



Release Notes for the CiscoWorks Wireless LAN Solution Engine, Release 2.15

June 13, 2007

Contents

These release notes contain the following sections.

- [Java Runtime Environment, page 1](#)
- [New Features, page 2](#)
- [Product Documentation, page 3](#)
- [Open Caveats, page 6](#)
- [Resolved Caveats, page 8](#)
- [Obtaining Documentation, page 9](#)
- [Cisco Product Security Overview, page 10](#)
- [Obtaining Technical Assistance, page 11](#)
- [Obtaining Additional Publications and Information, page 13](#)

Java Runtime Environment

To launch Location Manager from WLSE, you should have Java Runtime Environment version 1.5 installed on your system.



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

© 2007 Cisco Systems, Inc. All rights reserved.

New Features

WLSE 2.15 supports the following new features:

- When creating a template, you can now enable VLAN backup and specify up to three backup VLANs in the SSID Manager 802.11 pages (under Security) and in the VLAN page (under Services).
- Information about backup VLANs will appear in the following reports:
 - AP SSID Report
 - AP VLAN Report
 - Group SSID Report
 - Group VLAN Report.
 - VLAN Security Report
 - Per VLAN Client Report (both Device and Group Report).
- This release supports SNMPv3 for only IOS access points. WLSE itself will still be SNMPv2c-based. You can manage IOS access points using either SNMPv2c or SNMPv3, but not both simultaneously.
- When scheduling a job, you now have an option to erase the entire flash memory before uploading an image.
- You can now display the currently logged in users in WLSE.
- The WLSE IP filter is now applied before contacting a device instead of being applied after contacting the device. The WLSE will not discover devices excluded from the IP filter. Also, discovery and switch port tracing will use the filter to restrict access to excluded devices.
- WLSE now allows upgrade from versions 2.12, 2.13, and 2.13.1 to version 2.15.
- The Discovery Wizard has new enhancements. The Modify Periodic Device Discovery based on Cisco Discovery Protocol (CDP) option has been moved to the first page. In addition, a link to the SNMP credentials page has been added to the first page. Few more changes were also made to the other pages of the wizard.
- Enhancements were made to the WLSE reports to include more information to fix display problems

Product Documentation

You can access the WLSE online help by clicking the **Help** button in the top right corner of the screen or by selecting an option, then clicking the **Help** button. You can access the user guide from the online help by clicking the **View PDF** button.

The following product documentation is available for WLSE 2.15:

Table 1 Product Documentation

Document Title	Available Formats
<i>Installation and Configuration Guide for the 1030 CiscoWorks Wireless LAN Solution Engine Express</i>	<p>Describes how to install and configure the WLSE Express. Available in the following formats:</p> <ul style="list-style-type: none"> Printed document included with the product. PDF on the WLSE Recovery CD-ROM. On Cisco.com: http://www.cisco.com/en/US/products/sw/cscowork/ps3915/tsd_products_support_install_and_upgrade.html Printed document available by order (part number DOC-17252=)¹
<i>Installation and Configuration Guide for the 1130-19 CiscoWorks Wireless LAN Solution Engine Express</i>	<p>Describes how to install and configure the WLSE. Available in the following formats:</p> <ul style="list-style-type: none"> Printed document included with the product. PDF on the WLSE Recovery CD-ROM. On Cisco.com: http://www.cisco.com/en/US/products/sw/cscowork/ps3915/tsd_products_support_install_and_upgrade.html Printed document available by order (part number DOC-17251=)¹
<i>Installation and Configuration Guide for the 1133 CiscoWorks Wireless LAN Solution Engine Express</i>	<p>Describes how to install and configure the WLSE. Available in the following formats:</p> <ul style="list-style-type: none"> Printed document included with the product. PDF on the WLSE Recovery CD-ROM. On Cisco.com: http://www.cisco.com/en/US/products/sw/cscowork/ps3915/tsd_products_support_install_and_upgrade.html Printed document available by order (part number DOC-17476=)
<i>Regulatory Compliance and Safety Information for the 1030 CiscoWorks Wireless LAN Solution Engine Express</i>	<p>Provides regulatory compliance and safety information for the WLSE Express. Available in the following formats:</p> <ul style="list-style-type: none"> Printed document included with the product. PDF on the WLSE Recovery CD-ROM. On Cisco.com: http://www.cisco.com/en/US/products/sw/cscowork/ps3915/tsd_products_support_install_and_upgrade.html

Table 1 Product Documentation (Continued)

Document Title	Available Formats
<i>Regulatory Compliance and Safety Information for the 1130-19 CiscoWorks Wireless LAN Solution Engine</i>	<p>Provides regulatory compliance and safety information for the WLSE. Available in the following formats:</p> <ul style="list-style-type: none"> Printed document included with the product. PDF on the WLSE Recovery CD-ROM. On Cisco.com: http://www.cisco.com/en/US/products/sw/cscowork/ps3915/tsd_products_support_install_and_upgrade.html
<i>Regulatory Compliance and Safety Information for the 1133 CiscoWorks Wireless LAN Solution Engine</i>	<p>Provides regulatory compliance and safety information for the WLSE. Available in the following formats:</p> <ul style="list-style-type: none"> Printed document included with the product. PDF on the WLSE Recovery CD-ROM. On Cisco.com: http://www.cisco.com/en/US/products/sw/cscowork/ps3915/tsd_products_support_install_and_upgrade.html
<i>User Guide for the CiscoWorks Wireless LAN Solution Engine</i>	<p>Describes WLSE features and provides instructions for using it. Available in the following formats:</p> <ul style="list-style-type: none"> From the WLSE online help. PDF on the WLSE Recovery CD-ROM. On Cisco.com: http://www.cisco.com/en/US/products/sw/cscowork/ps3915/products_user_guide_list.html
<i>Upgrading CiscoWorks Wireless LAN Solution Engine Software</i>	<p>Describes the options available and how to upgrade to the WLSE system software to release 2.13. Available in the following formats:</p> <ul style="list-style-type: none"> From the WLSE online help. On Cisco.com: http://www.cisco.com/en/US/products/sw/cscowork/ps3915/tsd_products_support_install_and_upgrade.html
<i>FAQ and Troubleshooting Guide for the CiscoWorks Wireless LAN Solution Engine</i>	<p>Contains FAQs and troubleshooting information, and provides a table for all the faults displayed under Faults > Display Faults with explanations and possible actions. Available in the following formats:</p> <ul style="list-style-type: none"> From the WLSE online help. On Cisco.com: http://www.cisco.com/en/US/products/sw/cscowork/ps3915/prod_troubleshooting_guides_list.html
<i>Configuring Devices for Management by the CiscoWorks Wireless LAN Solution Engine</i>	<p>Contains procedures for converting non-IOS access points to IOS access points. Available in the following formats:</p> <ul style="list-style-type: none"> On Cisco.com: http://www.cisco.com/en/US/products/sw/cscowork/ps3915/products_installation_and_configuration_guides_list.html

Table 1 Product Documentation (Continued)

Document Title	Available Formats
<i>Supported Devices Table for the CiscoWorks Wireless LAN Solution Engine</i>	Lists the devices supported by WLSE. Available in the following formats: <ul style="list-style-type: none"> On Cisco.com: http://www.cisco.com/en/US/products/sw/cscowork/ps3915/products_device_support_tables_list.html
<i>Finding Documentation for the CiscoWorks Wireless LAN Solution Engine</i>	Lists the documents associated with this release of WLSE. Available in the following formats: <ul style="list-style-type: none"> Printed document included with product. PDF on the WLSE Recovery CD-ROM. On Cisco.com: http://www.cisco.com/en/US/products/sw/cscowork/ps3915/products_documentation_roadmaps_list.html
<i>Finding Documentation for the CiscoWorks Wireless LAN Solution Engine Express</i>	Lists the documents associated with this release of WLSE. Available in the following formats: <ul style="list-style-type: none"> Printed document included with product. PDF on the WLSE Recovery CD-ROM. On Cisco.com: http://www.cisco.com/en/US/products/ps6379/products_documentation_roadmaps_list.html
<i>Configuring the CiscoWorks Wireless LAN Solution Engine TACACS+/RADIUS Authentication Using Cisco Secure ACS</i>	Describes the procedure to configure the CiscoWorks Wireless LAN Solution Engine (WLSE) using ACS as a TACACS+/RADIUS authentication module. <ul style="list-style-type: none"> On Cisco.com: http://www.cisco.com/en/US/products/sw/cscowork/ps3915/products_installation_and_configuration_guides_list.html
<i>WLSE Express AAA Server Certificate Configuration Guide</i>	Provides information about public key infrastructure (PKI) and Rabin-Shamir-Adelmann (RSA) certificates, how to generate certificates to be used with the WLSE Express, and how to configure AAA certificates to be used on WLSE-Express. <ul style="list-style-type: none"> On Cisco.com: http://www.cisco.com/en/US/products/ps6379/products_installation_and_configuration_guides_list.html

1. See [Obtaining Documentation](#), page 9.

Open Caveats


Note

To obtain more information about known problems, access the Cisco Software bug Toolkit at <http://www.cisco.com/cgi-bin/Support/Bugtool/home.pl>. (You will be prompted to log into Cisco.com.)

- CSCse75262—When you configure the WLSE for remote authentication with the failover option, Telnet logins do not fail over. Users cannot log in with their locally defined password over Telnet.


Note

SSH does not exhibit this problem.

Workaround: None at this time.

- CSCsg88520—Exporting devices to CiscoWorks RME does not work (Devices > Discover > Export Devices > To CiscoWorks).

Exporting devices to CiscoWorks is recommended from LMS 2.5.

Workaround: None at this time.

- CSCsh76933—A user with Help Desk privilege can run non-monitor jobs using the Location Manager (Site > Location Manager).

If you enable the Location Manager option for users under Admin > User Admin > Help Desk, they will be able to perform all of the tasks in the Location Manager page (Sites > Location Manager).

Workaround: None at this time.

- CSCsi19952—A configuration job, running on devices that use the 12.3(8)JEB and 12.4(1)JA images, fails with the following error messages:

```
Both EAP and WPA-PSK cannot be configured on same ssid. To configure WPA-PSK disable EAP.
```

```
Key-management WPA is required for WPA-PSK
```

WLSE generates these error messages if the template has the following configuration:

```
Services: VLAN
-----
interface Dot11Radio 0.0
  no ssid ssid13
dot11 vlan-name vlan13 vlan 13
dot11 ssid ssid13
  vlan 13
interface Dot11Radio 0
  ssid ssid13
interface Dot11Radio 0.13
  encapsulation dot1q 13
  bridge-group 13
interface FastEthernet 0.13
  encapsulation dot1q 13
  bridge-group 13
Security : WEP Key Manager 802.11b/g/n
-----
dot11 ssid ssid13
  no authentication key-management
interface Dot11Radio 0
  no ssid ssid13
  no encryption vlan 13 mode
  no encryption vlan 13 key 1
  no encryption vlan 13 key 2
```

```

no encryption vlan 13 key 3
no encryption vlan 13 key 4
encryption vlan 13 key 3 size 128bit 0 ***** transmit-key
encryption vlan 13 mode ciphers tkip wep128
Security : SSID Manager 802.11b/g/n
-----
interface Dot11Radio 0.0
  no ssid ssid13
no dot11 ssid ssid13
dot11 ssid ssid13
  vlan 13
  authentication open
  authentication network-eap eap_methods
  authentication key-management wpa version 1 optional
  wpa-psk ascii 0 *****
interface Dot11Radio 0
  ssid ssid13

```

Workaround: Do the following in the SSID pages of the template (Configure > Templates > Security):

1. Uncheck the check box for **Network EAP** or any other EAP option.
 2. Check the **WPAv1** check box under Authenticated Key Management.
 3. In the Delete SSID section, enter the SSID in the SSID field, check the **Remove this SSID globally** check box, and click the >> button to move the SSID to the SSID to Delete list.
 4. Run a configuration job using this template. The job should succeed with all the configuration applied to the device.
- CSCsi33251—The device-specific settings are not imported to WLSE after uploading the Master tar file.

If you use the Master tar file to configure WLSE, the device-specific settings present in the WLSE and from which the Master tar was generated do not get imported.

Workaround: Export the device-specific settings from the WLSE from which the Master tar file was generated and import the resulting CSV file to the desired WLSE.

- CSCsi42820—When you upgrade the WLSE from 2.12 to 2.15, the **show version** CLI command does not display the serial number. This problem does not happen with a fresh installation of WLSE 2.15.

Workaround: None at this time.

- CSCsi46083—The performance inventory job took little longer than the default period setting of 31 minutes, which keeps the WLSE server resource usage at a high level all the time.

This happens when the WLSE server is under stress running with both S27 and S19 and managing the maximum number of supported devices (1500) with SNMPv3 and Radio management enabled in addition to voice traffic.



Note CPU usage is extremely high (about 90%) when you use SNMPv3.

Workaround: If you use SNMP v3 with a large number of managed devices, set the period for the default Performance Inventory job to 50 minutes or longer to improve the usage of WLSE server resources.

- CSCsi47520—When using the WLSE Wizard, if you click the Compare Known Devices Version button in the Software page, the resulting page does not show any devices in any of the columns of the table.

This problem happens when one or both of the following is true:

- The devices run versions 12.3(8)JA1, JA2... and 12.3(8)JEA, JEA1...
- The value of the Role in Radio Network option is other than AP Role (for example, WGB and BR).

Workaround: None at this time.

- CSCsi69077—When pushing a template created in WLSE 2.13.1 to 12.3(8)JEB or 12.4(3g)JA devices from WLSE 2.15, WLSE displays warning messages similar to the following:

```
This device version is not valid for the configuration template. The configuration job may fail if this template is applied to the device.
```

Workaround: Ignore the warnings and apply the template to the devices. Alternatively, resave the template in WLSE 2.15 and apply the template to the devices.

Resolved Caveats

These caveats are resolved in WLSE software release 2.15.

- CSCsa93652—Backing up data on WLSE occasionally fails due to database locks.
- CSCsf23048—When WLSE sends out a report by email, the report covers the requested time period plus one additional day.
- CSCsf96033—The CCMP error is erased from the Faults (IDS > Faults) and Display Faults (Faults > Display Faults) pages when WLSE receives the error twice.
- CSCsf96421—Creating a site, a building, and a floor with the same name in Location Manager results in floor subgroups with the same name being created in a loop in the Group Details window (Devices > Group Management).
- CSCsf98043—WLSE tries to send email notifications to deleted email addresses. In the process of sending the email notifications, WLSE replaces the deleted email addresses with null@domainname.
- CSCsc12519—If an AP 1230G device managed by WLSE is using channel 14, WLSE displays the following fault in the Display Faults page.


```
Inconsistent device state found: Device "<hostname>": Ifindex=1, MAC=<MAC Address>:
"current channel 14 is not permitted in Regulatory Domain "MKK(Japan)""
```
- CSCsc92799—Acknowledging Wireless Client MAC Spoofing faults does not work. After acknowledging a fault, the fault disappears from the Faults for Wireless Client MAC Spoofing page (IDS > Summary > Wireless Client MAC Spoofing), but after five minutes the fault reappears.
- CSCse62018—Sometimes device icons in Location Manger are not in sync with icons in the Device Center page. For example, a device icon is green in Location Manager, but is red in WLSE's Device Center page.
- CSCse64534—When configuring a network for radio management, after WLSE successfully authenticates to WDS and reaches the SECURITY KEYS SETUP status, WLSE generates the following fault:

```
A different WLSE (eth1 ip addr) is now Registered to this WDS
```

- CSCse75075—Friendly access points come back as rogues after rebooting WLSE.
- CSCse94731—When creating a new assisted-configuration job, if the channel or power settings in the Constraints/Goals page are different from the other jobs and the All AP's option is selected, all the Constraints/Goals settings for the other jobs change.
- CSCsf16231—When a WDS device is replaced with a new WDS device that has the same IP address as the old WDS device, the Location Manager does not list the new device. Instead, the Location Manager shows the old WDS device in gray color.
- CSCsg51990—WLSE does not show currently-suppressed ports. After WLSE successfully traces the switch port for a rogue access point, WLSE shuts down the port using SNMP. However, the Suppressed Switch Ports page (IDS > Manage Network-Wide IDS Settings > Rogue AP Detection > View current suppression), which should display a list of suppressed ports, is always blank.
- CSCsh35184—Switch port tracing occurs after being disabled.
- CSCsc65367—When running radio parameter generation (RPG) from an assisted-configuration HTML site, different numbers of access points and channel combinations sometime cause a problem when saving parameters to the database, which results in a failure to start RPG calculation.
- CSCsg25615—The access.log file continues to grow in size and is not rotated on a weekly basis.
- CSCsg53207—WLSE Express checks only the first 8 characters of the password used to log in to the admin account.
- CSCsg76517—The size of the back up files is different for similar WLSEs.
- CSCsh40709—After applying the WLSE 2.13.1 patch, the **show version** CLI command does not show the serial number.
- CSCsg72176—A high-availability cluster of two WLSEs loses connection and fails to replicate.
- CSCsd84989—The 2610 router appears as a WDS device in WLSE.

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

<http://www.cisco.com/techsupport>

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

Cisco documentation and additional literature are available in the Product Documentation DVD package, which may have shipped with your product. The Product Documentation DVD is updated regularly and may be more current than printed documentation.

The Product Documentation DVD is a comprehensive library of technical product documentation on portable media. The DVD enables you to access multiple versions of hardware and software installation, configuration, and command guides for Cisco products and to view technical documentation in HTML. With the DVD, you have access to the same documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .pdf versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD=) from Cisco Marketplace at this URL:

<http://www.cisco.com/go/marketplace/>

Ordering Documentation

Beginning June 30, 2005, registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

<http://www.cisco.com/go/marketplace/>

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can send comments about Cisco documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

<http://www.cisco.com/go/psirt>

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—security-alert@cisco.com

An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- Nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532



Tip

We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.x through 8.x.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

<http://www.cisco.com/techsupport>

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

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

**Note**

Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

<http://www.cisco.com/techsupport/servicerequest>

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/techsupport/contacts>

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:
<http://www.cisco.com/go/marketplace/>
- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:
<http://www.ciscopress.com>
- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:
<http://www.cisco.com/packet>
- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:
<http://www.cisco.com/go/iqmagazine>
or view the digital edition at this URL:
<http://ciscoiq.texterity.com/ciscoiq/sample/>
- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:
<http://www.cisco.com/ipj>
- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:
<http://www.cisco.com/en/US/products/index.html>

- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:
<http://www.cisco.com/discuss/networking>
- World-class networking training is available from Cisco. You can view current offerings at this URL:
<http://www.cisco.com/en/US/learning/index.html>

This document is to be used in conjunction with the documents listed in the “[Product Documentation](#)” section.

CCVP, the Cisco Logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, *Packet*, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath 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. (0704R)

© 2007 Cisco Systems, Inc. All rights reserved.