



Release Notes for 1100 Series Access Points for Cisco IOS Release 12.2(4)JA1

January 8, 2003

These release notes describe features, enhancements, and caveats for Cisco IOS Release 12.2(4)JA1. They also provide important information about 1100 series access points. Cisco IOS Release 12.2(4)JA1 fixes defect CSCdz60229.

Contents

These release notes contain the following sections:

- [Introduction, page 2](#)
- [System Requirements, page 2](#)
- [New Features, page 3](#)
- [Installation Notes, page 6](#)
- [Important Notes, page 7](#)
- [Caveats, page 7](#)
- [Troubleshooting, page 8](#)
- [Related Documentation, page 8](#)
- [Obtaining Documentation, page 12](#)
- [Obtaining Technical Assistance, page 13](#)



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

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

Introduction

The Cisco Aironet Access Point is a wireless LAN transceiver that can act as the connection point between wireless and wired networks or as the center point of a standalone wireless network. In large installations, the roaming functionality provided by multiple access points enables wireless users to move freely throughout the facility while maintaining uninterrupted access to the network.

You can configure and monitor the 1100 series access point using the command-line interface (CLI), the browser-based management system, or Simple Network Management Protocol (SNMP).

System Requirements

You must have an 1100 series access point to install Cisco IOS Release 12.2(4)JA1.

**Note**

Only 1100 series access points run Cisco IOS software; 1200, 350, and 340 series access points do not support Cisco IOS. Do not attempt to load a Cisco IOS image on a 1200, 350, or 340 series access point.

Determining the Software Version

To determine the version of Cisco IOS running on your access point, use a Telnet session to log into the access point and enter the **show version** EXEC command. This example shows command output from an access point running Cisco IOS Release 12.2(4)JA1:

```
ap1100>show version
Cisco Internetwork Operating System Software
IOS (tm) C1100 Software (C1100-K9W7-M), Version 12.2(4)JA1
Copyright (c) 1986-2002 by Cisco Systems, Inc.
```

You can also find the software version on the System Software Version page in the access point's web-browser interface.

Upgrading to a New Software Release

For instructions on installing access point software:

1. Follow this link to the Cisco Aironet documentation home page:
<http://www.cisco.com/univercd/cc/td/doc/product/wireless/index.htm>
2. Follow this path to the product, document, and chapter:
Aironet 1100 Series Wireless LAN Products > Cisco Aironet 1100 Series Access Points > Aironet 1100 Series Access Points, Cisco IOS Release 12.2(4)JA > Cisco Aironet 1100 Series Access Point Installation and Configuration Guide > Managing Firmware and Configurations > Working with Software Images
3. Click this link to browse to the Software Center on Cisco.com:
<http://www.cisco.com/public/sw-center/sw-wireless.shtml>
Select the **Cisco Aironet 1100 Series** link to download Cisco IOS version 12.2(4)JA1.

New Features

This section lists new features in Cisco IOS Release 12.2(4)JA, which are also included in Cisco IOS Release 12.2(4)JA1. These features, which existed in previous releases of Cisco access point firmware, were added to Cisco IOS in October, 2002.

Support for 802.11 Wireless Standards

Cisco IOS Release 12.2(4)JA supports IEEE 802.11 standards for wireless networking. This support enables interoperability under 802.11 specifications for network architecture, wireless association, and radio management. Support for 802.11 standards allows you to set the access point mode of operation (root or repeater), service set identifier (SSID), authentication type, channel selection, transmission rates, power-save mode, and security based on wired equivalent privacy (WEP), and other configurable fields.

Inter-Access Point Roaming

Clients who roam from one access point to another are supported with pre-standard services for seamless hand-off as defined under IEEE 802.11f Inter-Access Point Protocol (IAPP). When a client roams from one access point to another, the second access point sends a message to the first to update its association table, establishing a learning path to the client for the switch. This feature provides backward compatibility with the Cisco Aironet Data Delivery Protocol for inter-access point hand-off as implemented on 340, 350, and 1200 series access points.

**Note**

Wireless LAN users are sometimes concerned when a client device stays associated to a distant access point instead of roaming to a closer access point. However, if a client's signal to a distant access point remains strong, the client does not roam to a closer access point. If client devices checked constantly for closer access points, the extra radio traffic would slow throughput on the wireless LAN.

Multiple SSIDs

Access points can support up to 16 SSIDs, enabling flexible service deployment. You can configure each SSID for several parameters, creating up to 16 unique sets of services. Configurable parameters include mode for guest clients (enabling a broadcast SSID), client authentication method, maximum number of client associations, VLAN identifier, proxy Mobile IP, and RADIUS accounting list identifier. You can also designate an SSID as an infrastructure SSID that is used only by repeater access points.

World Mode

Each country regulates usage of the 2.4-GHz spectrum in its domain with respect to channel availability and allowable transmit power. The world mode feature automates client configuration of channel and transmit power settings by allowing world-mode-enabled access points to configure the settings on world-mode-enabled clients. For example, a user with a client device used primarily in Japan could rely on world mode to adjust its channel and power settings automatically when the user travels to Italy and joins a network there.

Configurable Radio Transmit Power

The transmit power of the access point radio can be configured from 1 mW up to 100 mW. You can manipulate the coverage area provided by the access point to meet your needs.

**Note**

The settings allowed in your regulatory domain might differ from the settings named here.

Link Diagnostics

This feature provides testing and diagnosis capabilities for the wireless interface's connectivity status and throughput performance. You can examine radio configuration information such as the operating channel, transmit power, supported data rates, and regulatory settings; run a link test; determine signal strength and quality; diagnose the client association and authentication process; and examine data packets sent over the radio interface.

Transparent Bridging

The access point bridges the network between the wired infrastructure and wireless devices, switching traffic between the radio and Ethernet interfaces. This feature provides transparent bridging and forwarding logic between these interfaces.

VLAN over Wireless

You use VLANs to partition your network into logical subnets that are independent of physical location. This allows you to differentiate services such as network access for network users. This feature defines 802.1q VLANs for wireless LANs, using a VLAN identifier in the Ethernet frame. Up to 16 VLANs, one per SSID, are supported in this release.

QoS over Wireless

This feature enables the access point to provide traffic prioritization services over the wireless interface for standards-based quality of service (QoS). This feature prioritizes traffic based on the 802.1p tag in the Ethernet header or the IP type of service/Differentiated Services Code Point (TOS/DSCP) bits in the IP header.

Proxy Mobile IP

This release supports the proxy Mobile IP protocol for seamless inter-subnet roaming. When you enable proxy Mobile IP on your access points, client devices that roam from one subnet to the next maintain their IP address and session. The access point acts as a mobile IP proxy for clients devices that do not have Mobile IP software installed. The access point informs the foreign agent router that the client has roamed to another subnet, while the foreign agent directs the home agent to reroute packets to it.

Hot Standby

This feature enables you to add redundant reliability to your wireless LAN by installing a standby access point as a backup for a primary device and configuring it for hot standby. When installed on the same Ethernet LAN and configured consistently as a primary device, the standby device associates to

the primary device as a client and monitors the primary device with periodic link test request packets sent over both the Ethernet and wireless interfaces. The standby device assumes the role of access point by activating its Ethernet port and accepting radio client associations if the primary device fails to respond with a link test response packet.

Load Balancing

The load-balancing feature optimizes aggregate bandwidth with intelligent user associations, resulting in a better load distribution. At initialization, the client polls all access points within range for the device load information, and selects the one with the lightest load. The access point interprets the request and provides loading information to the client.

HTTP Server

This feature enables Web-based graphical user interface (GUI) management by providing support for HTML Web pages and Common Gateway Interface (CGI) scripts using common Web browsers. You must use Microsoft Internet Explorer (version 5.x or later) or Netscape Navigator (version 4.x) to open the web-browser interface.

MIBs

This release provides support for standard and Cisco Enterprise MIB I and MIB II. For a complete list of supported MIBs, refer to Appendix F, “Supported MIBs,” in the *Cisco Aironet 1100 Series Access Point Installation and Configuration Guide*.

Access Control Lists

Access control lists allow filtering of traffic based on identifiable attributes within an Ethernet frame. You can filter data based on source or destination addresses, protocol used, protocol-specific options (Telnet, FTP, HTTP, and SNMP), and Media Access Control (MAC) address.

802.1X, EAP

This Cisco Wireless Security Suite feature supports the 802.1X standard port-based authentication framework including EAP Cisco Wireless (LEAP), Protected Extensible Authentication Protocol (PEAP), Extensible Authentication Protocol Transport Layer Security (EAP-TLS), and EAP-Tunneled TLS (EAP-TTLS).

Key Hashing (Temporal Key Integrity Protocol)

With this pre-standard implementation of the key hashing technique, the base key and packet-unique initialization vector are hashed together to create a new, per-packet key. This procedure mitigates passive attacks that attempt to determine the base key by accumulating weak initialization vectors. Key hashing is a component of the Cisco Wireless Security Suite pre-standard Temporal Key Integrity Protocol (TKIP), which is part of the draft for IEEE 802.11i enhanced wireless security.

Message Integrity Check

This feature supports a pre-standard implementation of the MIC protocol. With this feature, the access point validates that packets received from the client have not been tampered with by calculating the packet checksum and comparing it to the checksum calculated and sent by the client. This feature prevents active attacks such as bit-flipping attacks. MIC is also a component of the Cisco Wireless Security Suite pre-standard TKIP.

Broadcast Key Rotation

You use this Cisco Wireless Security Suite feature to set a timeout for the shared broadcast key, causing a new broadcast key to be generated. This feature mitigates passive attacks that attempt to determine the broadcast key from weak initialization vectors.

Installation Notes

This section lists information you should keep in mind when installing 1100 series access points.

Installation in Environmental Air Space

The 1100 series access point provides adequate fire resistance and low smoke-producing characteristics suitable for operation in a building's environmental air space, such as above suspended ceilings, in accordance with Section 300-22(C) of the *National Electrical Code* (NEC) and Sections 2-128, 12-010(3) and 12-100 of the *Canadian Electrical Code*, Part 1, C22.1.

**Caution**

The power injector is not intended for use in extremely high or low temperatures or in environmental air spaces, such as above suspended ceilings.

Power Considerations

**Caution**

The operational voltage range for 1100 series access points is 24 to 60 VDC, and the nominal voltage is 48 VDC. Voltage higher than 60 VDC can damage the equipment.

**Caution**

Cisco Aironet power injectors are designed for use with Cisco Aironet access points and bridges only. *Do not use the power injector with any other Ethernet-ready device.* Using the power injector with other Ethernet-ready devices can damage the equipment.

Important Notes

This section describes important information about the access point.

Radio MAC Address Appears in ACU

When a Cisco Aironet client device associates to an 1100 series access point, the access point MAC address that appears on the Status page in the Aironet Client Utility (ACU) is the MAC address for the access point radio. The MAC address for the access point Ethernet port is printed on the label on the back of the access point.

Caveats

This section lists resolved and open caveats in Cisco IOS Release 12.2(4)JA1.

Resolved Caveats

This caveat is resolved in Cisco IOS Release 12.2(4)JA1:

- Resolved: CSCdz60229—Access points are no longer vulnerable to a denial of service (DoS) when support for the Secure Shell (SSH) server is enabled. Malformed SSH packets directed at the access point no longer cause a reload of the device. Support for SSH is disabled by default.

Open Caveats

These caveats are open in Cisco IOS Release 12.2(4)JA1:

- CSCdy48684—If a client device is associated to a repeater access point and you clear the client on the repeater's parent access point, the repeater's virtual interface toggles on the parent access point, and the repeater must reassociate to the parent access point. Workaround: Log into the repeater access point, where the client is directly associated, and enter the **clear dot11 client H.H.H** command in the CLI to clear the client.
- CSCdy69161—The web-browser interface does not include a setting for limiting the radio transmit power of client devices associated to the access point. To enable this feature, use the **power client** command in the CLI.
- CSCdy69605—When a Symbol 802.11 phone associates to an access point using an SSID that contains more than 9 characters, the Symbol frequently disassociates, reassociates, and disassociates again. Workaround: Configure an SSID containing less than 9 characters, and configure the Symbol phones to associate using that SSID.
- CsCdy72333—When VLANs are enabled, you cannot use the web-browser interface to enable PSPF for the radio sub-interfaces. Workaround: Using the access point CLI, enter these commands to enable PSPF for a VLAN:

```
ap1100# configure terminal
ap1100(config)# interface dot11radio0.<vlan id>
ap1100(config-subif)# bridge-group <vlan id> port-protected
```

- CSCdy73237—The access point radio driver can enter a loop in which the driver tries to start the radio, the radio firmware reports an invalid configuration, the radio does not start, and the driver tries to start the radio again. This loop can occur when you use this configuration: you configure the access point to use VLANs; at least one VLAN has encryption; an SSID is configured to use shared key authentication and that SSID is assigned to a VLAN that has no encryption keys defined. Workaround: Make sure that the VLAN you use for shared key authentication has encryption enabled and at least one encryption key defined before the SSID is assigned to that VLAN. If the loop has already occurred, assign an encryption key to the unencrypted VLAN.
- CSCdy73490—When you upgrade access point software from the web-browser interface, errors that cause the upgrade to fail appear only on the CLI, and the web-browser interface does not indicate that the upgrade failed. Workaround: If the system software version number on the web-browser System Software page has not changed after an upgrade, use the privileged EXEC **show logging** command on the CLI to check for errors that occurred during the upgrade.
- CSCdy74184—The SNMP command **dot1qVlanCurrentTable** does not retrieve all the VLANs configured on the access point when one of the VLAN identifiers uses continuous characters, such as 1234. Workaround: Use the SNMP **get** and **get-next** commands to view the dot1qVlanCurrentTable.
- CSCdy74230—If the access point boots up when it is connected to a switch port that is in shut mode, the access point does not start its bridge virtual interface (BVI) even after the switch port is changed to no shut mode. Workaround: Power off the access point, change the switch port to no shut mode, and power up the access point; or, issue a **shut** command and a **no shut** command to the switch port.
- CSCdy75398—If you use SNMP to change the authentication method for an existing SSID, you cannot change it again. Workaround: If you need to change the authentication method twice for an SSID, delete the SSID and re-create it.
- CSCdy79971—The contents of the Software Image Filename field are incomplete on the System Software: Software Upgrade: TFTP Upgrade page in the web-browser interface. Workaround: View the system image filename on a different page, such as the System Software: Software Upgrade: HTTP Upgrade page.

Troubleshooting

For the most up-to-date, detailed troubleshooting information, refer to the Cisco TAC website at <http://www.cisco.com/tac>. Select **Wireless LAN** under Top Issues.

Related Documentation

This section lists documents related to Cisco IOS Release 12.2(4)JA1 and to 1100 series access points.

Platform-Specific Documents

These documents describe installation and configuration of 1100 series access points:

- *Quick Start Guide: Cisco Aironet 1100 Series Access Points*
- *Cisco Aironet 1100 Series Access Point Installation and Configuration Guide*
- *Cisco Aironet 1100 Series Access Point Command Reference*
- *Installation Instructions for Cisco Aironet Power Injectors*

Cisco IOS Software Documentation Set

[Table 1](#) lists the contents of the Cisco IOS Release 12.2 software documentation set. These documents are available in electronic form, and you can order them in printed form.

You can find the most current Cisco IOS documentation on Cisco.com. Follow this link path to find the documentation for Cisco IOS Release 12.2:

Technical Documents: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 12.2

Table 1 Cisco IOS Release 12.2 Documentation Set

Books	Major Topics
<ul style="list-style-type: none"> <i>Cisco IOS Configuration Fundamentals Configuration Guide</i> <i>Cisco IOS Configuration Fundamentals Command Reference</i> 	Cisco IOS User Interfaces File Management System Management
<ul style="list-style-type: none"> <i>Cisco IOS Bridging and IBM Networking Configuration Guide</i> <i>Cisco IOS Bridging and IBM Networking Command Reference, Volume 1 of 2</i> <i>Cisco IOS Bridging and IBM Networking Command Reference, Volume 2 of 2</i> 	Transparent Bridging SRB Token Ring Inter-Switch Link Token Ring Route Switch Module RSRB DLSW+ Serial Tunnel and Block Serial Tunnel LLC2 and SDLC IBM Network Media Translation SNA Frame Relay Access NCIA Client/Server Airline Product Set DSPU and SNA Service Point SNA Switching Services Cisco Transaction Connection Cisco Mainframe Channel Connection CLAW and TCP/IP Offload CSNA, CMPC, and CMPC+ TN3270 Server
<ul style="list-style-type: none"> <i>Cisco IOS Dial Technologies Configuration Guide: Dial Access</i> <i>Cisco IOS Dial Technologies Configuration Guide: Large-Scale Dial Applications</i> <i>Cisco IOS Dial Technologies Command Reference, Volume 1 of 2</i> <i>Cisco IOS Dial Technologies Command Reference, Volume 2 of 2</i> 	Dial Access Modem and Dial Shelf Configuration and Management ISDN Configuration Signaling Configuration Point-to-Point Protocols Dial-on-Demand Routing Dial Backup Dial Related Addressing Service Network Access Solutions Large-Scale Dial Solutions Cost-Control Solutions Internetworking Dial Access Scenarios

Table 1 Cisco IOS Release 12.2 Documentation Set (continued)

Books	Major Topics
<ul style="list-style-type: none"> • <i>Cisco IOS Interface Configuration Guide</i> • <i>Cisco IOS Interface Command Reference</i> 	LAN Interfaces Serial Interfaces Logical Interfaces
<ul style="list-style-type: none"> • <i>Cisco IOS IP Configuration Guide</i> • <i>Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services</i> • <i>Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols</i> • <i>Cisco IOS IP Command Reference, Volume 3 of 3: Multicast</i> 	IP Addressing IP Services IP Routing Protocols IP Multicast
<ul style="list-style-type: none"> • <i>Cisco IOS AppleTalk and Novell IPX Configuration Guide</i> • <i>Cisco IOS AppleTalk and Novell IPX Command Reference</i> 	AppleTalk Novell IPX
<ul style="list-style-type: none"> • <i>Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS, and XNS Configuration Guide</i> • <i>Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS, and XNS Command Reference</i> 	Apollo Domain Banyan VINES DECnet ISO CLNS XNS
<ul style="list-style-type: none"> • <i>Cisco IOS Voice, Video, and Fax Configuration Guide</i> • <i>Cisco IOS Voice, Video, and Fax Command Reference</i> 	Voice over IP Call Control Signaling Voice over Frame Relay Voice over ATM Telephony Applications Trunk Management Fax, Video, and Modem Support
<ul style="list-style-type: none"> • <i>Cisco IOS Quality of Service Solutions Configuration Guide</i> • <i>Cisco IOS Quality of Service Solutions Command Reference</i> 	Packet Classification Congestion Management Congestion Avoidance Policing and Shaping Signaling Link Efficiency Mechanisms
<ul style="list-style-type: none"> • <i>Cisco IOS Security Configuration Guide</i> • <i>Cisco IOS Security Command Reference</i> 	AAA Security Services Security Server Protocols Traffic Filtering and Firewalls IP Security and Encryption Passwords and Privileges Neighbor Router Authentication IP Security Options Supported AV Pairs

Table 1 Cisco IOS Release 12.2 Documentation Set (continued)

Books	Major Topics
<ul style="list-style-type: none"> • <i>Cisco IOS Switching Services Configuration Guide</i> • <i>Cisco IOS Switching Services Command Reference</i> 	Cisco IOS Switching Paths NetFlow Switching Multiprotocol Label Switching Multilayer Switching Multicast Distributed Switching Virtual LANs LAN Emulation
<ul style="list-style-type: none"> • <i>Cisco IOS Wide-Area Networking Configuration Guide</i> • <i>Cisco IOS Wide-Area Networking Command Reference</i> 	ATM Frame Relay SMDS X.25 and LAPB
<ul style="list-style-type: none"> • <i>Cisco IOS Mobile Wireless Configuration Guide</i> • <i>Cisco IOS Mobile Wireless Command Reference</i> 	General Packet Radio Service
<ul style="list-style-type: none"> • <i>Cisco IOS Terminal Services Configuration Guide</i> • <i>Cisco IOS Terminal Services Command Reference</i> 	ARA LAT NASI Telnet TN3270 XRemote X.28 PAD Protocol Translation
<ul style="list-style-type: none"> • <i>Cisco IOS Configuration Guide Master Index</i> • <i>Cisco IOS Command Reference Master Index</i> • <i>Cisco IOS Debug Command Reference</i> • <i>Cisco IOS Software System Error Messages</i> • <i>New Features in 12.2-Based Limited Lifetime Releases</i> • <i>New Features in Release 12.2 T</i> • Release Notes (Release note and caveat documentation for 12.2-based releases and various platforms) 	

Obtaining Documentation

These sections explain how to obtain documentation from Cisco Systems.

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at this URL:

<http://www.cisco.com>

Translated documentation is available at 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 might be included with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual subscription.

Ordering Documentation

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/cgi-bin/order/order_root.pl
- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:
<http://www.cisco.com/go/subscription>
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, U.S.A.) 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. In the Cisco Documentation home page, click the **Fax** or **Email** option in the “Leave Feedback” section at the bottom of the page.

You can e-mail your comments to bug-doc@cisco.com.

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

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

Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain online documentation, troubleshooting tips, and sample configurations from online tools by using the Cisco Technical Assistance Center (TAC) Web Site. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC Web Site.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com is a highly integrated Internet application and a powerful, easy-to-use tool that provides a broad range of features and services to help you with these tasks:

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

If you want to obtain customized information and service, you can self-register on Cisco.com. To access Cisco.com, go to this URL:

<http://www.cisco.com>

Technical Assistance Center

The Cisco Technical Assistance Center (TAC) is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two levels of support are available: the Cisco TAC Web Site and the Cisco TAC Escalation Center.

Cisco TAC inquiries are categorized according to the urgency of the issue:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration.
- Priority level 3 (P3)—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- Priority level 2 (P2)—Your production network is severely degraded, affecting significant aspects of business operations. No workaround is available.
- Priority level 1 (P1)—Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No workaround is available.

The Cisco TAC resource that you choose is based on the priority of the problem and the conditions of service contracts, when applicable.

Cisco TAC Web Site

You can use the Cisco TAC Web Site to resolve P3 and P4 issues yourself, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco TAC Web Site, go to this URL:

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

All customers, partners, and resellers who have a valid Cisco service contract have complete access to the technical support resources on the Cisco TAC Web Site. The Cisco TAC Web Site requires a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to this URL to register:

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

If you are a Cisco.com registered user, and you cannot resolve your technical issues by using the Cisco TAC Web Site, you can open a case online by using the TAC Case Open tool at this URL:

<http://www.cisco.com/tac/caseopen>

If you have Internet access, we recommend that you open P3 and P4 cases through the Cisco TAC Web Site.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses priority level 1 or priority level 2 issues. These classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer automatically opens a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to this URL:

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

Before calling, please check with your network operations center to determine the level of Cisco support services to which your company is entitled: for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). When you call the center, please have available your service agreement number and your product serial number.

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



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