter **cd /root/Desktop**.

Step 2 Enter **./WCS-STANDARD-K9-6.0.X.Y.bin** (for CD users) or **./WCS-STANDARD-LB-K9-6-0-X-Y.bin** (for Cisco.com users) to start the install script.

Step 3 The Install Anywhere message appears and prepares the system for installation. After a few seconds, the Introduction appears, followed by the license agreement statement. You must accept the license agreement to continue.

Step 4 At this point, the install wizard detects whether a previous version of WCS is installed and specifies whether the current version is eligible for an automated upgrade. You receive a notification whether or not your most recent WCS version is eligible for the automated upgrade.

Step 5 If you cannot continue to the automated upgrade because your current WCS version is not eligible, choose **Install** and continue to the manual upgrade (refer to the *WCS Configuration Guide* for manual upgrade instructions). You can also choose to do a manual upgrade rather than the recommended automated upgrade by choosing **Install** and continuing to the manual upgrade, but this is not recommended. If your current WCS version is eligible for the recommended automated upgrade, choose **Upgrade** and continue to Step 6.

Step 6 Several of the values from the previous installation are retained and carried over as part of the upgrade. These include the following:

- the ports
- the root password

- the root FTP password
- the TFTP server file location
- the FTP server file location
- the multi-homed server interfaces

Step 7 Choose a folder in which to install the Cisco WCS. It must be a different location than the previous installation. Click **Next** to continue.

Step 8 Choose a folder location to store the shortcuts. It must be a different location than the previous installation.

Step 9 Continue to follow the prompts that appear. You are notified when the system checks for required space, uninstalls previous versions, backs up files, restores, and so on. A prompt appears asking if you are ready to start WCS as a service. Click **Yes**.

Note The upgrade log is located in the standard log directory (\webnms\logs) if the automated upgrade completes. For an incomplete automated upgrade, the upgrade log is located in the user home directory.

Note If WCS is configured to use TACACS+ or RADIUS for external authentication, the custom vendor attribute list should be updated in the TACACS+ or RADIUS server with any new permissions. The attribute list for the appropriate UserGroup can be found at Administration > AAA > UserGroups. Click the **Export** link for the appropriate user group. Refer to Chapter 14 of the *Cisco Wireless Control System Configuration Guide* for additional information regarding upgrading.

Restoring the WCS Database in a High Availability Environment

During installation, you are prompted to determine if a secondary WCS server would be used for high availability support to the primary WCS server. If you opted for this high availability environment and enabled it in the Administration > High Availability window, the status appears as *HA enabled*. Before performing a database restore, you must convert the status to *HA not configured*.

Note If the restore is performed while the status is set to *HA enabled*, unexpected results may occur.

Follow one of these procedures to change the status from *HA enabled* to *HA not configured*:

- Click the **Remove** button on the HA Configuration window (Administration > High Availability).
- Restart the primary server. Go to the secondary HealthMonitor GUI (https://<SecondaryWCS>:8082) and click **Failback**.
  - This procedure is used when one of the following instances has occurred:

    The primary server is down and failover has not been executed, so the secondary server is in SecondaryLostPrimary state.

    or

The primary server is down and failover is already executed, so the secondary server is in the SecondaryActive state.

The primary server will now be in HA Not Configured mode, and you can safely perform a database restore.

Important Notes

This section describes important information about Cisco WCS.

If you change the report repository path under Administration > Settings > Report, then the existing saved download report will no longer work. To fix this, manually move the files to the new directory by cutting and pasting the files.

WPlus License Features Included in Base License

All features included in a Wireless LAN Controller WPlus license are now included in the base license; this change is introduced in controller release 6.0.196.0. There are no changes to WCS BASE and PLUS licensing.

These WPlus license features are included in the base license:

- Office Extend AP
- Enterprise Mesh
- CAPWAP Data Encryption

The licensing change can affect features on your wireless LAN when you upgrade or downgrade controller software releases, so you should be aware of these guidelines:

- If you have a WPlus license and you upgrade from 6.0.18x to 6.0.195.0: Your license file contains both Basic and WPlus license features. You won't see any disruption in feature availability and operation.
- If you have a WPlus license and you downgrade from 6.0.195.0 to 6.0.18x: The license file in 6.0.195.0 contains both Basic and WPlus license features, so you won't see any disruption in feature availability and operation.
- If you have a base license and you downgrade from 6.0.195.0 to 6.0.18x: When you downgrade, you lose all WPlus features.

Note Some references to Wireless LAN Controller WPlus licenses remain in WCS and in the controller CLI and GUI in release 6.0.196.0. However, WPlus license features have been included in the Base license, so you can ignore those references.

Duplicate AP Name

If you see access points with the same name while applying controller templates or adding them to the map, perform a refresh config. The duplicates in the database will be eliminated.

High Availability

An e-mail address is now optional when you configure high availability. However, if you enter a properly formatted email address you must also configure a WCS e-mail server.

Note High availability is supported on Linux, on Windows 2003, and on VMware environments. Specific operating system support is listed in the "Operating Systems Requirements" section on page 3.

Client Session Report

The new client session report replaces the existing Client Association and Client Detail Report. If you perform an upgrade, Client Association no longer appears in the Reports menu. The data pertaining to these reports migrates successfully, and saved report entries for Client Association and Client Detail reports are migrated. However, the new ClientSessionInfo table is not populated with data from the previous reporting period; the table is populated with client-related data that occurred after upgrade. The new client detail report contains the details of association time, disassociation time, and session timeout along with details of VLAN, session length, client location, Megabit information used, SNR, RSSI, and throughput.

Cisco WCS Supported on Windows 2003 English and Japanese Operating Systems Only

Cisco WCS is supported only on English or Japanese versions of the Windows 2003 operating system. Display problems sometimes occur when you install and run Cisco WCS on operating systems translated to other languages or with locale settings other than English or Japanese.

Notifications in Junk E-mail Folder

If a domain name is not set in the e-mail settings, notifications may end up in the junk e-mail. When the primary device is down, no e-mail notifications are received, but the log message indicates that an e-mail was successfully sent.

Internet Explorer Error

When you click certain links that call Javascript code, you may get an Internet Explorer error as follows:

Problems with this web page might prevent it from being displayed properly or functioning properly. In the future, you can display this message by double clicking the warning icon displayed in the status bar.

This problem appears if another program has deregistered the DLLs below. Re-registering them corrects the problem.

Follow these steps to reregister the DLLs:

Step 1 Open a command-line window in Windows XP (Start > All Programs > Accessories > Command Prompt).

Step 2 Run these commands one at a time in the following order. After each command successfully runs, you should receive a pop-up message that the DllRegisterServer in_*something*.dll succeeded.

1. regsvr32 msscript.ocx
2. regsvr32 dispex.dll
3. regsvr32 vbscript.dll
4. regsvr32 scrrun.dll
5. regsvr32 urlmon.dll
6. regsvr32 actxprxy.dll
7. regsvr32 shdocvw.dll

Step 3 Restart the computer.

Notes about Google Earth

When you launch Google Earth, this message appears:

```
Google Earth could not write to the current cache or myplaces file location. The values
will be set as follows:
My Places Path:"C:\Document and Settings\userid\Application Data\Google\GoogleEarth"
Cache Path: "C:\Documents and Settings\userid\Local Settings\Application
Data\Google\GoogleEarth"
```

This is expected behavior.

Also, if you visit the AP Details window a second time, you get an "invalid path / googleArthLradDetails was requested" HTTP status message. This Google Earth problem can be resolved by deleting the first AP Details occurrence.

Windows XP Cannot Load CAD Files

Internet Explorer 7 running on Windows XP cannot load CAD files because of missing DLLs (C:\Windows\system\DWMAPI.DLL). These DLLs are present only on Windows Vista.

Take one of the following actions:

- Uninstall IE7 and install IE6.
- Leave IE7 and install the missing DLLs.

Deletion of TFTP Server Is Not Updated in the Configuration Backup

To add a TFTP server, click **Configure > Controller Templates**, choose **TFTP server** from the left sidebar menu, and choose **Add TFTP Server** from the drop-down menu. To add the TFTP server, enter the name and IP address and click **Save**. If you later delete this TFTP server and back up the configuration (Administration > Background Task > Configuration Backup), the IP address of the TFTP server still appears in the TFTP Server window when only the default server appears.

Conflicting Ports Interrupt WCS Start

WCS fails to start if there is a conflicting port in use. You receive a "Failed to start WCS server" message, but you do not receive a list of conflicting ports. Go to WCS/webnms/logs/wcs-0-0.log and view the conflicting ports. Enter the following to get a list of the process IDs associated with each connection:

In Windows XP and Windows Server 2003, enter **netstat -na0.**

In Linux, enter **netstat -nlp.**

In the Task Manager, you see the respective PID and can stop the process using the port that WCS requires.

New Features

There are no new features in this maintenance release.

Caveats

The following sections list open and resolved caveats in Cisco WCS 6.0.181.0 for Windows and Linux. For your convenience in locating caveats in Cisco's Bug Toolkit, the caveat titles listed in this section are taken directly from the Bug Toolkit database. These caveat titles are not intended to be read as complete sentences because the title field length is limited. In the caveat titles, some truncation of wording or punctuation might be necessary to provide the most complete and concise description. The only modifications made to these titles are as follows:

- Commands are in **boldface** type.
- Product names and acronyms may be standardized.
- Spelling errors and typos may be corrected.

Note If you are a registered cisco.com user, view Bug Toolkit on cisco.com at the following website:

http://tools.cisco.com/Support/BugToolKit/.

To become a registered cisco.com user, go to the following website:

http://tools.cisco.com/RPF/register/register.do

Open Caveats

Table 1 lists the open caveats in Version 6.0.181.0.

Table 1 Open Caveats

ID Number	Caveat Title
CSCsy31225	Left nav disappears on AP config screens
CSCtd44718	Add user input required commands to CLI template parser.
CSCtd45012	WCS CLI Templates do not "time out"
CSCtd63818	WCS Migration template fails to convert AP to LWAP over WAN Links.
CSCte49211	WCS template sets Tx Power Assignment off if Default Tx Pwr Level not 1
CSCte49326	WCS background task configuration sync needs more details
CSCte50763	WCS TFTP Server stops existing transfer if unreach on previous recvd
CSCte51465	Migration analysis fails when autonomous AP is set to SSH only-TACACS
CSCte53277	WCS - License Centers shows License Id instead of PAK

Resolved Caveats

Table 2 lists caveats resolved in Cisco WCS 6.0.181.0

Table 2 Resolved Caveats

ID Number	Caveat Title
CSCsx96043	Client count graph in the home page is not showing Autonomous clients
CSCsz05354	4.2 AP(s) do not show up for AP Summary Report
CSCta92543	Tag should properly escape the HTML
CSCta94465	Need to treat sniffer mode AP as monitor mode AP & not show heatmap
CSCtb58698	WCS license error after upgrade
CSCtb73549	Tag Detail page shows null temperature in the telemetry data part
CSCtc36642	AutoCAD maps becomes blurry when used with MAP Editor
CSCtc40247	change Mhz to MHz on rrm configuration mismatch page
CSCtc41084	WCS map import from file fails and does not provide an error message
CSCtc44722	All WCS Page navigations get redirected to home page
CSCtc49690	WCS: Audit mismatch for LAG mode
CSCtc58081	Getting Error when View Rx Neighbors is clicked on mouse hover
CSCtc79940	Modify database properties for high-end servers
CSCtc88535	Refresh from Network shows Assoc Clients as 0
CSCtc91763	Friendly rogue AP gets classified as malicious rogue AP
CSCtc95697	No way to enable search log messages in WCS
CSCtd05700	Map - Mesh Filter page appears Null r Object not found exception display

Table 2 Resolved Caveats (continued)

ID Number	Caveat Title
CSCtd17650	Unable to create Client report by Floor Area
CSCtd20947	HTML reports don't block report if graphs > 500
CSCtd21014	Antenna Gains for Zest APs are wrong and also for cascade
CSCtd25646	Add points to Calibration fails if aIOS AP is present
CSCtd66943	WCS: Reports incorrect duplex mode for CDP neighbor of an AP
CSCtd67660	Current message-digest algorithm for self-signed cert
CSCtd70812	Rogue AP report does not produce consistent results
CSCtd75773	802.11a/n and b/g/n parameters template changes AP
CSCte12171	Guest accounts created in Virtual domains move

If You Need More Information

If you need information about a specific caveat that does not appear in these release notes, you can use the Cisco Bug Toolkit to find caveats of any severity. Click this URL to browse to the Bug Toolkit:

http://tools.cisco.com/Support/BugToolKit/

(If you request a defect that cannot be displayed, the defect number might not exist, the defect might not yet have a customer-visible description, or the defect might be marked Cisco Confidential.)

Troubleshooting

For the most up-to-date, detailed troubleshooting information, refer to the Cisco TAC website at the following location:

http://www.cisco.com/cisco/web/psa/troubleshoot.html

Click **Wireless** and **Wireless LAN Management**. Then choose **Autonomous Wireless LAN** and **Unified Wireless LAN Management**.

Related Documentation

For information on the Cisco Unified Wireless Network Solution and for instructions on how to configure and use the Cisco UWN, refer to the *Cisco Wireless Control System Configuration Guide* and the *Cisco Wireless LAN Controller Configuration Guide.*

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, 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 Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, 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. (0910R)