Release Notes for Cisco Wireless LAN Controllers and Lightweight Access Points for Release 3.2.116.21

March 3, 2006

These release notes describe new and changed information as well as open and resolved caveats for operating system release 3.2.116.21 for Cisco 2000, 4100, and 4400 Series Wireless LAN Controllers; Cisco Wireless Services Modules (WiSM); Cisco Wireless LAN Controller Network Modules; and Cisco Aironet 1000, 1130, 1200, 1240, and 1500 Series Lightweight Access Points, which comprise part of the Cisco Unified Wireless Network (Cisco UWN) Solution.

Note Unless otherwise noted, all of the Cisco wireless LAN controllers are hereafter referred to as *controllers*, and all of the Cisco lightweight access points are hereafter referred to as *access points.*

Contents

These release notes contain the following sections:

CISCO SYSTEMS

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

Cisco Unified Wireless Network Solution Components

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

• Operating system software release 3.2.116.21 for all Cisco controllers and lightweight access points

• Cisco Wireless Control System (WCS) software release 3.2.51.0

• Location appliance software release 2.0.42.0

• Cisco 2700 Series Location Appliances

• Cisco 2000, 4100, and 4400 Series Wireless LAN Controllers

• Cisco Wireless Service Module (WiSM) for Cisco Catalyst 6500 Series Switches

• Cisco Wireless LAN Controller Network Module for Cisco Integrated Services Routers

• Cisco Aironet 1000, 1130, 1200, 1240, and 1500 Lightweight Access Points

Controller Requirements

The controller graphical user interface (GUI) requires the following operating system and web browser:

• Windows XP SP1 or higher or Windows 2000 SP4 or higher

• Internet Explorer 6.0 SP1 or higher

Note   Opera, Mozilla, and Netscape are not supported.

Software Release Information

Operating system software is factory installed on your controller and automatically downloaded to the access points after a release upgrade and whenever an access point associates to a controller. As new releases become available for the controllers and their associated access points, consider upgrading.

Note   The Cisco WiSM requires software release SWISMK9-32 or later.

Finding the Software Release

To find the software release running on your controller, look on the Monitor > Summary page of the controller GUI or enter **show sysinfo** on the controller command line interface (CLI).

Upgrading to a New Software Release

When a controller is upgraded, the code on its associated access points is also automatically upgraded. When an access point is loading code, each of its lights blinks in succession.

⚠️
Caution Do not power down the controller or any access point during this process; otherwise, you might corrupt the software image! Upgrading a controller with a large number of access points can take as long as 30 minutes. The access points must remain powered, and the controller must not be reset during this time.

Cisco recommends the following sequence when performing an upgrade:

1. Upload your controller configuration files to a server to back them up.

2. Turn off the controller 802.11a and 802.11b networks.

3. Upgrade your controller to software release 3.2.116.21, following the instructions in the *Cisco Wireless LAN Controller Configuration Guide, Release 3.2*. Click this link to browse to that document:

   http://www.cisco.com/en/US/products/ps6366/products_installation_and_configuration_guides_list.html

4. Re-enable your 802.11a and 802.11b networks.

✎
Note Controllers can be upgraded from one release to another. However, should you require a downgrade from one release to another, you may be unable to use the higher release configuration. The workaround is to reload the previous controller configuration files saved on the backup server or to reconfigure the controller.

New and Changed Information

VPN Termination Module for the 4400 Series Controllers

A virtual private network (VPN) termination hardware module is being released for the 4400 series controllers. As with the VPN termination module available today for the 4100 series controllers, this module enables the 4400 series controllers to terminate VPN client sessions directly on the controller. The module features these capabilities:

- Support for one VPN termination module on the 4402 controller and one or two VPN termination modules on the 4404 controller
- On the 4404 controller, one ESM that is shared across both NPUs
- Automatic load balancing across modules if two modules are installed for the 4404 controller
- Retention of the client crypto state on the original crypto card when the client moves between access points on different NPUs
- Support for up to 1000 client VPN sessions per module
- Up to 1 Gbps of encryption/decryption per module
- Support for these IPsec clients: Cisco VPN Client, NetScreen Remote, SSH Sentinel, and Openswan

802.3 Bridging

Cisco 2000 series controllers support 802.3 bridging in software release 3.2.116.21. This feature is disabled by default. However, you can enable or disable it through the controller CLI by entering this command:

config network 802.3-bridging {**enable** | **disable**}

When 802.3 bridging is enabled, all of the 802.3 frames are forwarded to or from the client. The original LLC/SNAP and length of the frame is preserved during encapsulation or de-capsulation of the LWAPP data frame. For short frames, the trailer is stripped before adding the LWAPP header. Tunneling of 802.3 frames is not supported.

Note 802.3 bridging is supported only on 2000 series controllers and can be enabled or disabled only through the CLI.

Configurable DHCP Proxy

DHCP proxy is configurable in software release 3.2.116.21 using the following command:

config dhcp proxy {**enable** | **disable**}

Note When you choose the disable option, modification of the dhcp proxy packets is reduced to the level of a relay.

New LWAPP Power Injector Commands

Two new LWAPP power injector commands are available in software release 3.2.116.21. These commands are used when the access point is powered by a power injector that is connected to a Cisco pre-Intelligent Power Management (pre-IPM) switch.

- **config ap power injector enable ap installed**

  This command is recommended when the customer's network contains any older Cisco 6-Watt switches that could be accidentally overloaded if connected directly to the 12-Watt access point. The access point remembers that a power injector is connected to this particular switch port. If the access point is relocated, this command must be re-issued after the presence of a new power injector is verified.

- **config ap power injector enable ap override**

  This command is acceptable to use when the customer's network does not contain any older Cisco 6-Watt switches that could be overloaded if connected directly to the 12-Watt access point. The access point assumes that a power injector is always connected. If the access point is relocated, it continues to assume that a power injector is present.

Support for WPA1 and WPA2 Hex Keys

Cisco controllers support WPA1 and WPA2 hex keys in software release 3.2.116.21. You can specify these keys through the controller CLI by entering these commands:

config wlan security wpa1 pre-shared-key {**enable** | **disable**} *wlan_id* {**ascii** | **hex**} *key*

config wlan security wpa2 pre-shared-key {**enable** | **disable}** *wlan_id* {**ascii** | **hex**} *key*

Installation Notes

This section contains important information to keep in mind when installing your controllers and access points.

Warnings

Warning   **This warning means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents.**

Warning   **Only trained and qualified personnel should be allowed to install, replace, or service this equipment.**

Warning   **Do not locate any antenna near overhead power lines or other electric light or power circuits, or where it can come into contact with such circuits. When installing antennas, take extreme care not to come in contact with such circuits, as they may cause serious injury or death. For proper installation and grounding of the antenna, refer to national and local codes (e.g. U.S.: NFPA70, National Electrical Code, Article 810, in Canada: Canadian Electrical Code, Section 54).**

Warning   **This product relies on the building's installation for short-circuit (overcurrent) protection. Ensure that the protective device is rated not greater than 120 VAC, 15A U.S. (240vac, 10A International).**

Warning   **This equipment must be grounded. Never defeat the ground conductor or operate the equipment in the absence of a suitably installed ground connector. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available.**

Warning   **Read the installation instructions before you connect the system to its power source.**

Warning   **Do not work on the system or disconnect cables during periods of lightning activity.**

Warning **Do not operate your wireless network near unshielded blasting caps or in an explosive environment unless the device has been modified to be especially qualified for such use.**

Warning **In order to comply with radio frequency (RF) exposure limits, the antennas for this product should be positioned no less than 6.56 ft (2 m) from your body or nearby persons.**

Warning **This unit is intended for installation in restricted access areas. A restricted access area can be accessed only through the use of a special tool, lock and key, or other means of security.**

Safety Information

Follow the guidelines in this section to ensure proper operation and safe use of the controllers and access points.

FCC Safety Compliance Statement

FCC Compliance with its action in ET Docket 96-8, has adopted a safety standard for human exposure to RF electromagnetic energy emitted by FCC certified equipment. When used with approved Cisco Aironet antennas, Cisco Aironet products meet the uncontrolled environmental limits found in OET-65 and ANSI C95.1, 1991. Proper operation of this radio device according to the instructions in this publication results in user exposure substantially below the FCC recommended limits.

Safety Precautions

Each year hundreds of people are killed or injured when attempting to install an antenna. In many of these cases, the victim was aware of the danger of electrocution but did not take adequate steps to avoid the hazard.

For your safety, and to help you achieve a good installation, read and follow these safety precautions. **They may save your life!**

1. If you are installing an antenna for the first time, for your own safety as well as others, seek professional assistance. Your Cisco sales representative can explain which mounting method to use for the size and type of antenna you are about to install.

2. Select your installation site with safety as well as performance in mind. Electric power lines and phone lines look alike. For your safety, assume that any overhead line can kill you.

3. Call your electric power company. Tell them your plans and ask them to come look at your proposed installation. This is a small inconvenience considering your life is at stake.

4. Plan your installation carefully and completely before you begin. Successfully raising a mast or tower is largely a matter of coordination. Each person should be assigned to a specific task and should know what to do and when to do it. One person should be in charge of the operation to issue instructions and watch for signs of trouble.

5. When installing an antenna, remember:

 a. **Do not** use a metal ladder.

 b. **Do not** work on a wet or windy day.

 c. **Do** dress properly—shoes with rubber soles and heels, rubber gloves, and a long-sleeved shirt or jacket.

6. If the assembly starts to drop, get away from it and let it fall. Remember that the antenna, mast, cable, and metal guy wires are all excellent conductors of electrical current. Even the slightest touch of any of these parts to a power line completes an electrical path through the antenna and the installer: **you!**

7. If any part of an antenna system should come in contact with a power line, **do not touch it or try to remove it yourself. Call your local power company**. They will remove it safely.

8. If an accident should occur with the power lines, call for qualified emergency help immediately.

Installation Instructions

Refer to the appropriate Quick Start Guide or Hardware Installation Guide for instructions on installing your controllers and access points.

Note To meet regulatory restrictions, all external antenna configurations must be professionally installed.

Personnel installing the controllers and access points must understand wireless techniques and grounding methods. Access points with internal antennas can be installed by an experienced IT professional.

The controller must be installed by a network administrator or qualified IT professional, and the proper country code must be selected. Following installation, access to the controller should be password protected by the installer to maintain compliance with regulatory requirements and ensure proper unit functionality.

Important Notes

This section describes important information about the controllers and access points.

FIPS 140-2

The Cisco 4400 Series Controllers are on the NIST FIPS 140-2 Pre-Validation List.

Controllers Must Run Release 3.2.116.21 to Support -P Regulatory Domain

To support access points configured for use in Japan, you must upgrade the controller software to release 3.2.116.21. Earlier releases do not support access points configured for use in Japan (regulatory domain -P).

Voice WLAN Configuration

Cisco recommends that load balancing always be turned off in any wireless LAN that is supporting voice, regardless of vendor. When load balancing is turned on, voice clients can hear an audible artifact when roaming, and the handset is refused at its first reassociation attempt.

Inter-Subnet Roaming

Currently, multicast traffic cannot be passed during inter-subnet roaming.

Operating Mesh Networks Through Switches and Routers

In mesh networks that operate through low-speed switches and routers, access points can disconnect from the controller, causing the controller to generate alerts.

Heavily Loaded Controller CPU

When the controller CPU is heavily loaded (for example, when doing file copies or other tasks), it does not have time to process all of the ACKs that the NPU sends in response to configuration messages. When this happens, the CPU generates error messages. However, the error messages do not impact service or functionality.

RADIUS Servers and the Management VLAN

The RADIUS server can be on any subnet as long as it can be reached by the management VLAN subnet.

The controllers can be managed via the management VLAN subnet from any other subnet that can reach the management VLAN subnet.

Cisco 7920 Wireless IP Phone Support

When using Cisco 7920 Wireless IP Phones with controllers, make sure that the phones and controllers are configured as follows:

- Aggressive load balancing must be disabled on a per-controller basis. Otherwise, the initial roam attempt by the phone may fail, causing a disruption in the audio path.
- The QoS Basis Service Set (QBSS) information element (IE) must be enabled. The QBSS IE enables the access points to communicate their channel usage to wireless devices. Because access points with high channel usage might not be able to handle real-time traffic effectively, the 7920 phone uses the QBSS value to determine if it should associate with another access point. Use the following commands to enable the QBSS IE:
  - **sh wlan summary**

    ✎
    Note   Use this command to determine the WLAN ID number of the WLAN to which you want to add QBSS support.

- **config wlan disable** *wlan_id_number*
- **config wlan 7920-support ap-cac-limit enable** *wlan_id_number*
- **config wlan enable** *wlan_id_number*
- **sh wlan** *wlan_id_number*

> **Note** Use this command to verify that the WLAN is enabled and the Dot11-Phone Mode (7920) field is configured for compat mode.

- **save config**

- The Dynamic Transmit Power Control (DTPC) information element (IE) must be enabled using the **config 802.11a dtpc enable** command. The DTPC IE is a beacon and probe information element that allows the access point to broadcast information on its transmit power. The Cisco 7920 Wireless IP Phone uses this information to automatically adjust its transmit power to the same level as the access point to which it is associated. In this manner, both devices are transmitting at the same level.

- The 7920 phones and the controllers do not currently use compatible fast roaming mechanisms. The phone uses CCKM while the controllers use proactive key caching (PKC). To minimize roaming latency, static WEP is the recommended security mechanism.

- When configuring WEP, there is a difference in nomenclature for the controller and the 7920 phone. Configure the controller for 104 bits when using 128-bit WEP for the 7920.

Exclusion List (Blacklist) Client Feature

If a client is not able to connect to an access point and the security policy for the WLAN and/or client is correct, the client has probably been disabled. In the controller GUI, you can view the client's status on the Monitor > Summary page under Client Summary. If the client is disabled, click **Remove** to clear the disabled state for that client. The client automatically comes back and, if necessary, reattempts authentication.

Automatic disabling happens as a result of too many failed authentications. Clients disabled due to failed authorization do not appear on the permanent disable display. This display is only for those MACs that are set as permanently disabled by the administrator.

IPSec Clients Supported in This Release

This operating system release has been tested with the following IPSec clients:

- NetScreen v10.1.1 (build 10)
- Cisco VPN Client v4.6.04
- SSH Sentinel v1.4.1
- Openswan v2.4.0

> **Note** The Netscreen client does not handle fragmented ICMP packets, does not respond to large ping packets, and does not work with certificates. Other IP fragmented traffic should work correctly.

Maximum MAC Filter Entries

The controller database can contain up to 2048 MAC filter entries for local netusers.

Client Channel Changes

Cisco access points are known to go off channel for up to 30 seconds while identifying rogue access point threats. This activity can cause occasional dropped client connections.

Cisco Aironet 1030 Remote Edge Lightweight Access Points and WPA2-PSK

Cisco Aironet 1030 Remote Edge Lightweight Access Points do not support WPA2-PSK in REAP standalone mode.

XAuth Configuration with NetScreen

To initiate an XAuth session, configure XAuth on the controller and enable extended authentication on the NetScreen client.

Rekeys Not Supported with Cisco VPN Client

If a rekey occurs, clients must reauthenticate. To mitigate this problem, navigate to the WLANs > Edit page in the controller GUI, choose **IPsec** from the Layer 3 Security drop-down box, and change the Lifetime setting at the bottom of the page to a large value, such as 28800 seconds (this is the default value), depending upon your security requirements.

RADIUS Servers

This product has been tested with the following RADIUS servers:

* CiscoSecure ACS v3.2
* Funk Odyssey Client v1.1 and 2.0
* Funk Steel-Belted RADIUS release 4.71.739 and 5.03 Enterprise Edition
* Microsoft Internet Authentication Service (IAS) release 5.2.3790.1830 on Windows 2003 server

Management Usernames and Local Netuser Names

Management usernames and local netuser names must be unique because they are stored in the same database. That is, you cannot assign the same name to a management user and a local netuser.

802.1x and Microsoft Wireless Configuration Manager

Clients using the Microsoft Wireless Configuration Manager and 802.1x must use WLANs configured for 40- or 104-bit key length. Configuring for 128-bit key length results in clients that can associate but not authenticate.

Cisco Aironet 1030 Remote Edge Lightweight Access Point Default Operation

When a controller reboots, dropped Cisco Aironet 1030 Remote Edge Lightweight Access Points attempt to associate to any available controller. If the access points cannot contact a controller, they continue to offer 802.11a/b/g service on WLAN 1 only.

WEP Keys

This release supports four separate WEP index keys. These keys cannot be duplicated between WLANs. At most, four WEP WLANs can be configured on a controller. Each of these WLANs must use a different key index.

Using the Backup Image

The controller bootloader (ppcboot) stores a copy of the active primary image and the backup image. If the primary image becomes corrupted, you can use the bootloader to boot with the backup image.

With the backup image stored before rebooting, be sure to choose **Option 4: Change Active Boot Image** from the boot menu to set the backup image as the active boot image. Otherwise, when the controller resets, it again boots off the corrupted primary image.

After the controller boots, the active boot image can be changed to the backup image using the **config boot backup** command.

Home Page Retains Web Auth Login with IE 5.x

Due to a caching issue in the Internet Explorer 5.x browser, the home page retains the web authentication login. To correct this issue, clear the history or upgrade your workstation to Internet Explorer 6.x.

RLDP Enable/Disable

The RLDP protocol detects rogues on your wired network. When RLDP is enabled, the controller reports a threat alarm for each rogue detected on the wired network. When RLDP is disabled, rogues detected on the wired network are shown in the Alert state.

Disabling RLDP stops the controller from detecting rogues on the wired network. Rogues can be manually contained by changing the status of the detected rogues. When rogues are being contained, you must manually disable containment for each rogue individually.

Ad-Hoc Rogue Containment

Client card implementations may mitigate the effectiveness of ad hoc containment.

Apple iBook

Some Apple operating systems require shared key authentication for WEP. Other releases of the operating system do not work with shared key WEP unless the client saves the key in its key ring. How you should configure your controller is based on the client mix you expect to use. Cisco recommends testing these configurations before deployment.

Features Not Supported on 2000 Series Controllers

These hardware features are not supported on 2000 series controllers:

- Power over Ethernet
- Service port (separate out-of-band management 10/100-Mbps Ethernet interface)

These software features are not supported on 2000 series controllers:

- VPN termination (such as IPSec and L2TP)
- Termination of guest controller tunnels (Origination of guest controller tunnels is supported)
- External web authentication web server list
- Layer 2 LWAPP
- Spanning tree
- Port mirroring
- Cranite
- Fortress
- AppleTalk
- QoS per-user bandwidth contracts
- IPv6 pass-through

Some Clients See Only 64 Access Point MAC Addresses (BSSIDs) at a Time

In a crowded RF environment, clients may not be able to detect the desired SSID because of internal table limitations. Sometimes disabling and then enabling the client interface forces a rescan. Your RF environment needs to be controlled. Cisco UWN rogue access point detection and containment can help you to enforce RF policies in your buildings and campuses.

Pinging from Any Network Device to a Dynamic Interface IP Address Is Not Supported

Clients on the WLAN associated with the interface pass traffic normally.

2006 Image Not Supported for 3504 Controllers

The 2006 controller image is supported for use with only 2000 series controllers. Do not install the 2006 image on a 3504 controller. Otherwise, errors may occur. Install only the 3504 image on a 3504 controller.

Running a 3504 Image on a 2000 Series Controller

It is possible to run a 3504 controller image on a 2000 series controller, but Cisco Aironet 1130, 1200, and 1240 series access points will not be able to connect to the controller.

Cisco Lightweight Access Points Fail to Join Cisco Controllers

When a Cisco lightweight access point is connected to a terminal server port and reboots because of a join failure or timeout, this sequence repeats until the access point returns to the boot prompt and remains there. This condition occurs when there is no telnet session to the access point's console port and when the controller is not responding to the access point's join response.

Workaround: Disconnect the access point's console port from the terminal server. Reprogram the controller to have it respond to the access point's join request. Power cycle the access point to force a restart.

Upgrading External Web Authentication

When upgrading a controller from operating system release 2.0 or 2.2.127.4 to release 3.2.116.21, update the external web authentication configuration as follows:

1. Instead of using a preauthentication ACL, the network manager must configure the external web server IP address using this command:

   config custom-web ext-webserver add *IP-address*

   ✎

   Note   *IP-address* is the address of any web server that performs external web authentication.

2. The network manager must use the new login_template shown here:

```
<html>
<head>
<meta http-equiv="Pragma" content="no-cache"> <meta HTTP-EQUIV="Content-Type"
CONTENT="text/html; charset=iso-8859-1"> <title>Web Authentication</title> <script>

function submitAction(){
    var link = document.location.href;
    var searchString = "redirect=";
    var equalIndex = link.indexOf(searchString);
    var redirectUrl = "";
    var urlStr = "";
    if(equalIndex > 0) {
            equalIndex += searchString.length;
            urlStr = link.substring(equalIndex);
            if(urlStr.length > 0){
```

```
  redirectUrl += urlStr;
        if(redirectUrl.length > 255)
        redirectUrl = redirectUrl.substring(0,255);
      document.forms[0].redirect_url.value = redirectUrl;
  }
    }

    document.forms[0].buttonClicked.value = 4;
    document.forms[0].submit();
}

function loadAction(){
    var url = window.location.href;
    var args = new Object();
    var query = location.search.substring(1);
    var pairs = query.split("&");
    for(var i=0;i<pairs.length;i++){
        var pos = pairs[i].indexOf('=');
        if(pos == -1) continue;
        var argname = pairs[i].substring(0,pos);
        var value = pairs[i].substring(pos+1);
        args[argname] = unescape(value);
    }
    //alert( "AP MAC Address is " + args.ap_mac);
    //alert( "The Switch URL is " + args.switch_url);
    document.forms[0].action = args.switch_url;

    // This is the status code returned from webauth login action
    // Any value of status code from 1 to 5 is error condition and user
    // should be shown error as below or modify the message as it suits
    // the customer
    if(args.statusCode == 1){
        alert("You are already logged in. No further action is required on your
part.");
    }
    else if(args.statusCode == 2){
        alert("You are not configured to authenticate against web portal. No further
action is required on your part.");
    }
    else if(args.statusCode == 3){
        alert("The username specified cannot be used at this time. Perhaps the
username is already logged into the system?");
    }
    else if(args.statusCode == 4){
        alert("Wrong username and password. Please try again.");
    }
    else if(args.statusCode == 5){
        alert("The User Name and Password combination you have entered is invalid.
Please try again.");
    }

}

</script>
</head>
<body topmargin="50" marginheight="50" onload="loadAction();"> <form method="post">
<input TYPE="hidden" NAME="buttonClicked" SIZE="16" MAXLENGTH="15" value="0"> <input
TYPE="hidden" NAME="redirect_url" SIZE="255" MAXLENGTH="255" VALUE=""> <input
TYPE="hidden" NAME="err_flag" SIZE="16" MAXLENGTH="15" value="0">

<div align="center">
<table border="0" cellspacing="0" cellpadding="0"> <tr> <td> </td></tr>
```

```
<tr align="center"> <td colspan="2"><font size="10" color="#336699">Web
Authentication</font></td></tr>

<tr align="center">

<td colspan="2"> User Name    <input type="TEXT" name="username"
SIZE="25" MAXLENGTH="63" VALUE=""> </td> </tr> <tr align="center" > <td colspan="2">
Password      <input type="Password" name="password"
SIZE="25" MAXLENGTH="24"> </td> </tr>

<tr align="center">
<td colspan="2"><input type="button" name="Submit" value="Submit" class="button"
onclick="submitAction();"> </td> </tr> </table> </div>

</form>
</body>
</html>
```

Caveats

This section lists resolved and open caveats in operating system release 3.2.116.21 for Cisco controllers and lightweight access points.

Resolved Caveats

These caveats are resolved in operating system release 3.2.116.21.

- CSCeh68636—If a power injector is inserted between an AP1131 or AP1242 and a Cisco Catalyst switch and an AC power adapter is connected directly to the access point, the access point does not use the power from the switch. After the access point boots up, it waits for CDP packets from the switch. If the output power of the switch does not support the access point, the access point changes both 802.11 radio interfaces to a reset state.

- CSCsb13548—Cisco lightweight access points frequently reset.

- CSCsb63749—A client on an anchor controller cannot ping another client that has roamed to a foreign 2006 controller.

- CSCsb76419—The client state appears on two switches in a Layer 2 roaming environment.

- CSCsb78835—The controllers are not sending all rogue trap information to Cisco WCS.

- CSCsb88424—Cisco Aironet 1030 Remote Edge Lightweight Access Points in REAP mode reboot continuously.

- CSCsb97559—The candidate list returned by the controller in association/reassociation responses may have an access point that the client cannot reach as the top-most entry.

- CSCsc06090—For some systems with a large number of access points and controllers, the rogue access point scheduled task can take up to 35 or 45 minutes to complete.

- CSCsc33769—The controller's radio resource management (RRM) algorithms set the transmit power to 6 on Cisco Aironet 1000 Series Lightweight Access Points.

- CSCsc37217—Over the temperature extremes of the product specification (and primarily at the hot temperature extreme of 55 degrees Celsius), the Cisco Aironet 1500 Series Lightweight Outdoor Access Point may not meet the IEEE 802.11a/b/g transmitter linearity parameter of error vector magnitude (EVM) of the 54Mb and 48Mb product specification.

- CSCsc42773—LWAPP-enabled 1130 and 1200 series access points may shut down their radio interfaces because of insufficient power from power over Ethernet (PoE).

- CSCsc42923—A 32-character SSID does not allow access points to join the controller.

- CSCsc43587—The controller crashes in the apfReceiveTask software.

- CSCsc47951—The mmListen task may miss the software watchdog, causing the controller to reboot.

- CSCsc49148—The 2006 controller may crash because of a stack corruption of the apfRogueTask. When an SSID of 32 characters is advertised by the rogue access point, such a crash is likely.

- CSCsc51291—An EAP ID request is always sent to the client when the PMK/WEP+ cache expires, even if the client is not associated to a WLAN that is configured for WEP+ or WPA2 security.

- CSCsc59377—Access points fail to join a controller with sustained high CPU utilization (~97%). During a user-initiated reboot, the access points fail to join the controller until the access point count is reduced from 32 to 25. After the initial 25 join, the remaining access points can be added and will join the controller.

- CSCsc63217—Some AP1000 units are shipping from the factory with their LEDs disabled by default. Therefore, it appears as though the access points are not operating correctly.

- CSCsc70407—The controller may stop accepting new IPSec client authentications.

- CSCsc72027—Due to insufficient power over Ethernet (PoE), some access point radios may remain in reset even if a power injector is being used. When the access point is connected to a Cisco switch running older code that does not support intelligent power management (IPM), you must configure the access point for the inline power source. Two new LWAPP power injector commands are available for this purpose. See the "New LWAPP Power Injector Commands" section on page 4 for information on these commands.

- CSCsc72479—If an access point has a space in its name, the access point's configuration cannot be cleared and a static IP address cannot be assigned. This problem occurs only in the controller CLI, not in the GUI.

- CSCsc72899—A deadlock between tNetTask and spam task (when packets are being processed by one task while discovery is occurring) causes a REAP access point to crash.

- CSCsc75655—The IKE test suite causes the controller to reboot. For more details, see the Cisco Security Advisory for this issue:

  http://www.cisco.com/en/US/products/products_security_advisory09186a0080572f55.shtml

- CSCsc76782—When the controller terminates a client session, the access points need to see a deauthentication message.

- CSCsc82863—Hewlett-Packard (HP) laptops with Intel 2200 b/g or 2915 a/b/g clients may bluescreen and reboot after associating to a Cisco 1130 or 1230 access point that is running LWAPP with PEAP encryption. This problem occurs most often during logon, but it may also occur during logoff.

- CSCsc85671—When you modify any of the settings on the MAC Filtering page in the controller GUI and click Apply, the change is not reflected on other GUI pages.

- CSCsc86705—The controller becomes unstable and may crash when the system is configured for Cranite Layer 2 security and the system is being used by more than two users.

- CSCsc87698—If you create a TKIP WLAN with a key cache size that is not in the 0 to 31 range, the access point crashes.

- CSCsc91461—The controller cannot bring up the 802.11g radio interface if the access point's 802.11g radio is disabled.

- CSCsc93617—The lack of a MAC address during a secure shell (SSH) delete leads to an eventual crash of the controller.

- CSCsc94879—Cisco 1200 series access points continue to stream RTP packets to the Cisco 7920 Wireless IP Phone after the 7920 sends a deauthentication packet to the access point.

- CSCsc96640—Web authentication does not operate properly when clustered Checkpoint firewalls are set as the client's default gateway.

- CSCsc97687—Client devices experience slow roam times due to WPA-PSK failures.

- CSCsc98586—The controller's backup port is not operating correctly when configured for the management and dynamic interfaces. If the primary ports fails, the active port is not changed to the secondary port, and connectivity to the controller is lost.

- CSCsd00921—The controller does not accept broadcast discovery requests on the AP-manager interface if link aggregation (LAG) is enabled.

- CSCsd02525—If a Cisco 1200 series access point is reset while the 802.11a network is disabled, the access point sends a change state event to the controller when it comes back up indicating that its 802.11a radio is operational, but the power-over-Ethernet (PoE) power detection takes some time to complete.

- CSCsd03939—Enabling or disabling the 802.11g network causes the access points joined to the controller to reboot. This is normal operating behavior. However, no messages appear to explain why the access points suddenly reboot when WCS templates are applied and change the 802.11g state.

- CSCsd04657—The primary controller sends an LWAPP discovery response even when the maximum number of access points are joined, which causes any new access points to attempt to join the primary controller without trying the secondary or tertiary controller.

- CSCsd09768—The AP1000 loses its Ethernet buffers due to an invalid ARP packet generated by the neighbor switch. As a result, it is unable to receive any packets, including the DHCP offer, and becomes stuck in the DHCP Discover state.

- CSCsd09898—If a client has crypto handles that are set to 0, which is an invalid value, the traffic stops flowing for that particular client. Other clients with valid crypto handles are unaffected.

- CSCsd11774—LWAPP-enabled 1130 and 1230 access points may fragment large packets into two files after the LWAPP header is added and then do not send the second fragment to the controller.

- CSCsd14113—When the controller receives a delayed Access Request (with an ID out of order) from an MS-PEAP client, it adjusts the order of the packet and sends the request to the RADIUS server. However, the client fails to authenticate.

- CSCsd21147—When a client device roams from one controller to another, the ARP filters for the client are not deleted properly.

- CSCsd21248—A memory leak in buffer pool 0 in the NPU driver causes CPU/NPU communications to fail.

- CSCsd22087—Intel 2200 b/g clients cannot pass traffic with an AP1000 in 802.11g mode. This condition remains for 5 to 60 seconds and then recovers, but it can occur quite frequently.

- CSCsd32642, CSCsd23190, and CSCsc95614—The max retry count from the controller is being used as the total number of retries allowed per packet rather than the number of retries per rate. Therefore, the controller cannot rate shift down if a client needs lower rates.

- CSCsd44941—The 2.4-GHz radio in some AP1130 and AP1240 units produced after 1/23/2006 can enter a state in which all clients disassociate and the access points can no longer communicate with the clients.

Open Caveats

These caveats are open in operating system release 3.2.116.21.

- CSCar14535—When configuring a mobility group anchor that is not part of the mobility member list, the controller displays an "Invalid Parameter Provided" error message.

  Workaround: Make sure that the anchor controller is a mobility group member.

- CSCek16101—The Controller Network Module does not have the correct time when it is first booted up because it does not have a real-time clock. Therefore, it contacts the NTP server during the initial bootup to obtain the correct time. If the controller cannot reach the NTP server, it eventually gives up and boots without the correct time. When this happens, access points cannot register with the controller. The controller must wait for at least one hour before trying to poll the NTP server again for the correct time.

  Workaround: Manually configure the correct time on the controller (**config time manual** *date time*) or reconfigure the NTP server entry on the controller (**config time ntp server** *inex IP-address*). The second option triggers the controller to connect to the NTP server and synchronize its time.

- CSCsa89818—PDAs are unable to associate with Cisco Aironet 1030 Remote Edge Lightweight Access Points in REAP mode although local mode works correctly.

  Workaround: None at this time.

- CSCsa95763—The controller GUI cannot display more than 80 local net users on the Security > AAA > Local Net Users page.

  Workaround: Use the controller CLI to view all the Local Net User entries.

- CSCsb01980—When the operator enters incorrect data for the management interface in the controller web configuration wizard, error messages are shown only at the end of the wizard, and the user must return to the Management Interface page for correction. The data entered on the Management Interface page, such as the port number, are not validated immediately but at the end of the wizard. As a result, any error messages are shown only at the end.

  Workaround: This problem can cause some inconvenience, and the user may prefer to use the CLI configuration wizard instead to avoid it.

- CSCsb01983—The controller web configuration wizard is not reachable after making repeated invalid entries for the management interface port. If an operator connects to the wizard on address 192.168.1.1 and enters an invalid port number on the Management Interface page, the operator is redirected at the end of the wizard to the Management Interface page to correct the port. If the operator enters an incorrect port and submits, the wizard becomes inaccessible.

  Workaround: Reboot the controller through the CLI to access the wizard again.

- CSCsb20269—On the WiSM, when the service VLAN is configured as one of the VLANs on a data port, it does not operate correctly.

  Workaround: Do not configure the service VLAN as one of the VLANs on a data port.

- CSCsb34149—Disabling or deleting a wireless LAN on which a large number of clients exists may not result in all clients being deleted. This generally occurs when several thousand clients are using the wireless LAN.

  Workaround: Make sure that wireless LANs with a large number of clients associated are not deleted or disabled.

- CSCsb38486—The Cisco Aironet 1500 Series Lightweight Outdoor Access Point Bridge CLI does not accept 10-character bridge group names.

  Workaround: Use 9-character bridge group names.

- CSCsb39522—When a user changes the setting from a static IP address to DHCP and the DHCP IP address is not available, the supervisor loses keepalive, and the WiSM sends a WCP going down trap. Similarly, when a user changes a static IP address and enters an incorrect subnet on the service port, the supervisor detects a loss of WCP keepalive, and the WiSM sends a WCP going down trap.

  Workaround: None at this time.

  > **Note** WCP is the protocol running between the Cisco Catalyst 6500 Series Switch Supervisor and the WiSM. The supervisor uses WCP to monitor the health of the WiSM. If you enter the **show wism status** command or see a WiSM down trap on WCS, make sure that the WiSM service port and the supervisor are configured correctly. WCP can fail because of an incorrect configuration.

- CSCsb48197—Multiple authentication requests to the WCS server.

  Workaround: None in this release.

- CSCsb52557—Cisco access points do not connect to the 4400 series controller if the time is not set first.

  Workaround: Set the time on the controller before allowing the access points to connect to the controller.

- CSCsb53746—A 350 or CB20A client running ACU 6.5 or 6.4 and configured for LEAP authentication with WPA1 encryption can authenticate to a lightweight access point but does not receive an IP address. This problem does not affect clients running ACU 6.3, which does not use WMM data frames. To check for this problem, enter the following command on the controller:

  debug dot1x events enable

  In the body of the trace that follows authentication by an affected client, the following messages appear:

  > Fri Jun 3 07:29:59 2005: Received EAPOL-Key from mobile xx:xx:xx:xx:xx:xx

  > Fri Jun 3 07:29:59 2005: Received EAPOL-key message with invalid version number from mobile xx:xx:xx:xx:xx:xx

  Workaround: Configure WMM policy to be allowed for the wireless LAN on the controller. To do this on the GUI, browse to the WLANs > Edit page for the appropriate WPA1 wireless LAN, and choose **Allowed** or **Required** in the WMM Policy drop-down box. The Allowed option means that both WMM and non-WMM clients can authenticate and receive an IP address (for example, both Aironet ACU 6.5/6.4 and 6.3 clients could authenticate and receive an IP address). The Required option means that only WMM clients can authenticate (that is, only ACU 6.5/6.4 clients).

- CSCsb55937—VLAN-tagged large ICMP packets that need to be fragmented are not sent by Cisco Aironet 1000 series access points in direct-connection mode. Ping replies never come back when the access point sends requests to a gateway from a wireless client using large 1500-byte packets and with RADIUS override configured with any 1p tag. This condition exists for 4400 series controllers using direct-connect mode, with RADIUS override enabled, the override parameter set to 1p with any VLAN number, and Cisco Aironet 1000 series access points.

  Workaround: None at this time.

- CSCsb59898—Cisco Aironet 1030 Remote Edge Lightweight Access Points in REAP mode do not support roaming when configured with a WLAN that is set up for WPA security.

  Workaround: None for this release.

- CSCsb71060—Internal LAG errors occur when the management interface is changed from tagged to untagged.

  Workaround: Leave the WiSM management interface as tagged or untagged.

- CSCsb76389—Cannot failover to second instance IP address or port on a RADIUS server.

  Workaround: None for this release.

- CSCsb77595—When logging out from Telnet/SSH sessions, the session always prompts the user to save changes, even when no changes have been made.

  Workaround: Ignore the prompt and exit as usual.

- CSCsb85113—When users download the code image to WiSM using the CLI, associated access points are sometimes disconnected.

  Workaround: Download new code images to the WiSM at times when there are no clients to be affected.

- CSCsb85582—Cisco 4100 series controllers crash at PES_rqst_exec_again.

  Workaround: None for this release.

- CSCsb88588—Incorrect power levels are reported for access points when the controller is set to country code SG.

  Workaround: None for this release.

- CSCsb90622—AP impersonation alarms sometimes flood WCS.

  Workaround: None for this release.

- CSCsc01221—When downstream test data is sent from the wired endpoint to four wireless clients at different priority levels (voice, video, background, and best effort), the Cisco Aironet 1000 series access points crash.

  Workaround: None for this release.

- CSCsc02741—In the bootloader mode, users are unable to exit or return to the main prompt. If users make mistakes while entering values, they cannot quit the step and are unable to go back and change existing values.

  Workaround: Reset the system through IOS or power the device off and on if necessary.

- CSCsc02860—When users download the code image to a WiSM for the first time, the WiSM fails to download the new image to flash memory.

  Workaround: Download new code images to the WiSM a second time.

- CSCsc03072—Cisco lightweight access points do not always produce complete logs.

  Workaround: None for this release.

- CSCsc03644—Cisco lightweight access points do not retain location parameters after a reboot.

  Workaround: None for this release.

- CSCsc05495—Controllers running 3.0.107 code intermittently send a state attribute 24 in an access-request packet.

  Workaround: Apply the Microsoft KB 883659 patch to IAS. The Microsoft patch may or may not work. There is no workaround on the controller.

- CSCsc11660—The current country screen is not 100% accurate for all deployment scenarios, which may cause confusion in some instances.

  Workaround: None for this release.

- CSCsc14045—VPN passthrough should not be able to combine with web policy.

  Workaround: Do not assign VPN passthrough along with web policy.

- CSCsc15699—In Cisco Aironet 1000 series access points, the WMM IE (11) is correct, but the QBSS client cac limit (11) is still in its old place.

  Workaround: None for this release.

- CSCsc17827—For Cisco Aironet 1500 Series Lightweight Outdoor Access Points and Cisco Aironet 1030 Remote Edge Lightweight Access Points, channel 165 for the 802.11a radio is only available for the -A SKU when the country code is set to USX. Channel 165 is not available for the -N SKU for any of the countries that use this SKU.

  Workaround: In order to set the 802.11a radio to channel 165 when using the -A SKU, set the country code of the controller to USX. For the -N SKU, please select one of the available channels.

- CSCsc20416—ACU site survey disassociates other clients in the LWAPP environment.

  Workaround: Under investigation.

- CSCsc21196—Asymmetrical data rate with 802.11a radio on 4012 and 4024 controllers.

  Workaround: None for this release.

- CSCsc22084—Error messages and traps are not triggered when a PoE controller with CDP causes Cisco Aironet 1200 series access points to disable their radios.

  Workaround: Disabling CDP resolves this issue.

- CSCsc22663—Deleting a mobility member mapped to a controller as an anchor removes the anchor's entry as well, but the Auto Anchor knob remains enabled even though only the mobility anchor mapping is deleted.

  Workaround: Before deleting a mobility member, first delete the controller to which it is mapped from the WLAN.

- CSCsc26796—The WiSM web interface does not show the correct access point SNMP operator status (Registered versus Down).

  Workaround: Use WCS to view the correct values.

- CSCsc28571—Task 181 (do_linktest) is taking 4265111% of the CPU.

  Workaround: None for this release.

- CSCsc34060—IPSec clients enter the run state but do not communicate.

  Workaround: Under investigation.

- CSCsc35784—The transmit power control adjustment levels 3, 4, and 5 are not supported on Cisco Aironet 1500 Series Lightweight Outdoor Access Points in the 5745-to-5825-MHz band. The transmit power control adjustment levels 4 and 5 are not supported on Cisco Aironet 1500 series access points that operate in the 5500-to-5700-MHz band and at 2.4 GHz.

  These levels correspond to -6, -9, and (in the case of 5500 to 5700 MHz) -12 dB from the maximum power, respectively. Power levels 1, 2, and (in the case of 5500 to 5700 MHz) 3 are supported, which correspond to maximum power for the particular data rate and channel, and -3 dB relative to this maximum, at which these adjustment levels provide little or no further reduction in transmit power output.

  Workaround: Set the transmit power level to either 1 or 2 for 5745 to 5825 MHz. Set the transmit power level to either 1, 2, or 3 for all other bands.

- CSCsc38093—Wireless clients experience poor performance when associated to a 4400 series controller.

   Workaround: Under investigation.

- CSCsc40648—Rooftop access points are displayed in the web interface as poletop access points for more than four minutes, which prevents them from being configured.

   Workaround: Configure the access point as a rooftop access point using the controller CLI.

- CSCsc41313—The Cisco Aironet 1500 Series Lightweight Outdoor Access Points are configured by default to allow old bridges. When this configuration is enabled, the shared secret key set on the controller is not passed to the access points, so a few access points might be running on the old key. If these access points reset or new access points are waiting to join the running network, they may take a very long time to connect to the network or might not join at all. The default value has been changed to not allow old bridges to authenticate.

   Workaround: Configure the controller using this command: **config network allow-old-bridge-aps disable**.

- CSCsc61004—Poletop access points (PAPs) may not be able to move from one rooftop access point (RAP) to another if the first RAP goes down. This problem usually occurs if the RAPs are configured statically at "rooftop" and the PAPs are configured at "poletop."

   Workaround: Configure Auto mode on all RAPs and PAPs.

- CSCsd34555—The PC350 client adapter is unable to pass traffic when the access point is not in protection mode.

   Workaround: None at this time.

- CSCsd35492—The client exclusion feature does not operate correctly when aek keywrap is configured.

   Workaround: Use the non-keywrap method.

- CSCsd36689—Access points in monitor mode do not detect probing clients. These access points do not track the clients' RSSI values and do not contribute location information to the Location Appliance.

   Workaround: Configure the access points for local mode.

- CSCsd48466—Unless WMM policy is set to Allowed or Required on the WLAN, the 1200 series access point does not set the DSCP value in the outer LWAPP header for packets that it forwards to the controller. As a result, the controller cannot set the 1p tag on upstream packets.

   Workaround: Set the WMM Policy parameter to either **Allowed** or **Required**.

Troubleshooting

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

http://www.cisco.com/en/US/support/index.html

Click **Product Support** > **Wireless**. Then choose your product and **Troubleshooting** to find information on the problem you are experiencing.

Related Documentation

For additional information on the Cisco controllers and lightweight access points, refer to these documents:

- The Quick Start Guide for your particular controller or access point
- *Cisco Wireless LAN Controller Configuration Guide*
- *Cisco Wireless LAN Controller Command Reference*
- *Cisco Wireless LAN Controller Online Help*
- *Cisco Wireless Control System Configuration Guide*
- *Cisco Wireless Control System Online Help*

You can access these documents from this link:

http://www.cisco.com/en/US/products/hw/wireless/tsd_products_support_category_home.html

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

The Product Documentation DVD is a comprehensive library of technical product documentation on a portable medium. The DVD enables you to access multiple versions of installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the same HTML 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= or DOC-DOCDVD=SUB) from Cisco Marketplace at this URL:

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

Ordering Documentation

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 submit comments about Cisco documentation 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 will find information about how to:

- 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, security notices, and security responses for Cisco products is available at this URL:

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

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at 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 have identified a vulnerability in a Cisco product, contact PSIRT:

- For Emergencies only — 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.

- For 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 (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.*x* through 9.*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.

If you do not have or use PGP, contact PSIRT at the aforementioned e-mail addresses or phone numbers before sending any sensitive material to find other means of encrypting the data.

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)—An existing 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 operations 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 the network is impaired, while 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.

- The *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco offerings. To order and find out more about the Cisco Product Quick Reference Guide, go to this URL:

    http://www.cisco.com/go/guide

- 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 "Related Documentation" section.