



Release Notes for the CiscoWorks Wireless LAN Solution Engine, Release 2.5

These release notes are for use with the CiscoWorks Wireless LAN Solution Engine (WLSE).

These release notes provide:

- [New Features, page 2](#)
- [Product Documentation, page 2](#)
- [Documentation Updates, page 5](#)
- [Known and Resolved Problems, page 6](#)
- [Obtaining Documentation, page 20](#)
- [Obtaining Technical Assistance, page 21](#)
- [Obtaining Additional Publications and Information, page 23](#)



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

Copyright © 2003 Cisco Systems, Inc. All rights reserved.

New Features

The WLSE Release 2.5 contains management support for:

- Radio Management support for:
 - Rogue AP detection
 - Interference detection
 - Location Manager (for 2-D visualization)
 - Assisted site surveys
- Network management support for Firmware Version 12.2(13)JA

Product Documentation



Note

We sometimes update the printed and electronic documentation after original publication. Therefore, you should also review the documentation on Cisco.com for any updates.

[Table 1](#) describes the product documentation that is available.

Table 1 Product Documentation

Document Title	Available Formats
<i>Installation and Configuration Guide for the CiscoWorks Wireless LAN Solution Engine</i>	<ul style="list-style-type: none">• Printed document included with the product.• PDF on the WLSE Recovery CD-ROM.• On Cisco.com:<ul style="list-style-type: none">– Log into Cisco.com.– Select at Products & Services > Network Management CiscoWorks > Wireless LAN Solution Engine > Technical Documentation > Installation and Configuration Guides.• Printed document available by order (part number DOC-7815903=).¹
<i>User Guide for the CiscoWorks Wireless LAN Solution Engine</i>	<ul style="list-style-type: none">• From the WLSE online help.• PDF on the WLSE Recovery CD-ROM.• On Cisco.com:<ul style="list-style-type: none">– Log into Cisco.com.– Select at Products & Services > Network Management CiscoWorks > Wireless LAN Solution Engine > Technical Documentation > User Guides.• Printed document available by order (part number DOC-7815902=).²
<i>Regulatory Compliance and Safety Information for the CiscoWorks 1130 Wireless LAN Solution Engine</i>	<ul style="list-style-type: none">• Printed document included with the product.• PDF on the WLSE Recovery CD-ROM.• On Cisco.com:<ul style="list-style-type: none">– Log into Cisco.com.– Select Products & Services > Network Management CiscoWorks > Wireless LAN Solution Engine > Technical Documentation > Regulatory Approvals and Compliance.

Table 1 *Product Documentation (Continued)*

Document Title	Available Formats
<i>Supported Devices Table for the CiscoWorks Wireless LAN Solution Engine</i>	<ol style="list-style-type: none">1. Log into Cisco.com.2. Select Products & Services > Network Management CiscoWorks > Wireless LAN Solution Engine > Technical Documentation > Device Support Tables.
Context-sensitive online help	<ul style="list-style-type: none">• Select an option from the navigation tree, then click Help.• Click the Help button in the dialog box.
<i>FAQ and Troubleshooting Guide for the CiscoWorks Wireless LAN Solution Engine</i>	<ol style="list-style-type: none">1. Log into Cisco.com.2. Select Products & Services > Network Management CiscoWorks > Wireless LAN Solution Engine > Alerts and Troubleshooting > Troubleshooting Guides.

1. See the [“Obtaining Documentation”](#) section on page 20.
2. See the [“Obtaining Documentation”](#) section on page 20.

Documentation Updates

The latest version of the online help and/or User Guide for the CiscoWorks Wireless LAN Solution Engine does not include additions and corrections to the following sections:

Disabling or Enabling Telnet and Selecting SSH Type

This topic incorrectly states that Telnet is enabled by default. It is disabled by default.

Adding an AAA Server

The procedure for configuring a RADIUS AAA server states that only ACS servers can be configured as RADIUS AAA servers. However, CAR RADIUS servers can also be configured as RADIUS AAA servers.

Displaying Data Rate

This topic incorrectly states that the highest basic rate set of the APs is displayed on the Location Manager floor map. The topic should read that the highest *operational* rate set, whether it is a basic rate or the enabled rate, of the APs is displayed on the floor map.

Managing Processes

This topic incorrectly omits the WirelessSvcMgr process. The WirelessSvcMgr is the Radio Manager virtual machine.

Radio Management

The Radio Management chapter should clearly state that if you are using WDS on your wireless LAN, you must:

1. Configure the access point that is providing WDS.
2. Configure the WLSE to authenticate with the access point providing WDS.

Refer to the online help for the CiscoWorks Wireless LAN Solution for specific instructions.

In addition, the online help should state the following requirements:

The Radio Management portion of WLSE requires the following combinations of products and versions:

- WLSE (Release 2.5)

- IOS AP Release (12.2(13)JA)
- Cisco Aironet 11b-Client with 12.08 release

Radio Management functionality, such as client walkabout and radio monitoring, works when the client image is release 12.08 only. In addition, Radio Management functionality supports 802.11b radios only.

Naming Guidelines

The WLSE does not allow duplicate job names. Firmware, configuration, and radio management jobs must have unique names.

Known and Resolved Problems

[Table 2](#) describes the problems known to exist in this release; [Table 3](#) describes problems solved since the last release.



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.)

Table 2 *Known Problems in the WLSE*

Bug ID	Summary	Explanation
CSCea91955	<p>Fault Notification Syslog messages from WLSE are displayed in a truncated form on the Resource Manager Essentials (RME) 3.4 Syslog Standard Report.</p>	<p>The RME 3.4 Syslog Standard Report displays fault notification syslog messages sent in XML message format or in plain text message format in a truncated form.</p> <p>To work around this problem and view the syslog messages in an untruncated form, see the following flat syslog file located in:</p> <ul style="list-style-type: none"> • On the Solaris 2.8 based RME 3.4 server: /var/log/syslog_info • On the Windows 2000 based RME 3.4 server: C:/Program Files/CSCOpX/log/syslog.log
CSCeb23307	<p>Entering dates under the Advanced Options for Device Discovery can generate an error message even if the dates are valid.</p>	<p>When you select Devices > Discover > Discover > Advanced Options, and set the Filters Valid From date, only the day and month are checked for validity, not the year. Therefore, if you enter a date range such as 12/30/2003 to 01/20/2004, you will get an error message stating that the "Start Date is greater than End Date," even though the date range is valid.</p> <p>To work around this problem, do not enter date interval values when using the MAC filtering option.</p>
CSCeb23714	<p>You will get an error if you use the pound (#) sign in the password for device Telnet credentials.</p>	<p>When you use a pound (#) sign in the password field under Devices > Discover > Device Credentials > Telnet/SSH/User Password, a 500 Internal Server Error displays.</p> <p>To work around this problem, do not use pound (#) sign in the password.</p>

Table 2 *Known Problems in the WLSE (Continued)*

Bug ID	Summary	Explanation
CSCeb36372	The Client Historical Association report does not contain a disassociation time.	<p>The Client Historical Association report does not have the information about last time a client associated with the access point, the time it disconnected from the access point, the duration of the association, or the association state.</p> <p>There is no workaround for this problem.</p> <p>Note In the current release, only association times of a client are supported. Disassociation time of the client is not available in this release.</p>
CSCeb85931	In the Assisted Site Survey Wizard, the lock method should be implemented	<p>You can have a maximum of five Assisted Site Survey Wizard sessions, each using separate APs and clients, running at one time. There is currently no lock mechanism that prevents you from running more than one session on the same APs and clients.</p> <p>To work around this problem, do not run more than one session of the Assisted Site Survey Wizard on the same APs and clients.</p>
CSCec03535	Switch port detection does not work under some conditions.	<p>If you have a switch in a network that relies on trunking to pass packets and manage APs, but rogue AP ports are not trunk enabled, switch port detection fails.</p> <p>To work around this problem, enable trunking on the rogue AP's switch port.</p>
CSCec33330	A configuration job for a template which includes a banner command that spans multiple lines, will not complete successfully.	<p>If the configuration template used in the configuration job has banner command spanning multiple lines in the Custom Values section, the job may either report a failure or continue to appear in a Running state.</p> <p>To work around this problem either remove the banner command or make sure it only spans a single line, then run the configuration job again.</p>

Table 2 *Known Problems in the WLSE (Continued)*

Bug ID	Summary	Explanation
CSCec38013	When you upgrade to Release 2.5, the fault “Ethernet BV11 port is down” on IOS access points is not deleted.	<p>The IOS access point fault “Ethernet BV11 port is down” in a Release 2.0 WLSE is not deleted after an upgrade to WLSE Release 2.5.</p> <p>To work around this problem, after you upgrade to Release 2.5:</p> <ol style="list-style-type: none"> 1. Disable fault polling for the access point Ethernet Port Status Threshold. 2. Manually clear the 'Ethernet BV11 port is down' faults for the IOS access points.
CSCec40088	WDS server data defined in Release 2.0 Wireless Services templates is not retained after an upgrade to Release 2.5.	<p>If you created a template in Release 2.0, by selecting Configure > Templates > IOS > Wireless Services > WDS, and added server data, the data will not be retained when you upgrade to Release 2.5.</p> <p>To work around this problem, you will have to add the server data after you have upgraded to Release 2.5.</p>
CSCec41188	You cannot add a LEAP server to the WLSE if it is already a managed access point.	<p>You cannot add an access point, which is running the local RADIUS service and is managed as an access point by the WLSE, as a LEAP server. The WLSE will view it as a duplicate device.</p> <p>There is no workaround for this problem.</p>
CSCec42478	Dual band, non-IOS 1200 access points do not generate a Leap Disabled fault for the 802.11a RF port.	<p>When LEAP is disabled on the 802.11a RF port of a non-IOS, 1200 access point, it is not reported under Faults > Display Faults.</p> <p>This is a problem with the access point software, not the WLSE. Please refer to Bug ID CSCec47797.</p> <p>There is no workaround for this problem.</p>

Table 2 Known Problems in the WLSE (Continued)

Bug ID	Summary	Explanation
CSCec52282	You cannot use the CLI command ip domain-name to reset your domain.	<p>The CLI command IP domain-name does not work correctly.</p> <p>To work around this problem, use the CLI command erase config to erase the previous WLSE configuration, then run the setup program and enter your network information.</p>
CSCec53133	No Client Walkabout data is collected when you select “Use AP Current Power Setting.”	<p>When you chose the AP Power Setting in Client Walkabout, the “Use AP Current Power Setting” option does not work.</p> <p>To work around this problem, select one of the other options: Use AP Maximum Power Setting or Use No More than user-defined mW.</p>
CSCec54430	There are no SSIDs listed under Faults > Manage Fault Profiles > Access Point Policies > EAP per SSID Enforced for non-IOS, dual band, 1200 access points.	<p>Dual band, non-IOS 1200 access points running version 12.03T, fail to list the Available SSIDs for Radio 802.11a in the EAP per SSID Enforced policy under Faults > Manage Fault Profiles.</p> <p>There is no workaround for this problem.</p>
CSCec57354	AP350 radio interface might be disabled due to excessive scans after running for 11/2 days	<p>After running scans for 1 1/2 days, the AP radio interface might be disabled in some network environments.</p> <p>To work around this problem, do not schedule frequent AP radio scans in a 24-hour period. Instead, use Radio Monitoring, which is not service disrupting, to collect ongoing radio measurement data. Power cycle the AP if the radio interface is disabled.</p>
CSCec57502	When you export trend report data in a CSV format, some of the attributes are incomplete.	<p>When you use CSV format to export trend report data, the data in the CSV file is incomplete.</p> <p>There is no workaround for this problem.</p>

Table 2 *Known Problems in the WLSE (Continued)*

Bug ID	Summary	Explanation
CSCec59512	Duplicate EAP Disabled per SSID faults are generated for the 11b radio of dual band 1200 access point.	Dual band, 1200 access points generate duplicate EAP Disabled per SSID faults under Faults > Display Faults. There is no workaround for this problem.
CSCec64486	Firmware conversion jobs are reported as successful even though they are not.	Sometimes firmware conversions from non-IOS to IOS are terminated quickly and display as successful. However, the Job Run log indicates an error downloading the non-IOS configuration. To work around this problem, increase the SNMP timeout and retries for those devices, then run the job again.
CSCec70880	Disabling Interference Detection causes hung Radio Management processes	If you disable the Interference Detection fault setting (Faults>Manage Network-Wide Settings>Interference Detection), this can result in hung Radio Management operations (for example, radio scan). To work around this problem, never disable Interference Detection. If you are not interested in the interference faults, set the fault settings to the maximum values to reduce the number of interference faults generated.
CSCec70915	“SNMP unreachable” APs can cause Client Walkabout to never stop.	If any APs included in a client walkabout session are “SNMP unreachable,” client walkabout does not stop. This prevents other jobs (for example, radio scan and other client walkabout tasks) from running. The user interface indicates that the task has stopped, but the task is still running in the background. To work around this problem, make sure all APs you select for a client walkabout session are SNMP reachable before starting the client walkabout. If the client walkabout never stops, you need to restart WLSE.

Table 2 *Known Problems in the WLSE (Continued)*

Bug ID	Summary	Explanation
CSCec72920	After converting an non-IOS access point to an IOS access point, the correct native VLAN may not be configured.	<p>If you convert from a non-IOS access point to an IOS access point, and the non-IOS access point does not have a native VLAN configured, a VLAN will be automatically assigned as the native VLAN. However, the assigned native VLAN may not be correct.</p> <p>To work around this problem, log in to the access point and change the native VLAN to the correct one.</p>

Table 2 Known Problems in the WLSE (Continued)

Bug ID	Summary	Explanation
CSCsa03154	When you log in, you get the following error message: User role empty.	<p>After applying a patch, you may get an error message when you log in.</p> <p>To work around this problem, reboot the machine.</p>
CSCsa08621	When you use the CLI command interface to set the WLSE to half-duplex, the WLSE crashes.	<p>Setting the WLSE interface duplex mode may cause a catastrophic segmentation fault that corrupts the WLSE flash.</p> <p>There is no workaround for setting the duplex mode.</p> <p>Recovery requires erasing WLSE configuration in flash and rerunning the setup script.</p> <p>To recover, do the following:</p> <ol style="list-style-type: none"> 1. Connect to the WLSE console port 2. Power cycle the WLSE 3. When the WLSE powers up, wait for the GRUB loader to present you with OS options 4. At the GRUB loader, select CiscoBreR. This will boot you into the recovery image and present you with a Linux shell prompt. 5. At the shell prompt, type the command erase config. This will erase the flash (leaving the WLSE database intact), then reboot the WLSE. 6. When the WLSE reboots, you will be forced to rerun the setup script.

Table 3 *Resolved Problems in the WLSE*

Bug ID	Summary	Explanation
CSCdz34064	The number of clients seen in the AP Associations report and the Group Client Association report do not match.	<p>The data in the Number of Clients Connected field in the Group Client Association report is collected using the performance inventory. The client information displayed in the AP Associations Report is collected using the client inventory.</p> <p>Because the inventory polling frequencies for client and performance inventory are mismatched, the data in these reports do not always match.</p> <p>There is no workaround for this problem.</p> <p>However, in the case of some access points, you can use the Run Inventory Now and Scheduled Inventory features to synchronize the data.</p>
CSCea61722	The 1200 access point Cisco IOS images do not show up when importing from Cisco.com.	<p>When you try to import a Cisco IOS image for the AP 1200 from Cisco.com by selecting Firmware > Import > From Cisco.com, the image does not show up.</p> <p>To work around this problem, download the firmware image from Cisco.com, then import it to the WLSE by selecting Firmware > Import > From Desktop.</p>

Table 3 Resolved Problems in the WLSE (Continued)

Bug ID	Summary	Explanation
CSCea88793	A non-IOS to Cisco IOS access point conversion job is successful but is reported as not verified.	<p>When you run a non-IOS to IOS conversion job, the results are displayed as not verified even though the job is successful. The timeout and retries values need to be increased.</p> <p>To work around this problem, and to ensure that future jobs are successful, do the following:</p> <ol style="list-style-type: none"> 1. Access the Job Properties dialog box by entering the following URL: <code>http://wlse IP address:1741/debug/jobprops.jsp</code>. 2. Increase the value for <ul style="list-style-type: none"> – Vxworks to IOS SNMP timeout. – Vxworks to IOS SNMP retries. – Device reboot wait timeout.

Table 3 *Resolved Problems in the WLSE (Continued)*

Bug ID	Summary	Explanation
CSCeb19507	<p>An error message appears in the Install Software Updates window in two possible circumstances:</p> <ul style="list-style-type: none"> • After having upgraded to Release 2.0 from a previous release of the WLSE. • On a newly installed WLSE, Release 2.0. 	<p>After having upgraded to a WLSE 2.0 or after newly installing a WLSE 2.0, if you either:</p> <ol style="list-style-type: none"> 1. Use the CLI command <code>hostname</code> to change the hostname to one that is not configured under IP Name Server on the WLSE. 2. Use the CLI commands <code>services stop</code> then <code>services start</code> to stop then start services. <p>then the WLSE will not accept the host name change, and the following problems occur:</p> <ul style="list-style-type: none"> • An error message appears in the Install Software Updates window. • You cannot e-mail any log files (e.g. tomcat.log) in the View Log File window. • The “AAA Server is Not Available” fault is erroneously generated and stays in active state indefinitely even though the AAA servers are actually available. • Fault notification e-mails display the previous hostname, not the current one. <p>To work around this problem, use the CLI command <code>reload</code> after having executed foregoing two steps.</p>

Table 3 Resolved Problems in the WLSE (Continued)

Bug ID	Summary	Explanation
CSCeb32794	Specific trap host configuration using IOS configuration templates removes previously configured trap host configurations.	<p>Whenever a specific trap host is defined using the IOS configuration template, all previous specific trap host configuration commands are removed from the access point by the WLSE.</p> <p>For example, if you use the WLSE to configure host xxx.xxx.xxx.xxx to be the trap receiver for receiving hot standby switchover type traps, then push it to the access point, the access point will have this host as the trap receiver for switchover type traps. If the access point already has another trap receiver, yyy.yyy.yyy.yyy, configured to receive association and disassociation type traps, it will be removed.</p> <p>This is because the WLSE generates commands to disable all non switchover type traps (because this is the only type we selected in the template) from being generated.</p> <p>To work around this problem, select trap types that are already configured on the access point, in addition to the new trap type.</p> <p>Using the example above, if switchover and associate and disassociate type traps are selected, then the WLSE will not disable the associate and disassociate type traps.</p> <p>You can also use commands in the custom templates to work around this problem.</p>
CSCeb40356	When you rediscover an already-discovered device, inventory is not run automatically.	<p>When discovery is run on an already-discovered device, even though it is auto-managed, the inventory feature is not triggered.</p> <p>To work around this problem, you must run an on-demand inventory by selecting Administration > Discover > Inventory > Run Inventory Now, or wait for the next available inventory cycle.</p>

Table 3 *Resolved Problems in the WLSE (Continued)*

Bug ID	Summary	Explanation
CSCeb46145	The non-IOS to Cisco IOS upgrade images are not available from Cisco.com.	When you try to download an upgrade image from Cisco.com, the image does not show up. To work around this problem, download the firmware image from Cisco.com to your desktop, then import it to the WLSE by selecting Firmware > Import > From Desktop .

Table 3 Resolved Problems in the WLSE (Continued)

Bug ID	Summary	Explanation
CSCeb50004	<p>The View current faults for this setting link under Faults > Manage Profiles cannot be used to clear Vlan WEP key length policy violation faults.</p>	<p>When you display WEP Encryption per VLAN security policy profile under Faults > Manage Profiles, then click View current faults for this setting, the window for the previously selected link in a different policy window appears. This means that the VLAN WEP key length policy violation fault cannot be cleared using this link.</p> <p>To work around this problem:</p> <ol style="list-style-type: none"> 1. Select Faults > Display Faults 2. Select the Vlan WEP key length policy violation faults for the affected access points 3. Click Clear. <hr/> <p>When you select the WEP Key Length security policy window under Faults > Manage Profiles, then click View current faults for this setting, the window for the previously selected link in a different policy window appears. This means the WEP key length policy violation fault cannot be cleared using this link.</p> <p>To work around this problem:</p> <ol style="list-style-type: none"> 1. Select Faults > Display Faults 2. Select the Vlan WEP key length policy violation faults for the affected access points 3. Click Clear.
CSCeb52919	<p>Initial configuration of RADIUS TACACS+, or MS NT Domain authentication fails.</p>	<p>When you configure the RADIUS, TACACS+, or MS NT Domain authentication modules for the first time, the WLSE does not accept the configuration; it retains the original Local Authentication module.</p> <p>To work around this problem, configure the RADIUS, TACACS+, or MS NT Domain authentication modules a second time.</p>

Obtaining Documentation

Cisco provides several ways to obtain documentation, 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 on the World Wide Web at this URL:

<http://www.cisco.com/univercd/home/home.htm>

You can access the Cisco website at this URL:

<http://www.cisco.com>

International Cisco websites can be accessed from this URL:

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

Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which may have shipped with your product. The Documentation CD-ROM is updated regularly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual or quarterly subscription.

Registered Cisco.com users can order a single Documentation CD-ROM (product number DOC-CONDOCCD=) through the Cisco Ordering tool:

http://www.cisco.com/en/US/partner/ordering/ordering_place_order_ordering_tool_launch.html

All users can order annual or quarterly subscriptions through the online Subscription Store:

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

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpk/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:

<http://www.cisco.com/en/US/partner/ordering/index.shtml>

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can submit comments electronically on Cisco.com. On the Cisco Documentation home page, click **Feedback** at the top of the page.

You can send your comments in e-mail 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.

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, the Cisco Technical Assistance Center (TAC) provides 24-hour, award-winning technical support services, online and over the phone. Cisco.com features the Cisco TAC website as an online starting point for technical assistance.

Cisco TAC Website

The Cisco TAC website (<http://www.cisco.com/tac>) provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The Cisco TAC website is available 24 hours a day, 365 days a year.

Accessing all the tools on the Cisco TAC website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a login ID or password, register at this URL:

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

Opening a TAC Case

The online TAC Case Open Tool (<http://www.cisco.com/tac/caseopen>) is the fastest way to open P3 and P4 cases. (Your network is minimally impaired or you require product information). After you describe your situation, the TAC Case Open Tool automatically recommends resources for an immediate solution. If your issue is not resolved using these recommendations, your case will be assigned to a Cisco TAC engineer.

For P1 or P2 cases (your production network is down or severely degraded) or if you do not have Internet access, contact Cisco TAC by telephone. Cisco TAC engineers are assigned immediately to P1 and P2 cases to help keep your business operations running smoothly.

To open a case 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 listing of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml>

TAC Case Priority Definitions

To ensure that all cases are reported in a standard format, Cisco has established case priority definitions.

Priority 1 (P1)—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.

Priority 2 (P2)—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.

Priority 3 (P3)—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.

Priority 4 (P4)—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.

- The Cisco Product Catalog describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the Cisco Product Catalog at this URL:

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

- Cisco Press publishes a wide range of networking publications. Cisco suggests these titles for new and experienced users: Internetworking Terms and Acronyms Dictionary, Internetworking Technology Handbook, Internetworking Troubleshooting Guide, and the Internetworking Design Guide. For current Cisco Press titles and other information, go to Cisco Press online at this URL:

<http://www.ciscopress.com>

- Packet magazine is the Cisco quarterly publication that provides the latest networking trends, technology breakthroughs, and Cisco products and solutions to help industry professionals get the most from their networking investment. Included are networking deployment and troubleshooting tips,

configuration examples, customer case studies, tutorials and training, certification information, and links to numerous in-depth online resources. You can access Packet magazine at this URL:

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

- iQ Magazine is the Cisco bimonthly publication that delivers the latest information about Internet business strategies for executives. You can access iQ Magazine at this URL:

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

- 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/en/US/about/ac123/ac147/about_cisco_the_internet_protocol_journal.html

- Training—Cisco offers world-class networking training. Current offerings in network training are listed 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, iQuic Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, PIX, ProConnect ScriptShare, 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. (0709R)

Copyright © 2003 Cisco Systems, Inc.
All rights reserved.

 Printed in the USA on recycled paper containing 10% postconsumer waste.

