Release Notes for Cisco Wireless LAN Controllers and Lightweight Access Points for Release 6.0.202.0

April 2011

These release notes describe open and resolved caveats for maintenance **software** release 6.0.202.0 for Cisco 2100, 4400, and 5500 Series Wireless LAN Controllers; Cisco Wireless Services Modules (WiSMs); Cisco Wireless LAN Controller Network Modules; Catalyst 3750G Integrated Wireless LAN Controller Switches; Cisco 3201 Wireless Mobile Interface Cards (WMICs); Cisco Aironet 1100, 1130, 1140, 1200, 1230AG, 1240, 1250, 1300, and AP801 Series Lightweight Access Points; Cisco Aironet 1130AG, 1240AG, 1522, and 1524 Mesh Access Points, which comprise part of the Cisco Unified Wireless Network (UWN) Solution.

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

To know more about the open and resolved caveats, see Caveats, page 38.

Contents

These release notes contain the following sections.

Americas 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:

- Software release 6.0.202.0 for all Cisco controllers and lightweight access points
- Cisco autonomous to lightweight mode upgrade tool release 3.0
- Cisco Wireless Control System (WCS) software release 6.0.202.0
- Cisco WCS Navigator 1.5.202.0
- Location appliance software release 6.0.202.0
- Cisco 2700 Series Location Appliances
- Mobility services engine software release 6.0.202.0 and Context Aware Software

Note Client and tag licenses are required in order to retrieve contextual (such as location) information within the Context Aware Software. See the *Release Notes for Cisco 3350 Mobility Services Engine for Software Release 6.0* for more information.

- Cisco 3350 Mobility Services Engines
- Cisco 2100 Series Wireless LAN Controllers
- Cisco 4400 Series Wireless LAN Controllers
- Cisco 5500 Series Wireless LAN Controllers
- Cisco Wireless Services Module (WiSM) for Cisco Catalyst 6500 Series Switches and Cisco 7600 Series Routers
- Cisco Wireless LAN Controller Network Module for Cisco Integrated Services Routers

Note The 6.0.202.0 release does not support the NM-AIR-WLC6 platform. The NME-AIR-WLC platform is supported.

- Catalyst 3750G Wireless LAN Controller Switches
- Cisco 3201 Wireless Mobile Interface Card (WMIC)
- Cisco Aironet 1130AG, 1240AG, 1522, and 1524 Mesh Access Points

Note This release does not support Cisco Aironet 1260, 1505, 1510, and 3500 access points.

- Cisco Aironet 1100, 1130, 1140, 1200, 1230AG, 1240, 1250, 1300, and AP801 Series Lightweight Access Points
- Cisco 3310 mobility Service Engine

Note Controller software release 5.0.148.0 or later releases is not compatible with Cisco Aironet 1000 series access points.

Note The AP801 is an integrated access point on the Cisco 800 Series Integrated Services Routers (ISRs).

Note The integrated controller in Cisco 2800 series routers is not supported in the 6.0.200.1 release. Do not install these releases on the integrated controller in 2800 series routers. The is upgrade from 6.0 to 7.0 is not supported.

Note Only Cisco Aironet 1200 Series Access Points that contain 802.11g (AIR-MP21G) or second-generation 802.11a radios (AIR-RM21A or AIR-RM22A) are supported for use with controller software releases. The AIR-RM20A radio, which was included in early 1200 series access point models, is not supported. To see the type of radio module installed in your access point, enter this command on the access point: **show controller dot11radio** *n*, where *n* is the number of the radio (0 or 1).

Note For 5500 Series controller, the Dot1p value in the capwap packet between controller and the AP is always 0 irrespective of the profile configured on the WLAN and the DSCP value.

Controller Requirements

The controller GUI requires the following operating system and web browser:

- Windows XP SP1 (or later) or Windows 2000 SP4 (or later)
- Internet Explorer 6.0 SP1 (or later) or Mozilla Firefox 2.0.0.11 (or later)

Note Internet Explorer 6.0 SP1 (or later) and Mozilla Firefox 2.0.0.11 (or later) are the only browsers supported for using the controller GUI and web authentication.

MIB Files

Cisco controllers support standard SNMP Management Information Base (MIB) files. MIBs can be downloaded from the Software Center on Cisco.com. Only one MIB is posted per major release (6.0, 5.2, 5.1, and so on). If an updated MIB becomes available, the previous version is removed from the Software Center and replaced by the new version.

New Features

The following new features are available in controller software release 6.0.202.0.

CLI to disable AMSDU per Priority

With WPA2-AES enabled, sometimes a frame following an aggregated A-MSDU frame, has corrupted PN sequence number. Source MAC address seems to be directly encoded in the place of PN sequence number. This leads to decrypt errors on the client side and dropping of phone calls. This issue was seen with third party 11n phones and is common to all 11n clients. Disabling AMSDU for Voice priority solves the problem.

To specify the aggregation method used for 802.11n packets, use the **config 802.11{a | b} 11nsupport a-msdu tx priority {0-7 | all} {enable | disable}** command.

The **config 802.11a 11nSupport rifs rx enable** command is used to enable the RIFS. By default, the RIFS is enabled. This means that the RIFS Rx is enabled but the Polycom WAR is disabled. Hence Polycom 11n phones have some problem (receiver gets stuck for 100 ms).

If you disable RIFS using the **config 802.11a 11nSupport rifs rx disable** command, RIFS Rx is disabled (non-compliance with standard) but the WAR is applied which resolves the receiver stuck issue. This is recommended only when the Polycom 11n phones are displayed.

To display the A-MSDU and RIFS priority information, use the **show 802.11 {a | b}** command.

```
> show 802.11a
802.11a Network..................................... Enabled
11nSupport.......................................... Enabled
      802.11a Low Band.............................. Enabled
      802.11a Mid Band.............................. Enabled
      802.11a High Band............................. Enabled
802.11a Operational Rates
    802.11a 6M Rate................................. Mandatory
    802.11a 9M Rate................................. Supported
    802.11a 12M Rate................................ Mandatory
    802.11a 18M Rate................................ Supported
    802.11a 24M Rate................................ Mandatory
    802.11a 36M Rate................................ Supported
    802.11a 48M Rate................................ Supported
    802.11a 54M Rate................................ Supported
802.11n MCS Settings:
    MCS 0........................................... Supported
    MCS 1........................................... Supported
    MCS 2........................................... Supported
    MCS 3........................................... Supported
    MCS 4........................................... Supported
    MCS 5........................................... Supported
    MCS 6........................................... Supported
    MCS 7........................................... Supported
    MCS 8........................................... Supported
    MCS 9........................................... Supported
    MCS 10.......................................... Supported
    MCS 11.......................................... Supported
    MCS 12.......................................... Supported
    MCS 13.......................................... Supported
    MCS 14.......................................... Supported
    MCS 15.......................................... Supported
802.11n Status:
    A-MPDU Tx:
        Priority 0.................................. Enabled
        Priority 1.................................. Disabled
```

```
        Priority 2.............................. Disabled
        Priority 3.............................. Disabled
        Priority 4.............................. Enabled
        Priority 5.............................. Enabled
        Priority 6.............................. Disabled
        Priority 7.............................. Disabled
    A-MSDU Tx:
        Priority 0.............................. Enabled
        Priority 1.............................. Enabled
        Priority 2.............................. Enabled
        Priority 3.............................. Enabled
        Priority 4.............................. Enabled
        Priority 5.............................. Enabled
        Priority 6.............................. Disabled
        Priority 7.............................. Disabled
    Rifs Rx ..................................... Enabled
    Guard Interval ............................. Any
Beacon Interval................................. 100
```

Regulatory Domain Updates

International regulatory requirements are constantly changing. To stay up-to-date on these changes, the following regulatory domain updates are included in the Cisco Unified Wireless Network Software release 6.0.200.201.

Addition of the -R regulatory domain to support the new 802.11a(except52) and 802.11b/g channel and power setting for Russia. The following combinations of access points are permitted:

- 1130, 1240, 1250, 1140, 1520
- AIR-AP1131AG-R-K9, AIR-LAP1131AG-R-K9, AIR-AP1242AG-R-K9, AIR-LAP1242AG-R-K9, AIR-AP1252AG-R-K9, AIR-LAP1252AG-R-K9, AIR-AP1142N-R-K9, AIR-LAP1142N-R-K9, AIR-AP1262N-R-K9, AIR-LAP1262N-R-K9,AIR-CAP3502I-R-K9, AIR-CAP3502E-R-K9, AIR-LAP1522AG-R-K9, AIR-LAP1522HZ-R-K9, AIR-LAP1524SB-R-K9

Software Release Information

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

Note The Cisco WiSM requires software release SWISMK9-32 or later releases. The Supervisor 720 12.2(18)SXF2 supports the Cisco WiSM software release 3.2.78.4 or later releases, and the Supervisor 720 12.2(18)SXF5 (Cisco IOS Software Modularity) supports the Cisco WiSM software release 4.0.155.5 (with Cisco IOS Software Modularity).

Note To use the Cisco WiSM in the Cisco 7609 and 7613 Series Routers, the routers must be running Cisco IOS Release 12.2(18)SXF5 or later releases.

Note The **Cisco Wireless LAN Controller Network Module is supported on** Cisco 28/37/38xx Series Integrated Services Routers running Cisco IOS Release 12.4(11)T2, 12.4(11)T3, and 12.5.

Note To use the controller in the Catalyst 3750G Wireless LAN Controller Switch, the switch must be running Cisco IOS Release 12.2(25)FZ, 12.2(35)SE or later releases, 12.2(37)SE or later releases, 12.2(44)SE or later releases, or 12.2(46)SE or later releases. The following Cisco IOS Releases and any variants are not supported: 12.2(25)SEC, 12.2(25)SED, 12.2(25)SEE, 12.2(25)SEF, and 12.2(25)SEG. All Catalyst 3750 software feature sets (IP Base, IP Service, and Advanced IP Services) are supported for use with the controller.

Note You can use the 2112 and 2125 controllers only with software release 5.1.151.0 or later releases.

Finding the Software Release

To find the software release running on your controller, click **Monitor** and look at the Software Version field under Controller Summary on the controller GUI or enter **show sysinfo** on the controller CLI.

Special Rules for Upgrading to Controller Software Release 6.0.202.0

Caution Before upgrading your controller to software release 6.0.202.0, you must comply with the following rules.

Note Session from cat6000 to WiSM controllers can be blocked only on service port interface by adding a ACL on cat6000.

Note DCA channel list changes when controller is upgraded to 6.0.202.0 / 7.0.98.0 from 4.2 release. For example, if channels {36, 40, 44, 48} are configured as 802.11a DCA channel list while running controller with 4.2 image, when the controller is upgraded to 6.0.202.0 / 7.0.98.0 release, then the DCA channel list may not retain as {36, 40, 44, 48}. After the upgrade, if the channel list proves to be incorrect, then you can download a CLI config file that has the desired channel configurations. For example, in the CLI config file, remove the invalid channels or the correct ones with:

```
config advanced [802.11b|802.11a]channel add <desired channel(s)
```

For example, “config advanced 802.11b channel add 6” will add the channel number 6 to the DCA channel list for the 2.4 GHz band.

Alternatively, you can also rely on the controller web GUI or WCS if it is available to add and remove channels as desired.

- Before you download a software image or an ER.aes file to a 2100 series controller or a controller network module, use the **show memory statistics CLI** command to see the current amount of free memory. If the controller has less than 90 MB of free memory, you need to reboot it before downloading the file.
- Before you use an AP801 series lightweight access point with controller software release 6.0.202.0, you must upgrade the software in the Cisco 860 and 880 Series Integrated Services Routers (ISRs) to Cisco IOS 12.4(22)T and the software in the Cisco 890 Series Integrated Services Router to Cisco IOS 12.4(22)YB.
- Make sure you have a TFTP or FTP server available for the software upgrade. Keep these guidelines in mind when setting up a TFTP or FTP server:
  - Controller software release 6.0.202.0 is larger than 32 MB; therefore, you must make sure that your TFTP server supports files that are larger than 32 MB. Some TFTP servers that support files of this size are tftpd and the TFTP server within the WCS. If you attempt to download the 6.0.202.0 controller software and your TFTP server does not support files of this size, the following error message appears: "TFTP failure while storing in flash."
  - If you are upgrading through the service port, the TFTP or FTP server must be on the same subnet as the service port because the service port is not routable, or you must create static routes on the controller.
  - If you are upgrading through the distribution system network port, the TFTP or FTP server can be on the same or a different subnet because the distribution system port is routable.
  - A third-party TFTP or FTP server cannot run on the same computer as WCS because the WCS built-in TFTP or FTP server and the third-party TFTP or FTP server require the same communication port.
- You can upgrade or downgrade the controller software only between certain releases. In some instances, you must first install an intermediate release prior to upgrading to software release 6.0.202.0. Table 1 shows the upgrade path that you must follow before downloading software release 6.0.202.0.

Table 1 Upgrade Path to Controller Software Release 6.0.202.0

Current Software Release	Upgrade Path to 6.0.202.0 Software
3.2.78.0 or later 3.2 release	Upgrade to 4.0.206.0 or later 4.0 release, then upgrade to 4.2.176.0, before upgrading to 6.0.202.0.
4.0.155.5 or later 4.0 release	Upgrade to 4.2.176.0 before upgrading to 6.0.202.0.
4.1.171.0 or later 4.1 release	Upgrade to 4.2.176.0 before upgrading to 6.0.202.0.
4.1.191.xM	Upgrade to 4.1.192.35M and then to 6.0.182.0 before upgrading to 6.0.202.0.
4.1.192.22M or 4.1.192.35M	Upgrade to 6.0.182.0 before upgrading to 6.0.202.0.
4.2.130.0 or earlier 4.2 release	Upgrade to 4.2.176.0 before upgrading to 6.0.202.0.
4.2.173.0 or later 4.2 release	You can upgrade directly to 6.0.202.0.
5.0.148.0 or later 5.0 release	You can upgrade directly to 6.0.202.0.
5.1.151.0 or later 5.1 release	You can upgrade directly to 6.0.202.0.
5.2.157.0 or later 5.2 release	You can upgrade directly to 6.0.202.0.
6.0.182.0 or later 6.0 release	You can upgrade directly to 6.0.202.0.

Note When you upgrade the controller to an intermediate software release, wait until all of the access points joined to the controller are upgraded to the intermediate release before you install the 6.0.202.0 software. In large networks, it can take some time to download the software on each access point.

Note You cannot install the Cisco Unified Wireless Network Controller Boot Software 5.2.157.0ER.aes file on Cisco 5500 Controller platform.

- For WiSM and standalone 4400 Controllers, we recommend that you install the Cisco Unified Wireless Network Controller Boot Software 5.2.157.0 ER.aes file. This file resolves CSCsm03461 and is necessary in order for you to view the version information for ER.aes files in the output of the **show sysinfo** CLI command. If you do not install this ER.aes file, your controller does not obtain the fix for this defect, and "N/A" appears in the Emergency Image Version field in the output of this command.

  Note The ER .aes files are independent from the controller software files. You can run any controller software file with any ER.aes file. However, installing the latest boot software file (5.2.157.0 ER.aes) ensures that the boot software modifications in all of the previous and current boot software ER.aes files are installed.

Caution If you require a downgrade from one release to another, you may lose the configuration from your current release. The workaround is to reload the previous controller configuration files saved on the backup server or to reconfigure the controller.

Software Release Support for Access Points

Table 2 lists the controller software releases that support specific Cisco access points. The First Support column lists the earliest controller software release that supports the access point. For access points that are not supported in ongoing releases, the Last Support column lists the last release that supports the access point.

Table 2 Software Support for Access Points

Access Points		First Support	Last Support
1000 Series	AIR-AP1010	3.0.100.0	4.2.207.0
	AIR-AP1020	3.0.100.0	4.2.207.0
	AIR-AP1030	3.0.100.0	4.2.207.0
	Airespace AS1200	—	4.0
1100 Series	AIR-LAP1121	4.0.155.0	—
	AIR-LAP1131	3.1.59.24	—
	AIR-LAP1141N	5.2.157.0	—
	AIR-LAP1142N	5.2.157.0	—

Table 2 Software Support for Access Points (continued)

Access Points		First Support	Last Support
1200 Series	AIR-AP1220A	3.1.59.24	—
	AIR-AP1220B	3.1.59.24	—
1230 Series	AIR-AP1230A	3.1.59.24	—
	AIR-AP1230B	3.1.59.24	—
	AIR-LAP1231G	3.1.59.24	—
	AIR-LAP1232AG	3.1.59.24	—
1240 Series	AIR-LAP1242G	3.1.59.24	—
	AIR-LAP1242AG	3.1.59.24	—
1250 Series	AIR-LAP1250	4.2.61.0	—
	AIR-LAP1252G	4.2.61.0	—
	AIR-LAP1252AG	4.2.61.0	—
1300 Series	AIR-BR1310G	4.0.155.0	—
1400 Series	Standalone Only	N/A	—
1500 Mesh Series	AIR-LAP-1505	3.1.59.24	4.2.176.51M
	AIR-LAP-1510	3.1.59.24	4.2.176.51M

Table 2 Software Support for Access Points (continued)

Access Points		First Support	Last Support
1520 Mesh Series	AIR-LAP1522AG	-A and N: 4.1.190.1 or 5.2 or later releases[1]	—
		All other reg. domains: 4.1.191.24M or 5.2 or later releases[1]	—
	AIR-LAP1522HZ	-A and N: 4.1.190.1 or 5.2 or later releases[1]	—
		All other reg. domains: 4.1.191.24M or 5.2 or later releases[1]	—
	AIR-LAP1522PC	-A and N: 4.1.190.1 or 5.2 or later releases[1]	—
		All other reg. domains: 4.1.191.24M or 5.2 or later releases[1]	—
	AIR_LAP1523CM	6.0.196.0	
	AIR-LAP1524SB	-A, C and N: 6.0 or later releases	—
	AIR-LAP1524PS	-A: 4.1.192.22M or 5.2 or later releases[1]	—

1. These access points are supported in the separate 4.1.19x.x Mesh Software Release train or with Release 5.2 or later releases. These access points are not supported in the 4.2, 5.0, or 5.1 Release trains.

Interoperability With Other Clients

This section describes the interoperability of the version of controller software with other client devices. Table 3 describes the configuration used for testing the clients.

Table 3 Test Bed Configuration for Interoperability

Hardware/Software Parameter	Hardware/Software Configuration Type
Release	6.0.202.0
Controller	Cisco 4400 Series Controller and Cisco 5500 Series Controller
Access Points	1131, 1142, 1242, 1252
Radio	802.11a, 802.11g, 802.11n2, 802.11n5
Security	Open, WEP, PSK (WPA and WPA2), 802.1X (WPA-TKIP and WPA2-AES) (LEAP, PEAP, EAP-FAST, EAP-TLS)
RADIUS	ACS 4.2, FreeRadius
Type of tests	Connectivity, traffic, and roaming between two access points.

Table 4 lists the versions of the clients. The traffic tests included data or voice. The clients included laptops, handheld devices, phones, and printers.

Table 4 Client Type

Client Type and Name	Version
Laptop	
Intel 3945/4965	13.4
Intel 5100/5300/6200/6300	13.4
Dell 1395/1397/Broadcom 4312HMG(L)	XP/Vista: 5.60.18.8 Win7: 5.30.21.0
Dell 1505/1510/Broadcom 4321MCAG/4322HM	5.60.18.8
Dell 1520/Broadcom 43224HMS	5.60.48.18
Atheros HB92/HB97	8.0.0.320
Atheros HB95	7.7.0.358
Apple MacBook Pro (Broadcom)	5.10.91.26
Apple iPad	4.2
Handheld Devices	
Falcon 4200/WinCE 4.2	5.60.21
Intermec CK3/WM 6,1:	6.20.33.0475
Intermec CK31/WinCE 4.2	4.02.00.0959
Intermec CN3/Windows Mobile 5.0	7.00.36.0592
Honeywell Dolphin 9900/ WM 6	1.71.2.0
Psion 7535/WinCE 5.0	2.03.47
Psion WAP/WinCE 5.0	1.02.42
Motorola Symbol 3090/WinCE 5.0	2.57.0.0.022
Motorola Symbol 4090/WinCE 5.0	2.5.0.0.049
Motorola Symbol 5590/WM 6.5	3.00.0.0.051
Motorola Symbol 7090 /WM 5.0	2.55.1.0.010
Motorola Symbol 9090/WinCE 5.0	2.57.0.0.022

Table 4 Client Type (continued)

Client Type and Name	Version
Phones and Printers	
Cisco 7921G	1.3.4LOADSR1
Cisco 7925G	1.3.4LOADSR2
Cisco Cius/Android 2.2	2.6.31.6-mrst
Apple iPhone 4	4.2
Ascom i75	1.7.10
Ascom i62	2.2.14
Nokia e72	021.024
Nokia N97	11.0.0.15
Spectralink 8030	119.067/122.023/123.023
Spectralink i640/PTX110	110.036/091.047/104.025
Vocera B1000A	4.1 1942
Vocera B2000	4.0.0.345
Zebra QL320	HTNVK49s
Monarch 9855	3.2AB
Samsung Galaxy/Android 2.2.1	2.2.1
HTC Hero/Android 1.5	2.6.27-8dd6deee
HTC Legend/Android 2.1	2.6.29-e3993620
Motorola Droid/Android 2.0	2.6.29-omap1
Blackberry Bold 9700	5.0.0.330
Blackberry Torch 9800	6.0 965

Special Rules for Upgrading to Controller Software 6.0.202.0 in Mesh Networks

Caution Before upgrading your controller to software release 6.0.202.0 in a mesh network, you must comply with the following rules.

Upgrade Compatibility Matrix

Table 5 outlines the upgrade compatibility of controller mesh and nonmesh releases and indicates the intermediate software releases required as part of the upgrade path.

Software Upgrade Notes

- You can upgrade from 4.1.192.22M and 4.1.192.35M to 6.0.202.0 without any configuration file loss. See Table 5 for the available upgrade paths.

Note If you downgrade to a mesh release, you must then reconfigure the controller. We recommend that you save the configuration from the mesh release before upgrading to release 6.0.202.0 for the first time. Then, you can reapply the configuration if you need to downgrade.

- You cannot downgrade from controller software release 6.0.202.0 to a mesh release (for example, 4.1.190.5, 4.1.191.22M, or 4.1.192.xM) without losing your configuration settings.
- Configuration files are in the binary state immediately after an upgrade from a mesh release to controller software release 6.0.202.0. After reset, the XML configuration file is selected.
- Do not edit XML files.
- Any field with an invalid value is filtered out and set to default by the XML validation engine. Validation occurs during bootup.
- If you upgrade the controller from software release 4.1.191.xM to 4.1.192.xM and then to software release 6.0.202.0, the controller might reboot without a crash file. To work around this problem, manually reset the controller without saving the configuration after you upgrade the controller to software release 6.0.202.0. Also, make sure to check the RRM configuration settings after the reset to verify that they are correct (CSCsv50357).

Table 5 Upgrade Compatibility Matrix for Controller Mesh and Nonmesh Releases from 4.0.206.0 release and above

Upgrade to / Upgrade from	6.0.202.0	6.0.199.4	6.0.196.0	6.0.188.0	6.0.182.0	5.2	4.1.192.35M	4.1.191.24M	4.1.190.5	4.1.185.0	4.1.171.0	4.0.219.0	4.0.217.204	4.0.217.0
6.0.199.4	Y	Y	Y	Y	Y									
6.0.196.0	Y	Y	Y	Y	Y									
6.0.188.0	Y	Y	Y	Y	Y									
6.0.182.0	Y	Y	Y	Y	Y									
4.1.192.35M					Y	Y								
4.1.192.22M					Y	Y	Y							
4.1.191.24M							Y	–						
4.1.190.5							Y [1]	Y	–					
4.1.185.0								Y	Y [2]	–				
4.1.181.0									Y [2]	Y [2]				

Table 5 Upgrade Compatibility Matrix for Controller Mesh and Nonmesh Releases from 4.0.206.0 release and above (continued)

Upgrade to	6.0.202.0	6.0.199.4	6.0.196.0	6.0.188.0	6.0.182.0	5.2	4.1.192.35M	4.1.191.24M	4.1.190.5	4.1.185.0	4.1.171.0	4.0.219.0	4.0.217.204	4.0.217.0
4.1.171.0									Y [2]	Y [2]	–			
4.0.219.0										Y [2]	Y [2]	–		
4.0.217.204								Y [2]		Y [2]	Y [2]	Y [2]	–	
4.0.217.0										Y [2]	Y [2]	Y [2]	Y [3]	–
4.0.216.0										Y [2]	Y [2]	Y [2]	Y [3]	Y
4.0.206.0										Y [2]	Y [2]	Y [2]	Y [3]	Y

1. You can upgrade directly from software release 4.1.190.5 to 4.1.192.35M; however, upgrading to 4.1.191.24M before upgrading to 4.1.192.35M is highly recommended.

2. Customers who require dynamic frequency selection (DFS) functionality should not use this release. This release does not provide DFS functionality fixes found in release 4.0.217.204. Additionally, this release is not supported in ETSI-compliant countries or Singapore.

3. Release 4.0.217.204 provides fixes for DFS on 1510 series access points. This functionality is needed only in countries where DFS rules apply.

Table 6 Upgrade Compatibility Matrix for Controller Mesh and Nonmesh Releases from 4.0.179.11 release and below versions

Upgrade to	4.0.217.0	4.0.216.0	4.0.206.0	4.0.179.11	4.0.179.8	4.0.155.5	4.0.155.0	3.2.195.10	3.2.193.5	3.2.171.6	3.2.171.5	3.2.150.10	3.2.150.6	3.2.116.21	3.2.78.0	3.1.111.0	3.1.105.0
Upgrade from																	
4.0.179.11	Y		Y [1]	–													
4.0.179.8	Y		Y [4]	Y	–												
4.0.155.5	Y		Y [4]	Y	Y	–											
4.0.155.0	Y		Y [4]	Y	Y	Y	–										
3.2.195.10	Y		Y [4]	Y	Y	Y		–									

Table 6 Upgrade Compatibility Matrix for Controller Mesh and Nonmesh Releases from 4.0.179.11 release and below versions

Upgrade to	4.0.217.0	4.0.216.0	4.0.206.0	4.0.179.11	4.0.179.8	4.0.155.5	4.0.155.0	3.2.195.10	3.2.193.5	3.2.171.6	3.2.171.5	3.2.150.10	3.2.150.6	3.2.116.21	3.2.78.0	3.1.111.0	3.1.105.0
3.2.193.5	Y		Y [4]	Y	Y	Y		Y	–								
3.2.171.6	Y		Y [4]	Y	Y	Y		Y		–							
3.2.171.5	Y		Y [4]	Y	Y	Y		Y		Y	–						
3.2.150.10	Y		Y [4]	Y	Y	Y		Y		Y		–					
3.2.150.6	Y		Y [4]	Y	Y	Y		Y		Y		Y	–				
3.2.116.21	Y		Y [4]	Y	Y	Y		Y		Y		Y		–			
3.2.78.0	Y		Y [4]	Y	Y	Y		Y		Y		Y		Y	–		
3.1.111.0								Y		Y		Y		Y	Y	–	
3.1.105.0								Y		Y		Y		Y	Y	Y	–
3.1.59.24								Y		Y		Y		Y	Y	Y	Y

1. An upgrade to 4.0.206.0 is not allowed in the following country codes when operating with the following access points: Australia (1505 and 1510), Brazil (1505 and 1510), Hong Kong (1505 and 1510), India (1505 and 1510), Japan (1510), Korea (1505 and 1510), Mexico (1505 and 1510), New Zealand (1505 and 1510), and Russia (1505 and 1510). Note: The 1505 mesh access point is not supported in release 5.0 and later releases. The 1510 mesh access point is supported only in mesh releases 4.1.190.5, 4.1.191.22M, and 4.1.192.xxM.

Upgrading to a New Software Release

When you upgrade the controller's software, the software on the controller's associated access points is also automatically upgraded. When an access point is loading software, each of its LEDs blinks in succession. Up to 10 access points can be concurrently upgraded from the controller.

Note The Cisco 5500 Series Controllers can download the 6.0.202.0 software to 100 access points simultaneously.

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, depending on the size of your network. However, with the increased number of concurrent

access point upgrades supported in software release 4.0.206.0 and later releases, the upgrade time should be significantly reduced. The access points must remain powered, and the controller must not be reset during this time.

Note In controller software release 5.2 or later releases, the WLAN override feature has been removed from both the controller GUI and CLI. If your controller is configured for WLAN override and you upgrade to controller software release 6.0.202.0, the controller deletes the WLAN configuration and broadcasts all WLANs. You can specify that only certain WLANs be transmitted by configuring access point groups. Each access point advertises only the enabled WLANs that belong to its access point group. Access point groups do not enable WLANs to be transmitted on per radio interface of AP.

Note If a WiSM controller is heavily loaded with access points and clients and is running heavy traffic, software upgrade sometimes causes Ethernet receive-path lockup and the hardware watchdog sometimes trips. You might need to reset the controller to return to normal operation.

Note Do not install the 6.0.202.0 controller software file and the 5.2.157.0 ER.aes boot software file at the same time. Install one file and reboot the controller, and then install the other file and reboot the controller.

To upgrade the controller software using the controller GUI, follow these steps:

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

Note We highly recommend that you back up your controller's configuration files prior to upgrading the controller software. Otherwise, you must manually reconfigure the controller.

Step 2 Obtain the 6.0.202.0 controller software and the Cisco Unified Wireless Network Controller Boot Software 5.2.157.0 ER.aes file from the Software Center on Cisco.com as follows:

a. Click this URL to go to the Software Center:

   http://tools.cisco.com/support/downloads/go/Redirect.x?mdfid=278875243

b. Click **Wireless Software**.

c. Click **Wireless LAN Controllers**.

d. Click **Standalone Controllers** or **Integrated Controllers and Controller Modules**.

e. Click a controller series.

f. If necessary, click a controller model.

g. If you chose Standalone Controllers in Step d., click **Wireless LAN Controller Software**.

h. If you chose Cisco Catalyst 6500 Series/7600 Series Wireless Services Module (WiSM) in Step e., click **Wireless Services Modules (WiSM) Software**.

i. Click a controller software release. The software releases are labeled as follows to help you determine which release to download:

   - **Early Deployment (ED)**—These software releases provide new features and new hardware platform support as well as bug fixes.

- **Maintenance Deployment (MD)**—These software releases provide bug fixes and ongoing software maintenance.
- **Deferred (DF)**—These software releases have been deferred. We recommend that you migrate to an upgraded release.

j. Click a software release number.

k. Click the filename (*filename*.aes).

l. Click **Download**.

m. Read Cisco's End User Software License Agreement and then click **Agree**.

n. Save the file to your hard drive.

o. Repeat steps a. through n. to download the remaining file (either the 6.0.202.0 controller software or the Cisco Unified Wireless Network Controller Boot Software 5.2.157.0 ER.aes file).

Step 3 Copy the controller software file (*filename*.aes) and the Cisco Unified Wireless Network Controller Boot Software 5.2.157.0 ER.aes file to the default directory on your TFTP or FTP server.

Step 4 Disable the controller 802.11a and 802.11b/g networks.

Step 5 Disable any WLANs on the controller.

Step 6 Choose **Commands** > **Download File** to open the Download File to Controller page.

Step 7 From the File Type drop-down box, choose **Code**.

Step 8 From the Transfer Mode drop-down box, choose **TFTP** or **FTP.**

Step 9 In the IP Address field, enter the IP address of the TFTP or FTP server.

Step 10 If you are using a TFTP server, the default values of 10 retries and 6 seconds for the Maximum Retries and Timeout fields should work fine without any adjustment. However, you can change these values if desired. To do so, enter the maximum number of times that the TFTP server attempts to download the software in the Maximum Retries field and the amount of time (in seconds) that the TFTP server attempts to download the software in the Timeout field.

Step 11 In the File Path field, enter the directory path of the software.

Step 12 In the File Name field, enter the name of the software file (*filename*.aes).

Step 13 If you are using an FTP server, follow these steps:

a. In the Server Login Username field, enter the username to log into the FTP server.

b. In the Server Login Password field, enter the password to log into the FTP server.

c. In the Server Port Number field, enter the port number on the FTP server through which the download occurs. The default value is 21.

Step 14 Click **Download** to download the software to the controller. A message appears indicating the status of the download.

Step 15 After the download is complete, click **Reboot**.

Step 16 If prompted to save your changes, click **Save and Reboot**.

Step 17 Click **OK** to confirm your decision to reboot the controller.

Step 18 After the controller reboots, repeat Step 6 to Step 17 to install the remaining file (either the 6.0.202.0 controller software or the Cisco Unified Wireless Network Controller Boot Software 5.2.157.0 ER.aes file).

Step 19 Reenable the WLANs.

Step 20 For Cisco WiSMs, reenable the controller port channel on the Catalyst switch.

Step 21 Reenable your 802.11a and 802.11b/g networks.

Step 22 If desired, reload your latest configuration file to the controller.

Step 23 To verify that the 6.0.202.0 controller software is installed on your controller, click **Monitor** on the controller GUI and look at the Software Version field under Controller Summary.

Step 24 To verify that the Cisco Unified Wireless Network Controller Boot Software 5.2.157.0 ER.aes file is installed on your controller, enter the **show sysinfo** command on the controller CLI and look at the Emergency Image Version field.

Note If you do not install the 5.2.157.0 ER.aes file, the Emergency Image Version field shows "N/A."

Installation Notes

This section contains important information to keep in mind when installing 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. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device.** Statement 1071

Warning **Only trained and qualified personnel should be allowed to install, replace, or service this equipment.** Statement 1030

Warning **Do not locate the antenna near overhead power lines or other electric light or power circuits, or where it can come into contact with such circuits. When installing the antenna, take extreme care not to come into contact with such circuits, as they may cause serious injury or death. For proper installation and grounding of the antenna, please refer to national and local codes (e.g. U.S.: NFPA 70, National Electrical Code, Article 810, Canada: Canadian Electrical Code, Section 54).** Statement 280

Warning **This product relies on the building's installation for short-circuit (overcurrent) protection. Ensure that a fuse or circuit breaker no larger than 120 VAC, 15A U.S. (240 VAC, 10A international) is used on the phase conductors (all current-carrying conductors).** Statement 13

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.** Statement 1024

Warning **Read the installation instructions before you connect the system to its power source.** Statement 10

Warning **Do not work on the system or connect or disconnect any cables (Ethernet, cable, or power) during periods of lightning activity. The possibility of serious physical injury exists if lightning should strike and travel through those cables. In addition, the equipment could be damaged by the higher levels of static electricity present in the atmosphere.** Statement 276

Warning **Do not operate the unit near unshielded blasting caps or in an explosive environment unless the device has been modified to be especially qualified for such use.** Statement 364

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.** Statement 339

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.** Statement 1017

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

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, 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

See the appropriate quick start guide or hardware installation guide for instructions on installing 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.

Using the Cisco 5500 Series Controller USB Console Port

The USB console port on the Cisco 5500 Series Controllers connects directly to the USB connector of a PC using a USB Type A-to-5-pin mini Type B cable.

Note The 4-pin mini Type B connector is easily confused with the 5-pin mini Type B connector. They are not compatible. Only the 5-pin mini Type B connector can be used.

For operation with Microsoft Windows, the Cisco Windows USB console driver must be installed on any PC connected to the console port. With this driver, you can plug and unplug the USB cable into and from the console port without affecting Windows HyperTerminal operations.

Note Only one console port can be active at a time. When a cable is plugged into the USB console port, the RJ-45 port becomes inactive. Conversely, when the USB cable is removed from the USB port, the RJ-45 port becomes active.

USB Console OS Compatibility

- Microsoft Windows 2000, XP, Vista (Cisco Windows USB console driver required)
- Apple Mac OS X 10.5.2 (no driver required)
- Linux (no driver required)

To install the Cisco Windows USB console driver, follow these steps:

Step 1 Follow these steps to download the USB_Console.inf driver file:

a. Click this URL to go to the Software Center:

http://tools.cisco.com/support/downloads/go/Redirect.x?mdfid=278875243

b. Click **Wireless LAN Controllers**.

c. Click **Standalone Controllers**.

d. Click **Cisco 5500 Series Wireless LAN Controllers**.

e. Click **Cisco 5508 Wireless LAN Controller**.

f. Choose the USB driver file.

g. Save the file to your hard drive.

Step 2 Connect the Type A connector to a USB port on your PC.

Step 3 Connect the mini Type B connector to the USB console port on the controller.

Step 4 When prompted for a driver, browse to the USB_Console.inf file on your PC. Follow the prompts to install the USB driver.

Note Some systems might also require an additional system file. You can download the Usbser.sys file from the Microsoft Website

The USB driver is mapped to COM port 6. Some terminal emulation programs do not recognize a port higher than COM 4. If necessary, change the Cisco USB systems management console COM port to an unused port of COM 4 or lower. To do so, follow these steps:

Step 1 From your Windows desktop, right-click **My Computer** and choose **Manage**.

Step 2 From the list on the left side, choose **Device Manager**.

Step 3 From the device list on the right side, double-click **Ports (COM & LPT)**.

Step 4 Right-click **Cisco USB System Management Console 0108** and choose **Properties**.

Step 5 Click the **Port Settings** tab and click the **Advanced** button.

Step 6 From the COM Port Number drop-down box, choose an unused COM port of 4 or lower.

Step 7 Click **OK** to save; then close the Advanced Settings dialog box.

Step 8 Click **OK** to save; then close the Communications Port Properties dialog box.

Important Notes for Controllers and Nonmesh Access Points

This section describes important information about controllers and nonmesh lightweight access points.

Cisco 1140 Series Access Points may record "watchdog timer expired" as last reset reason

The following error message sometimes appears as the last reset reason when the access points are power cycled:

```
Watchdog timer expired
```

This symptom is observed only in Cisco 1140 Series Access Point and does not have any impact on functionality. Ignore the watchdog timer expired after power cycled. You can also overwrite the reset reason to"reload" by rebooting with command operation.

Increase in the IGMP Timeout Value from 30 Seconds to 120 Minutes

To set the IGMP timeout, enter a value between 30 and 7200 seconds in the IGMP Timeout field. The controller sends three queries in one timeout value at an interval of *timeout* /3 (if the timeout value is more than 360 seconds, controller sends one query every 120 seconds, irrespective of the value configured) to see if any clients exist for a particular multicast group. If the controller does not receive a response through an IGMP report from the client, the controller times out the client entry from the MGID table. When no clients are left for a particular multicast group, the controller waits for the IGMP timeout value (if the timeout value is more than 360 seconds, controller waits for 360 seconds irrespective of the value configured) to expire and then deletes the MGID entry from the controller. The controller always generates a general IGMP query (that is, to destination address 224.0.0.1) and sends it on all WLANs with an MGID value of 1.

ARP Requests Sometimes Fail for Access Points Connected Directly to Cisco 2100 Series Controllers

Cisco 2100 Series Controllers do not support ARP requests from access points connected directly to a port on the controller unless there is an interface configured on that controller port. ARP requests from the access point cannot reach the gateway on the interface VLAN and the access point might lose its connection to the controller.

To work around this limitation, configure the access point’s default gateway to match the controller’s management IP address, or connect the access point to a switch port between the access point and the 2100 series controller.

HREAP AP VLAN Mapping

If the HREAP joins any other controller that does not have the same set of WLANs, the HREAP loses the previous mapping. To preserve the VLAN mapping in the AP, it is necessary that the AP join is restricted to the WLC for which it is primed. This implies that you must not have another discoverable WLC with a different configuration that should be available by other means (broadcast, DNS, Option 43, OTA, etc).

WPlus License Features Included in Base License

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

These WPlus license features are included in the base license:

- Office Extend AP
- Enterprise Mesh
- CAPWAP Data Encryption

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

- If you have a WPlus license and you upgrade from 6.0.18x to 6.0.202.0, your license file contains both Basic and WPlus license features. You will not see any disruption in feature availability and operation.
- If you have a WPlus license and you downgrade from 6.0.202.0 to 6.0.196 or 6.0.188, the license file in 6.0.202.0 contains both Basic and WPlus license features, so you will not see any disruption in feature availability and operation.
- If you have a base license and you downgrade from 6.0.202.0 to 6.0.196 or 6.0.188, when you downgrade, you lose all WPlus features.

Note Some references to Wireless LAN Controller WPlus licenses remain in WCS and in the controller CLI and GUI in release 6.0.202.0. However, WLC WPlus license features have been included in the Base license, so you can ignore those references.

Additive Licenses Available for Cisco 5500 Series Controllers

You can now purchase licenses to support additional access points on Cisco 5500 Series Controllers. The new additive licenses (for 25, 50, or 100 access points) can be upgraded from all license tiers (12, 25, 50, 100, and 250 access points). The additive licenses are supported through both rehosting and RMAs.

One-Time Password (OTP) Support

One Time Passwords (OTP) are supported on the Wireless Lan Controller (WLC) using TACACS and RADIUS. In this configuration, the controller acts as a transparent pass-through device. The controller forwards all client requests to the TACACS/RADIUS server without inspecting the client behavior.

When using OTP, the client must only establish a single connection to the controller to function properly. The controller currently does not have any intelligence or checks to correct a client that is trying to establish multiple connections.

RADIUS Called-station-id and Calling-station-id Attributes

In software releases prior to 6.0, the controller sends uppercase alpha characters in the MAC address. In software release 6.0 or later releases, the controller sends lowercase alpha characters in the MAC address for the RADIUS called-station-id and calling-station-id attributes. If you enabled these attributes for 802.1X authentication in previous releases and upgrade to software release 6.0, client authentication fails. Therefore, you must change the MAC addresses to lowercase characters on the RADIUS server before upgrading to software release 6.0.

Access Point Groups

You can create up to 50 access point groups for Cisco 2100 Series Controllers and controller network modules and up to 192 access point groups for Cisco 4400 Series Controllers, Cisco 5500 Series Controllers, the Cisco WiSM, and the 3750G wireless LAN controller switch.

Using Access Points in Sniffer Mode

You must disable IP-MAC address binding in order to use an access point in sniffer mode if the access point is joined to a 5500 series controller, a 2100 series controller, or a controller network module running software release 6.0. To disable IP-MAC address binding, enter this command using the controller CLI: **config network ip-mac-binding disable**.

WLAN 1 must be enabled in order to use an access point in sniffer mode if the access point is joined to a 5500 series controller, a 2100 series controller, or a controller network module running software release 6.0. If WLAN 1 is disabled, the access point cannot send packets.

Inter-Release Controller Mobility

When controllers in the mobility list are running different software releases (such as 5.0, 5.1, 5.2, and 6.0), Layer 2 or Layer 3 client roaming is not supported between GD to ED. It is supported only between controllers running the same and GD release such as 6.0 and 4.2.

Guest tunneling works only between controllers running the same software release or between controllers running software release 4.2 and controllers running any later software release (for example, 4.2 to 5.0, 4.2 to 5.1, 4.2 to 5.2, or 4.2 to 6.0). Guest tunneling does not work among controllers running other combinations of software.

RLDP Limitations in This Release

Rogue Location Discovery Protocol (RLDP) is a controller feature that detects the presence of rogue access points that are connected to your wired network. In this software release, RLDP operates with these limitations:

- RLDP detects rogue access points that are configured for open authentication.

- RLDP detects rogue access points that use a broadcast BSSID (that is, the access point broadcasts its SSID in beacons).
- RLDP detects only rogue access points that are on the same network. In other words, if an access list in the network prevents the sending of RLDP traffic from the rogue access point to the controller, RLDP does not work.
- RLDP does not work on 5-GHz dynamic frequency selection (DFS) channels.
- If the automatic RLDP attempt does not detect the rogue (due to a noisy RF environment, for example), the controller does not retry. However, you can initiate RLDP manually on a rogue at any time.

Also, in controller software release 6.0, the rogue containment packet transmission times have changed as follows:

- For monitor mode, rogue containment deauthentication packets are still sent at 100-msec intervals.
- For non-monitor mode, deauthentication packets are sent at 500 msec (minimum). In previous releases, they are sent at 100-msec intervals.

Internal DHCP Server

When clients use the controller's internal DHCP server, IP addresses are not preserved across reboots. As a result, multiple clients can be assigned the same IP address. To resolve any IP address conflicts, clients must release their existing IP address and request a new one.

Bootloader Menu

When you plug a controller into an AC power source, the bootup script and power-on self-test run to initialize the system. During this time, you can press **Esc** to display the bootloader Boot Options Menu. The menu options for the Cisco 5500 Series Controllers are different than for other controller platforms.

Bootloader Menu for Cisco 5500 Series Controllers

```
   Boot Options
Please choose an option from below:
 1. Run primary image
 2. Run backup image
 3. Change active boot image
 4. Clear Configuration
 5. Format FLASH Drive
    6. Manually update images
Please enter your choice:
```

Bootloader Menu for Other Controller Platforms

```
   Boot Options
Please choose an option from below:
 1. Run primary image
 2. Run backup image
 3. Manually update images
 4. Change active boot image
 5. Clear Configuration
```

Please enter your choice:

Enter **1** to run the current software, enter **2** to run the previous software, or enter **4** (on a 5500 series controller) or **5** (on another controller platform) to run the current software and set the controller configuration to factory defaults. Do not choose the other options unless directed to do so.

Note Only options 1 through 3 are available on Cisco 5500 Series Controllers in FIPS mode.

Note See the Installation Guide or Quick Start Guide for your controller for more details on running the bootup script and power-on self-test.

Fragmented Pings

Cisco 5500 Series Controllers do not support fragmented pings on any interface. Similarly, Cisco 4400 Series Controllers, the Cisco WiSM, and the Catalyst 3750G Integrated Wireless LAN Controller Switch do not support fragmented pings on the AP-manager interface.

802.11g Controller and 802.11b Clients

When a controller is configured to allow only 802.11g traffic, 802.11b client devices are able to successfully associate to an access point but cannot pass traffic. When you configure the controller for 802.11g traffic only, disable any channels (such as channel 14 in Japan) that allow associations from 802.11b client devices.

FIPS 140-2

The Cisco 4400 Series Controllers, the Cisco WiSM, and the Catalyst 3750G Wireless LAN Controller Switch have received NIST FIPS 140-2 Level 2 certification. Click this link to view the NIST Security Policies and compliant software versions:

http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401vend.htm

CAPWAP Problems with Firewalls and ACLs

If you have a firewall or access control list (ACL) between the controller and its access points that allows LWAPP traffic, before upgrading to software release 5.2 or later releases and CAPWAP, you should allow CAPWAP traffic from the access points to the controller by opening the following destination ports:

- UDP 5246
- UDP 5247

The access points use a random UDP source port to reach these destination ports on the controller. In controller software release 5.2, LWAPP was removed and replaced by CAPWAP, but if you have a new out-of-the-box access point, it could try to use LWAPP to contact the controller before downloading the CAPWAP image from the controller. Once the access point downloads the CAPWAP image from the controller, it uses only CAPWAP to communicate with the controller.

Note After 60 seconds of trying to join a controller with CAPWAP, the access point falls back to using LWAPP. If it cannot find a controller using LWAPP within 60 seconds, it tries again to join a controller using CAPWAP. The access point repeats this cycle of switching from CAPWAP to LWAPP and back again every 60 seconds until it joins a controller.

Note An access point with the LWAPP recovery image (an access point converted from autonomous mode or an out-of-the-box access point) uses only LWAPP to try to join a controller before downloading the CAPWAP image from the controller.

Messages Appearing Upon Controller Bootup

Several messages might flood the message logs when the controller boots up. These messages appear because of a failure to read or delete several different configuration files. These are low-severity messages that can safely be ignored. They do not affect controller functionality. These are some examples:

```
Mar 18 16:05:56.753 osapi_file.c:274 OSAPI-5-FILE_DEL_FAILED: Failed to delete the file :
sshpmInitParms.cfg. file removal failed.
-Process: Name:fp_main_task, Id:11ca7618
Mar 18 16:05:56.753 osapi_file.c:274 OSAPI-5-FILE_DEL_FAILED: Failed to delete the file :
bcastInitParms.cfg. file removal failed.
-Process: Name:fp_main_task, Id:11ca7618
```

Web Authentication Redirects

The controller supports web authentication redirects only to HTTP (HTTP over TCP) servers. It does not support web authentication redirects to HTTPS (HTTP over SSL) servers.

Note For Cisco 5500 Series Controllers, Cisco 2100 Series Controllers, and controller network modules, you must configure a preauthentication access control list (ACL) on the WLAN for the external web server and then choose this ACL as the WLAN preauthentication ACL under Security Policies > Web Policy on the WLANs > Edit page.

Cisco 1250 Series Access Points and Cisco 7920 IP Phones

Cisco 1250 Series Access Points are not supported for use with the Cisco 7920 IP phone. They can, however, be used with the Cisco 7921 and 7925 IP phones.

Crash Files for Cisco 1250 Series Access Points

The Cisco 1250 Series Access Points may contain a bootloader older than version 12.4(10b)JA. Units with old bootloaders do not generate a crash log when a crash occurs. The crash log is disabled so that a crash does not corrupt the flash file system. Units with bootloader versions 12.4(10b)JA or later versions generate a crash log if the access point is associated to a controller running software release 4.2.112.0 or later releases.

New Cisco 1250 Series Access Points shipped from the factory contain new bootloader images, which fix the flash file system after it is corrupted during a crash (without losing files). This new bootloader automatically sets a new CRASH_LOG environment variable to “yes,” which enables a crash log to be generated following a crash but only on controllers running software release 4.2.112.0 or later releases. Therefore, no user configuration is needed to enable a crash log on new Cisco 1250 Series Access Points shipped from the factory.

This example shows how to enable debugging on access point AP01:

```
debug ap enable AP01
```

This example shows how to debug the **show version** command on access point AP02:

```
debug ap command show version AP002
```

Information similar to the following appears:

```
Tue July 06 09:31:38 2010: AP001b.d513.1754: BOOTLDR: C1250 Boot Loader
(C1250-BOOT-M) Version 12.4(10b)JA, RELEASE SOFTWARE (fc1)
```

This example shows how to display the access point version number:

```
show version
```

Information similar to the following appears:

```
BOOTLDR: C1250 Boot Loader (C1250-BOOT-M) Version 12.4(10b)JA, RELEASE SOFTWARE (fc1)
```

Configuration File Stored in XML

In controller software release 4.2.61.0 and later releases, the controller’s bootup configuration file is stored in an Extensible Markup Language (XML) format rather than in binary format. Therefore you cannot download a binary configuration file onto a controller running software release 4.2.61.0 or later releases. However, when you upgrade a controller from a previous software release to 4.2.61.0 or later releases, the configuration file is migrated and converted to XML.

Note Do not download a configuration file to your controller that was uploaded from a different controller platform. For example, a Cisco 5500 Series Controller does not support the configuration file from a Cisco 4400 Series or 2100 Series Controller.

In controller software release 4.2 or later releases, the controller’s bootup configuration file is stored in an Extensible Markup Language (XML) format rather than in a binary format. Therefore, you cannot download a binary configuration file onto a controller running software release 4.2 or later releases. However, when you upgrade a controller from a previous software release to 4.2 or later releases, the configuration file is migrated and converted to XML.

Note Controller software release 5.2 or later releases enable you to read and modify the configuration file. See the “Editing Configuration Files” section on page 29 for details. Controller software releases prior to 5.2 do not allow configuration files to be modified. If you attempt to make changes to a 4.2, 5.0, or 5.1 configuration file and then download the file to a controller, the controller displays a cyclic redundancy checksum (CRC) error while it is rebooting and returns the configuration parameters to their default values.

Saving Configurations

Controllers contain two kinds of memory: volatile RAM and NVRAM. At any time, you can save the configuration changes from active volatile RAM to nonvolatile RAM (NVRAM) using one of these commands:

- **save config**—Saves the configuration from volatile RAM to NVRAM without resetting the controller.
- **reset system**—Prompts you to confirm that you want to save configuration changes before the controller reboots.
- **logout**—Prompts you to confirm that you want to save configuration changes before you log out.

Editing Configuration Files

When you save the controller's configuration, the controller stores it in XML format in flash memory. Controller software release 5.2 or later releases enable you to easily read and modify the configuration file by converting it to CLI format. When you upload the configuration file to a TFTP or FTP server, the controller initiates the conversion from XML to CLI. You can then read or edit the configuration file in a CLI format on the server. When you are finished, you download the file back to the controller, where it is reconverted to an XML format and saved.

To edit the controller's configuration file, follow these steps:

Step 1 Upload the configuration file to a TFTP or FTP server using either the GUI or the CLI.

Step 2 Read or edit the configuration file on the server. You can modify or delete existing CLI commands and add new CLI commands to the file.

Note To edit the configuration file, you can use either Notepad or WordPad on Windows or the VI editor on Linux.

Step 3 Save your changes to the configuration file on the server.

Step 4 Download the configuration file to the controller using either the GUI or the CLI.

The controller converts the configuration file to an XML format, saves it to flash memory, and then reboots using the new configuration. CLI commands with known keywords and proper syntax are converted to XML while improper CLI commands are ignored and saved to flash memory. Any CLI commands that have invalid values are replaced with default values. To see any ignored commands or invalid configuration values, enter this command:

show invalid-config

Note You cannot execute this command after the **clear config** or **save config** command.

Step 5 If the downloaded configuration contains a large number of invalid CLI commands, you might want to upload the invalid configuration to the TFTP or FTP server for analysis using either the GUI or the CLI. The controller does not support the uploading and downloading of port configuration CLI commands. If you want to configure the controller ports, enter these commands:

- **config port linktrap** {*port* | **all**} {**enable** | **disable**}—Enables or disables the up and down link traps for a specific controller port or for all ports.
- **config port adminmode** {*port* | **all**} {**enable** | **disable**}—Enables or disables the administrative mode for a specific controller port or for all ports.

Step 6 Save your changes by entering this command:

save config

LWAPP Mode Changes

When you upgrade to controller software release 5.0.148.0 or later releases, the LWAPP mode changes to Layer 3 if it was previously configured for Layer 2.

If you downgrade from controller software release 6.0.202.0, 6.0.199.4, 6.0.196.0, 6.0.188.0, 5.2.178.0, 5.2.157.0, 5.1.151.0, or 5.0.148.0 to 4.2.61.0 or an earlier release, the LWAPP mode changes from Layer 3 to Layer 2. Access points might not join the controller, and you must manually reset the controller to Layer 3 to resolve this issue.

Access Points Send Multicast and Management Frames at Highest Basic Rate

Access points running recent Cisco IOS versions transmit multicast frames at the highest configured basic rate and management frames at lowest basic mandatory rates. This can cause reliability problems. Access points running LWAPP or autonomous Cisco IOS should transmit multicast and management frames at the lowest configured basic rate. Such behavior is necessary to provide good coverage at the cell's edge, especially for unacknowledged multicast transmissions where multicast wireless transmissions may fail to be received.

Because multicast frames are not retransmitted at the MAC layer, clients at the edge of the cell may fail to receive them successfully. If reliable reception is a goal, then multicast frames should be transmitted at a low data rate. If support for high data rate multicast frames is required, then it may be useful to shrink the cell size and disable all lower data rates.

Depending on your specific requirements, you can take the following action:

- If you need to transmit multicast data with the greatest reliability and if there is no need for great multicast bandwidth, then configure a single basic rate, one that is low enough to reach the edges of the wireless cells.
- If you need to transmit multicast data at a certain data rate in order to achieve a certain throughput, then configure that rate as the highest basic rate. You can also set a lower basic rate for coverage of non-multicast clients.

Disabling Radio Bands

The controller disables the radio bands that are not permitted by the configured country of operation (CSCsi48220).

40-MHz Channels in the 2.4-GHz Band

This is not supported in 6.0.202.0 release.

802.11a Channels 120, 124, and 128 Disabled

802.11a channels 120, 124, and 128 are disabled to achieve compliance with draft EN 301 893 version 1.5.1 on the following -E regulatory domain products: AP1131AG, AP1243AG, and AP1252AG.

Multicast Queue Depth

The multicast queue depth is 512 packets on all controller platforms. However, the following message might appear on 2106 controllers: "Rx Multicast Queue is full on Controller." This message does not appear on Cisco 4400 Series Controllers because the 4400 NPU filters ARP packets while all forwarding (multicast or otherwise) and multicast replication are done in the software on the 2106.

This message appears when too many multicast messages are sent to the CPU. In controller software releases prior to 5.1, multicast, CDP, and ARP packets share the same queue. However, in software releases 5.1 and later releases, these packets are separated into different queues. There are currently no controller commands that can be entered to determine if the multicast receive queue is full. When the queue is full, some packets are randomly discarded.

MAC Filtering for WGB Wired Clients

Controller software release 4.1.178.0 or later releases enables you to configure a MAC-filtering IP address for a workgroup bridge (WGB) wired client to allow passive WGB wired clients, such as terminal servers or printers with static IP addresses, to be added and remain in the controller's client table while the WGB is associated to a controller in the mobility group. This feature, activated by the **config macfilter ipaddress** *MAC_address IP_address* CLI command, can be used with any passive device that does not initiate any traffic but waits for another device to start communication.

This feature allows the controller to learn the IP address of a passive WGB wired client when the WGB sends an IAPP message to the controller that contains only the WGB wired client's MAC address. Upon receiving this message from the WGB, the controller checks the local MAC filter list (or the anchor controller's MAC filter list if the WGB has roamed) for the client's MAC address. If an entry is found and it contains an IP address for the client, the controller adds the client to the controller's client table.

Note Unlike the existing MAC filtering feature for wireless clients, you are not required to enable MAC filtering on the WLAN for WGB wired clients.

Note WGB wired clients using MAC filtering do not need to obtain an IP address through DHCP to be added to the controller's client table.

CKIP Not Supported with Dynamic WEP

In controller software release 4.1.185.0 or later releases, CKIP is supported for use only with static WEP. It is not supported for use with dynamic WEP. Therefore, a wireless client that is configured to use CKIP with dynamic WEP is unable to associate to a wireless LAN that is configured for CKIP. We recommend that you use either dynamic WEP without CKIP (which is less secure) or WPA/WPA2 with TKIP or AES (which are more secure).

Setting the Date and Time on the Controller

Cisco Aironet lightweight access points do not connect to the controller if the date and time are not set properly. Set the current date and time on the controller before allowing the access points to connect to it.

Containment of Rogue AP and Rogue Client

Containment of rogue AP and rogue client does not work for particular drivers like Intel.

Synchronizing the Controller and Location Appliance

For controller software release 4.2 or later releases, if a location appliance (release 3.1 or later releases) is installed on your network, the time zone must be set on the controller to ensure proper synchronization between the two systems. Also, we highly recommend that the time be set for networks that do not have location appliances. Refer to Chapter 4 of the *Cisco Wireless LAN Controller Configuration Guide, Release 6.0* for instructions for setting the time and date on the controller.

Note The time zone can be different for the controller and the location appliance, but the time zone delta must be configured accordingly, based on Greenwich Mean Time (GMT).

FCC DFS Support on Cisco 1130 Series Access Points

Federal Communications Commission (FCC) dynamic frequency selection (DFS) is supported only on 1130 series access points in the United States, Canada, and the Philippines that have a new FCC ID. Access points use DFS to detect radar signals such as military and weather sources and then switch channels to avoid interfering with them. The Cisco 1130 Series Access Points with FCC DFS support have an FCC ID *LDK102054E* sticker. The Cisco 1130 Series Access Points without FCC DFS support have an *LDK102054* (no *E* suffix) sticker. The Cisco 1130 Series Access Points that are operating in the United States, Canada, or the Philippines, have an FCC ID *E* sticker, are running the 4.1.171.0 software release or later releases, and can use channels 100 through 140 in the UNII-2 band.

Inaccurate Transmit Power Display

After you change the position of the 802.11a radio antenna for a lightweight Cisco 1200 or Cisco 1230 Series Access Point, the power setting is not updated in the controller GUI and CLI. Regardless of the user display, the internal data is updated, and the transmit power output is changed accordingly. To see the correct transmit power display values, reboot the access point after changing the antenna's position. (CSCsf02280)

Setting the Retransmit Timeout Value for TACACS+ Servers

We recommend that the retransmit timeout value for TACACS+ authentication, authorization, and accounting servers be increased if you experience repeated reauthentication attempts or the controller falls back to the backup server when the primary server is active and reachable. The default retransmit timeout value is 2 seconds and can be increased to a maximum of 30 seconds.

Configuring an Access Point's Prestandard Power Setting

An access point can be powered by a Cisco prestandard 15-watt switch with Power over Ethernet (PoE) by entering this command:

config ap power pre-standard {**enable** | **disable**} {**all** | *Cisco_AP*}

A Cisco prestandard 15-watt switch does not support intelligent power management (IPM) but does have sufficient power for a standard access point. The following Cisco prestandard 15-watt switches are available:

- AIR-WLC2106-K9
- WS-C3550, WS-C3560, WS-C3750
- C1880
- 2600, 2610, 2611, 2621, 2650, 2651
- 2610XM, 2611XM, 2621XM, 2650XM, 2651XM, 2691
- 2811, 2821, 2851
- 3631-telco, 3620, 3640, 3660
- 3725, 3745
- 3825, 3845

The **enable** version of this command is required for full functionality when the access point is powered by a Cisco prestandard 15-watt switch. It is safe to use if the access point is powered by either an IPM switch or a power injector or if the access point is not using one of the 15-watt switches listed above.

You might need this command if your radio operational status is "Down" when you expect it to be "Up." Enter the **show msglog** command to look for this error message, which indicates a PoE problem:

```
Apr 13 09:08:24.986 spam_lrad.c:2262 LWAPP-3-MSGTAG041: AP 00:14:f1:af:f3:40 is unable to
verify sufficient in-line power. Radio slot 0 disabled.
```

Controller Functions that Require a Reboot

After you perform these functions on the controller, you must reboot the controller in order for them to take effect:

- Enable or disable link aggregation (LAG)
- Enable a feature that is dependent on certificates (such as HTTPS and web authentication)
- Add new or modify existing SNMP v3 users
- Install a license, change the license feature set, or change the priority of an AP-count evaluation license on a Cisco 5500 Series Controller

Cisco 2106 Controller LEDs

The Cisco 2106 Series Controller's Status LED and AP LED do not flash amber when software is being uploaded to the controller or downloaded to an access point, respectively.

Note Some versions of the *Cisco 2106 Wireless LAN Controller Quick Start Guide* might incorrectly state that these LEDs flash amber during a software upload or download.

Rate-Limiting on the Controller

Rate-limiting is applicable to all traffic destined to the CPU from either direction (wireless or wired). We recommend that you always run the controller with the default **config advanced rate enable** command in effect in order to rate-limit traffic to the controller and protect against denial-of-service (DoS) attacks. You can use the **config advanced rate disable** command to stop rate-limiting of Internet Control Message Protocol (ICMP) echo responses for testing purposes. However, we recommend that you reapply the **config advanced rate enable** command after testing is complete.

GLBP Not Supported

Controller software release 4.2 or later releases is not compatible with the Gateway Load Balancing Protocol (GLBP). Make sure to configure the controller's default gateway to a fixed address and not to the GLBP virtual address.

Cisco 4400 Series Controllers Do Not Forward Subnet Broadcasts through the Guest Tunnel

As designed, Cisco 4400 Series Controllers do not forward IP subnet broadcasts from the wired network to wireless clients across the EoIP guest tunnel.

Preventing Clients from Accessing the Management Network on a Controller

To prevent or block a wired or wireless client from accessing the management network on a controller (from the wireless client dynamic interface or VLAN), the network administrator should ensure that there is no route through which to reach the controller from the dynamic interface or use a firewall between the client dynamic interface and the management network.

Voice Wireless LAN Configuration

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

Changing the IOS LWAPP Access Point Password

Cisco IOS Lightweight Access Point Protocol (LWAPP) access points have a default password of *Cisco*, and the pre-stage configuration for LWAPP access points is disabled by default. To enable it, you must configure the access point with a new username and password when it joins the controller. Enter this command using the controller CLI to push a new username and password to the access point:

config ap mgmtuser add *user_id* **password** *password* {*Cisco_AP* | **all**}

- The *Cisco_AP* parameter configures the username and password on the specified access point.
- The **all** parameter configures the username and password on all the access points registered to the controller.

The password pushed from the controller is configured as “enable password” on the access point.

There are some cases where the pre-stage configuration for LWAPP access points is disabled and the access point displays the following error message when the CLI commands are applied:

“ERROR!!! Command is disabled.”

For more information, see the *Upgrading Autonomous Cisco Aironet Access Points to Lightweight Mode.*

Exclusion List Client Feature

If a client is not able to connect to an access point, and the security policy for the WLAN and client are 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.

RADIUS Servers and the Management VLAN

If a RADIUS server is on a directly connected subnet (with respect to the controller), then that subnet must be the management VLAN subnet.

RADIUS Servers

This product has been tested with CiscoSecure ACS 4.2 and later releases and works with any RFC-compliant RADIUS 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.

Using the Backup Image

The controller bootloader 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 2: Run Backup Image** from the boot menu to boot from the backup image. Then, upgrade with a known working image and reboot the controller.

Home Page Retains Web Authentication Login with IE 5.x

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

Ad-Hoc Rogue Containment

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

Changing the Default Values of SNMP Community Strings

The controller has commonly known default values of “public” and “private” for the read-only and read-write SNMP community strings. Using these standard values presents a security risk. Therefore, we strongly advise that you change these values. See the *Cisco Wireless LAN Controller Configuration Guide, Release 6.0*, for configuration instructions. In addition, restore of config backup could result with re-enabling default communities or snmp communities disabled with incorrect privileges. You should manually reconfigure these snmp communities in this situation. SNMP configuration should be reviewed after config restore on a new WLC (from defaults).

Changing the Default Values for SNMP v3 Users

The controller uses a default value of "default" for the username, authentication password, and privacy password for SNMP v3 users. Using these standard values presents a security risk. Therefore, we strongly advise that you change these values. See the *Cisco Wireless LAN Controller Configuration Guide, Release 6.0,* for configuration instructions.

Note SNMP v3 is time sensitive. Make sure that you have configured the correct time and time zone on your controller.

Features Not Supported on Cisco 2100 Series Controllers

This hardware feature is not supported on Cisco 2100 Series Controllers:

- Service port (separate out-of-band management 10/100-Mbps Ethernet interface)
- Termination of guest controller tunnels (origination of guest controller tunnels is supported)
- External web authentication web server list
- Port mirroring
- AppleTalk
- QoS per-user bandwidth contracts
- IPv6 pass-through
- Link aggregation (LAG)
- Multicast-unicast mode

Features Not Supported on Cisco 5500 Series Controllers

These software features are not supported on Cisco 5500 Series Controllers:

- For Cisco 5500 Series Controllers, you are not required to configure an AP-manager interface. The management interface acts like an AP-manager interface by default, and the access points can join on this interface.
- Port mirroring.
- Layer 2 access control list (ACL) support.
- Configuration of 802.3 bridging, AppleTalk, and Point-to-Point Protocol over Ethernet (PPPoE).

Note The Cisco 5500 Series Controllers bridge these packets by default. If desired, you can use ACLs to block the bridging of these protocols.

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.

2106 Image Not Supported for 3504 Controllers

The 2106 controller image is supported for use with only Cisco 2100 Series Controllers. Do not install the 2106 image on a 3504 controller. Otherwise, errors may occur. Install only the 3504 image on a 3504 controller.

Important Notes for Controllers and Mesh Access Points

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

Features Not Supported on Mesh Networks

The following controller features are **not** supported on mesh networks:

- Multi-country support
- Load-based CAC (Mesh networks support only bandwidth-based, or static, CAC.)
- High availability (fast heartbeat and primary discovery join timer)
- Access point join priority (Mesh access points have a fixed priority.)
- Locally significant certificate
- Location-based services

Caveats

The following sections lists Open Caveats and Resolved Caveats for Cisco controllers and lightweight access points for version 6.0.202.0. For your convenience in locating caveats in Cisco's Bug Toolkit, the caveat titles listed in this section are drawn directly from the Bug Toolkit database. These caveat titles are not intended to be read as complete sentences because the title field length is limited. In the caveat titles, some truncation of wording or punctuation might be necessary to provide the most complete and concise description. The only modifications made to these titles are as follows:

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

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

https://tools.cisco.com/bugsearch/

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

https://tools.cisco.com/IDREG/guestRegistration.do?locale=en_US

Open Caveats

Table 7 lists open caveats in controller software release 6.0.202.0.

Table 7 Open Caveats

ID Number	Description
CSCts70063	Headline: bootup "Error (xx) found in fsck check - attempt to repair" Symptom: When a 5500 series wireless LAN controller boots, a message similar to the following may appear on the console: `Error (2048) found in fsck check - attempt to repair` The specific error number within parenthesis might vary. Conditions: Booting up a 6.0 release of controller software on a Cisco 5508 Controller manufactured from June (serial number range FCW1511xxxx or later). Workaround: Ignore the message. This condition is strictly cosmetic; the error has no effect on the functioning of the controller. If you upgrade to a 7.0 release of the controller software, the message does not appear.
CSCsw93671	Headline: Controller sources packets for web auth clients from management or service-port int. Symptom: When you see traffic on the network being sourced from the service port, all these packets are either SYN, ACK, or FIN ACK packets with either a source port of TCP 2006 or TCP 2008. The service port is not connected to the network and when you look through the sniffer captures, there is no packet going to the controller that would cause these packets to be sent. Condition: The condition seems to happen rarely when a client associated to web-auth enabled WLAN sends only a TCP SYN for a web-session and terminates the connection. Workaround: None.

Table 7 Open Caveats (continued)

ID Number	Description
CSCtb78072	Headline: SNMPv3 communication breaks with NAC Appliance CAM. Symptom: Wireless clients are not moving into the access state even when the NAC agent on the client passed posture validation. This issue originates because of the following: 1. The controller reboots in between 2. The CAM is using an old SNMPv3 session to communicate (send Traps) with the controller Above are Quarantine to access traps that are dropped by the controller due to a mismatch in their SNMP session (CAM - old , WLC- new after reboot). Conditions: SNMPv3 is used for traps originating from the NAC appliance CAM to WLC. Workaround: On the CAM, change SNMPv3 to SNMPv2 and immediately change it back to SNMPv3. The existing SNMPv3 connections will be reset and reinitiated.
CSCtb23682	Headline: When logged into 5500 via telnet, characters are shown multiple times. Symptom: When logging into the WLC via Telnet, you may experience characters appearing multiple times when you press the key. An example is as follows: <Switch> telnet <IP Address> Trying <IP Address>... Connected to <IP Address>. Escape character is '^]'. ^M User:aaddmmiinn^M Password:l*a*b*^M (WLC) >sshh ow aapp ssuu mmary ^M Conditions: Unknown. Workaround: You can end the current session and attempt a new Telnet session.
CSCth36045	Headline: SNMP OID is not increasing in clcrRoamReasonReport table. Symptom: SNMP walk on WLC stops at clcrRoamReasonReport table because the OID is not increasing. Conditions: Unknown. Workaround: If you are using snmp-get tool for SNMP walk, use the -Cc option to ignore this problem. The other tools might have similar options.
CSCti06835	Headline: Multicast packets are stuck on the radio forever after WLAN changes. Symptom: TXSM Beacon information is incremented constantly and you can see this problem when you enter the **show controller do0** command. Conditions: The controller running 7.0.98.0. AP believes that the packet is stuck on the radio. The following is the TXSM Beacon information: Monitoring State: 1 Flags: 80000000 Beacons seen: 30628334 Time since: 2 Max Time w/o beacons: 135 Beacon stopped count: 0 Counts > 120 1 Counts > 90 0 Counts > 60 0 Counts > 30 0 Counts > 15 0 Counts > 10 0 Counts > 5 2642 Workaround: Disable the radio and enable it again.

Table 7 Open Caveats (continued)

ID Number	Description
CSCtj58064	Headline: CAPWAP encap ICMP reply pkt from mgmt int uses burned-in mac in HSRP. Symptom: CAPWAP encapsulated ICMP reply packets from management interface in different subnet uses SVI burned-in MAC address as the destination MAC address instead of HSRP virtual MAC address. Conditions: This problem happens when multiple Nexus switches are used in the HSRP configurations. Workaround: 1. Do not use HSRP. 2. If you are using a Nexus, then you need to enable the vPC **peer gateway** command.
CSCtj97821	Headline: The WLC does not use a consistent MAC address for forwarding traffic. Symptom: Src MAC address for WLC packets may be inconsistent. Conditions: When LAG is enabled on the WLC, src MAC address of WLC packets may not be LAG MAC but port MAC. Workaround: None.
CSCtj53036	Headline: PMK timers removed on client, so session timeout is changed to infinite. Symptom: This is a very rare condition. When the timers are removed on the client, the session timeout changes to infinite without PMK. Randomly, the WPA2 clients are showing up with the session timeout as infinite. Conditions: 1. WLAN session timeout is not infinite. 2. AAA override. 3. The **sh pmk-cache all** command does not have any entry for client. Workaround: Deauthenticate the client.
CSCtn16347	Headline: WLC does not rewrite DHCP ACK packets correctly for DHCP inform. Symptom: DHCP ACK packets are not rewritten correctly to DHCP inform packets by the WLC (in DHCP Proxy Mode): Sent as broadcast and server IP is not rewritten. This has no functionality impact on the DHCP protocol. Conditions: This problem happens when the DHCP server replies to DHCP inform packets (Authoritative mode). Workaround: None.
CSCtn44422	Headline: LAP detects an AES-CCMP replay error after WGB-AP 802.1x authentication. Symptom: LAP detects an AES-CCMP replay error after WGB-AP 802.1X authentication. The issue continues until the next WGB-AP 802.1X authentication. During this issue, WGB-AP and all WGB wired clients cannot communicate with the network. Conditions: WLC 6.0.199.4 WGB 12.4(21a)JY, 12.4(25d)JA Workaround: Use WPA-TKIP instead of WPA2-AES.

Table 7 Open Caveats (continued)

ID Number	Description
CSCti83804	Headline: Slow Memory leak in emWeb. Symptom: This is a very rare condition. Slow memory leak occurred in emweb task when a client page is visited when there are no clients. Conditions: This problem occurs when a user navigates to WLC GUN's Monitor > Client page and there are no clients to be shown. Error message is shown. If this screen is accessed multiple times when there are no clients, there is a small leak. Workaround: It is not expected that real deployments will have scenarios where there are no clients. It can be seen that there are no clients, in that case, the user should not navigate to this page.
CSCtj45508	Headline: Controller mobility control and data path shows as "down". Symptom: Mobility does not work with clients. Conditions: The mobility path between the wireless LAN controller in the mobility setup is going down (both control and data). It is found internally in scale testing in 72 wireless LAN controllers and 5000 clients, but this problem is not consistently reproducible. Workaround: None as of now, rebooting is the only option.
CSCtn96348	Headline: Config restore error for SNMP community. Symptom: Restore of config backup in the 5508 controller ends with SNMP communities disabled or without RW privileges. Condition: During the restore of config backup operation, some entries of SNMP communities are modified when the wireless LAN controller comes up. Workaround: Manually reconfigure the SNMP community. This is specifically impacting the second entry.
CSCti59414	Headline: Unable to add 72 mobility group member Symptom: Cannot add mobility member. Conditions: WLC1: 5508 code: 6.0.199.0 mac:68:ef:bd:8e:e8:60 WLC2:5508 code:6.0.199.0 mac:68:ef:bd:8e:96:a0 Same issue is there is 4400 and 2106 also Issue: When adding the mobility member to WLC1 via GUI; this error is shown "Error adding mobility member" Tried adding using CLI on WLC1: (wlc-unv-3-02) > config mobility group member add 68:EF:BD:8E:96:A0 10.34.100.246 UNV1 Invalid parameter provided. msglogs indicate: *Sep 01 13:45:04.548: %USMDB-3-MSGTAG006: usmdb_mm.c:891 Cannot add Mobility Member, duplicate IP, Saved Member:68:ffffffef:ffffffbd:ffffff8e:ffffff96:ffffffa0 Member:00:00:00:00:00:00, IP: 10.34.100.246 Workaround: (wlc-unv-3-02) config mobility group member delete 00:00:00:00:00:00 this clears the member that was failing to be added and then re-issue. For example, config mobility group member add 68:EF:BD:8E:96:A0 10.34.100.246 UNV1

Table 7 Open Caveats (continued)

ID Number	Description
CSCtj05569	Headline: WLC is not releasing the BIND for the 1st LDAP, next user fail auth Symptom: 1. User1 authenticating, wlc binds with configured username wlc admin, search for user1, user1 found in the tree, wlc binds with user1 to test password and user1 gets authenticated. 2. User2 authenticating, wlc does not bind with wlcadmin, rather keeps the bind of user1 and search for user2 with user1 bind. search doesn't find user2 since user1 doesn't have search priv and authentication for user2 fails. 3. The WLC is keeping the bind for the previous user and it is not releasing it. Conditions: If the READ permission is not given to the users to search for the other users in the LDAP account. Workaround: When READ permission is provided to the User to search for other user on the LDAP account, it does work. PS: This fix is provided only for J-MR1 release. This will not be fixed in H-MR as this is a new change and the earlier day-1 behavior no customer reported this issue. Also, this was discussed with escalation team not to fix this in H-MR4.
CSCtg67029	Headline: 'show client tsm' does not display full output. Symptom: 'show client tsm', web, and SNMP do not report full TSM information for all clients. Conditions: This happens in a very big setup when the TSM reports fill up the availability memory for TSM. Workaround: Cleanup the TSM reports which are not required.
CSCto25030	Headline: AP hostname displays 31 characters after upgrading to 6.0 on WLC Symptom: Access Point host-name displays 31 characters after upgrading to 6.0. Condition: Access Point initially configured for 32 characters for the host-name. Post upgrade to 6.0 only 31 characters are shown when you run-config and show ap summary commands. Workaround: Add 32 characters in the GUI.

Resolved Caveats

Table 8 lists caveats resolved in controller software release 6.0.202.0.

Table 8 Resolved Caveats

ID Number	Caveat Title
CSCso22875	Access points get disconnected during code upgrade
CSCsw68997	HREAP AP VLAN mappings are mismatched.
CSCsv14863	Controller sends and displays channel 0 and power level 0 settings to AP
CSCsv34136	WLC should not enforce source port check on RFC3576 Disconnect-Request
CSCsv97224	Customer web not selected still user prompted with custom page

Table 8 Resolved Caveats (continued)

ID Number	Caveat Title
CSCsw80627	Controller fails to respond on task emWeb in 5.1.151.0
CSCsx50408	LWAP DOS Attack trap message does not record the source MAC address
CSCsx94570	AP is stuck in image state and not responding to join response
CSCsz14861	Virtual Domain broken for maps
CSCta72642	Access Point logging related command not getting uploaded
CSCtb16583	AP changes from Static IP to DHCP and doesn't covert back to Static
CSCtb23924	HREAP: WebAuth user cannot logout after roaming
CSCtb49021	WLC 5508 with APs fails to respond multiple times at spamApTask
CSCtb91371	Non-root users unable to authenticate for AP timers config list page
CSCtc01947	Initial CAWAP Packets are sent to burned-in mac by controller in HSRP
CSCtc32748	Noise/Channel measurements not done on all DCA channels
CSCtc74940	HREAP is stuck in standalone mode even when CT5500 is reachable
CSCtc87690	Clients are mapped to the native VLAN of the h-reap AP switchport trunk
CSCtd29026	WCS can't create static WEP key with same index number on different WLAN
CSCtd49495	AP crashes in heap check process due to red zone overrun
CSCtd58904	AP crash on SNMP query
CSCtd72280	Multicast mobility accepts reserved multicast address
CSCtd74870	Massive DHCP flood / loop with NAC OOB - DHCP Proxy disabled
CSCtd75094	AP fails to respond when clearing CAPWAP MGIDs for new client
CSCtd82509	WLC fails to respond when performing findContextInfo+268
CSCtd90694	Cannot create a session with WiSM slot with DHCP enabled service port
CSCtd99602	Wired Guest: DHCP Required Breaks Web Auth Following Session Timeout
CSCte08057	AW: J: FFT: 5508 freezes with crash
CSCte08161	cannot get IP address from server if key-management is “wpa optional”
CSCte18071	there are several inconsistencies of MAC address on WLC
CSCte19845	Emergency image lost on upgrade to 6.0.190.0
CSCte24079	2106 LAN hangs after high load with duplex mismatch
CSCte39477	Web GUI: External Web Servers Field Needs to Always Be Displayed
CSCte45826	AP drops packets with SIP Based CAC- WPA2/AES or tcp-adjust-mss/WPA/TKIP
CSCte53175	Per-User bandwidth contract blocks all traffic when set to 0
CSCte57615	1250 AP cannot negotiate PoE through CDP with dot1x enabled on the port
CSCte78841	1250 Unicast transmit queue locks up in Tx to client X
CSCte95626	5508 controller not forwarding 100% of packets for Gig Line Burst
CSCtf11461	J: CPU ACL check for Outbound ICMP traffic should be removed on 5500
CSCtf17352	MSE goes unreachable because of out-of-memory in an overloaded system
CSCtf23192	Solid DB 4.50.150 in WCS become unresponsive

Table 8 Resolved Caveats (continued)

ID Number	Caveat Title
CSCtf27779	Show tech from CAPWAP ap does not include capwap info
CSCtf39826	AP 1131 stops responding to Polycom phone
CSCtf57349	WLC only allows 47 Ap's to join on single port
CSCtf62737	WLC URL Sanitation Issue
CSCtf69598	Memory leak in AP on CCKM Failure
CSCtf72094	AP1250 d1 goes into reset status immediately after reboot
CSCtf81266	APF-1-ROGUE_CLIENT_UPDATE_FAILED filling up syslog
CSCtf84619	WLC should not take into account the antenna gain on 1522 on 5.8ghz
CSCtf90579	With TACACS/Radius auth, lobby admin unable to edit Guest user role
CSCtf91342	After bad UN used, LDAP server not functional for 15 minutes
CSCtg09589	Duplex mismatch When 1140 AP is Directly Connected to 2100 WLC
CSCtg21950	WGB intracontroller roaming must update its clients without IAPP frame
CSCtg23396	“show dhcp stats” will not display when DHCP Proxy is changed to enabled
CSCtg23491	WLC does not process flooded unicast traffic properly
CSCtg23618	WiSM goes unreachable outside of Cat6k
CSCtg30694	WLC webauth client never has to reauthenticate after session timeout
CSCtg41911	Radio may stop transmitting for several seconds due to MSDU packet load
CSCtg42711	SANITY:5500 DP CRASH: Hardware deadlock - all Packet Buffers in use
CSCtg50508	Mbuf leaks have been seen during webauth test
CSCtg51702	Degraded voice performance on HREAP local switching with TKIP + CCKM
CSCtg57607	WGB fails to send IAPP updates after roaming
CSCtg70271	Observed WEBAUTH_REQD (8) Reached ERROR: from line 4055 in client debug.
CSCtg80660	WCM: Clients are not getting IP when connected to OEAP behind a PAT
CSCtg84677	AP is deauthenticated with a reason: power capability is unacceptable
CSCtg92171	WLC stops responding to network
CSCtg94347	AP fails to join intermittently due to wrong source port generated in AP
CSCtg96725	Mesh testbed is UP even when the network "A" is disabled
CSCtg97178	File/Socket handle is Invalid. Handle = 0. after downgrading to HMR3
CSCtg97706	WCS - Remove the 5 sec option from the auto refresh on the maps.
CSCth08926	WLC 5508 fails with the Task Name: emWeb
CSCth12513	LAG fail-over does not work on CT5508
CSCth14584	Msglog reports %LWAPP-4-AP_DUPLEX_MISMATCH when connected to 3Com Switch
CSCth17649	OEAP does not update rogue information to controller
CSCth19326	cldCountryTable is not lexicographically ordered
CSCth25811	Mobility anchor configuration is not displayed on GUI after config upload

Table 8 Resolved Caveats (continued)

ID Number	Caveat Title
CSCth27809	Running the CLI command crashes the WLC
CSCth30456	Need to prevent from enabling vlan support for OEAP
CSCth31771	AP crashes while changing mode to H-REAP
CSCth33080	LAP mark DSCP CS3 to Priority 3 as 11e UP instead of 4
CSCth37438	A few WLCs will be missing for CLI templates
CSCth37539	Wrong error message is displayed while applying 802.11b/g template
CSCth38561	Client moving between guest SSID to any other SSID would not work.
CSCth41876	AMAC: MFP - Invalid MIC error due to held beacons on the radio
CSCth42489	Multicast traffic stops after fast roaming - incorrect AP client count
CSCth43717	1520 RAP drop all gig interface traffic after losing connection to WLC
CSCth48443	Location Appliance stops tracking Wireless Client when WLC code is 7.0
CSCth51509	AW: controller crash at task dtlArpTask
CSCth59030	The AP1140 fails for radio status check task
CSCth60816	Mesh: A MAP fails to join the WLC again if the MAP switches a RAP
CSCth61007	False absence notification if the device probes slower than config value
CSCth65673	InSNMPv3, unable to add controllers on WCS & seeing wrong MAC addr
CSCth68708	Clients are unable to get a DHCP offer from WLC internal DHCP scope
CSCth69732	The 1252 APs moves to probes disabled status intermittently
CSCth70299	WCS: untaggedInterfaceWithSamePort error when changing DHCP server addr
CSCth73209	Increase max IGMP timeout from 5 minutes to 2 hours
CSCth90250	WLC does not bridge DHCP NAK to station and puts it into the RUN state
CSCth91462	Video admission control admission threshold tuning values changed.
CSCth93062	WLC may hang due to kernel Oops exception.
CSCth93785	5508WLC Generate Duplicate IP Add Message & Cause Connectivity Issue
CSCth95098	WCS: SSLv2 should be disabled by default
CSCth95281	WCS adds mobility group members using incorrect MAC address
CSCth96194	WLC kernel hang followed by flash issue, WLC not rebooting.
CSCth96617	Native VLAN configuration is not consistent in HREAP
CSCth98074	clMeshNodeBatteryChargingState OID always returns '1'
CSCti00211	Association fails on H-REAP AP when client changes SSID
CSCti00488	ARP entry cannot be deleted permanently in WLC
CSCti01885	Drop down window for selecting AP's primary WLC is too small
CSCti02690	AP1140 Ethernet link problem when setting both speed and duplex
CSCti04259	Intermittent webauth page with HREAP local switching
CSCti06687	MSE unable to start due to database corruption
CSCti21621	switch CAM table not updated after L2 roam

Table 8 Resolved Caveats (continued)

ID Number	Caveat Title
CSCti28989	Can't create secondary AP-manager interface on the same VLAN as primary
CSCti34667	WLC 5508 drops TCP, UDP packets
CSCti35617	Management interface does not use HSRP MAC address when replying
CSCti37832	Memory leak caused by https
CSCti45379	CT5508 crashes when trying to shut the data ports one by one
CSCti49408	JIAN & TALWAR with 18-line banner unresponsive after clear config
CSCti73277	Prioritized data to WMM client is marked incorrectly in 802.11QoS header
CSCti79172	Security baseline violation: backup restore on unit replacement
CSCti83830	Passive clients are unable to pass traffic on 5500, working on 4400 WLCs
CSCti86618	AP3500 in local mode stops servicing allowed WLANs on 2.4GHz
CSCti87085	AP pre-download marks version numbers incorrectly
CSCti91944	Unified APs removing clients on maximum retries.
CSCtj02084	JMR1: Ambassador Crash on task emWeb running stress test
CSCtj09107	C1130_rack3_gig1_0_30 crashed "CAPWAP CLIENT" CPU Vector: Unknown
CSCtj16545	MSE: Out of memory due to API calls to GetTagLocationList
CSCtj16960	WLC with of Web-auth users may go unreachable or fail to redirect client
CSCtj20996	Controller unresponsive when using a Bluetooth console serial adapter
CSCtj21321	AP error due to process_execute; unexpected exception to CPUvector
CSCtj21464	WLC dataplane core fails to respond due to memory corruption
CSCtj23398	HA Status toggles between Primary Active & Primary Lost Secondary
CSCtj26384	WCS not updating SSC after migrating 1230 AP
CSCtj28483	C1130 core dump: Radio command cmd 21 (FF50,0,0) status 7F17
CSCtj30204	Chirp DFS detection removal on ETSI 11n radios
CSCtj30518	ARP storm can cause out of sync CAPWAP AP-WLC situation for mesh
CSCtj33453	WLC emWeb error when running 6.0.199 in disabled client page
CSCtj47041	JMR1:AP crashes and coredumps due to low memory
CSCtj47495	5508: WLC is forwarding traffic on incorrect VLAN in AP-group setup
CSCtj55649	Delay in packet transmission causing beacon outages on non-11n APs
CSCtj61260	11r IE should be removed from open auth reassociation response
CSCtj74549	Failed to add controller to WCS
CSCtj81930	AP1140 reboot by 'Reason: Radio Not Beaconing for too long'
CSCtj95360	Single radio h-reap ap not joining back to WLC.
CSCtj96734	Association fails intermittently on H-REAP with: At maximum associations
CSCtk08478	AW: AP stops send/ack for 20-500ms to new Polycom phone
CSCtk11838	WiSM memory leak on mobility task
CSCtk12832	ARP poisoning attack from wireless client on dynamic interface

Table 8 Resolved Caveats (continued)

ID Number	Caveat Title
CSCtk32374	AP crash on CheckAdjustTransmitRate due to packet retries of WGB
CSCtk34878	JMR1:1130/1240: Crash in cdp_prot accessing freed memory
CSCtk34919	IF-MIB:ifDescr changed in release 5.2 and later
CSCtk36070	H-MR4: All user groups show Unknown exception error message
CSCtk53570	DP crash file sometimes contains incomplete backtrace
CSCtk53680	WiSM not able to ftp coredump when running low on memory
CSCtk60177	WLC 4402 (SW 7.0.98.0) crash with "Out of Memory" and "mwar_exit.crash"
CSCtk83586	Controller Crash Task: dtlArpTask
CSCtk95795	Controller fails at spamReceiveTask due to "show ap eventlog"
CSCtk99565	JMR: Memory management changes to avoid memory exhaustion/corruption
CSCtl04377	DHCP flooded with redundant anchors and proxy disabled
CSCtl42414	Possible re-entrancy and bad share problems in the upstream DTLS code
CSCtl42518	Old Security reports should be removed
CSCtl55910	HMR4: 5508 crash in task apfRLDP
CSCtl66341	HMR4: Fix to eliminate AMAC AP crash in process_one_rx_packet
CSCtl71583	Memory leak sshpm, on sshencode. line 252
CSCtl91742	Access Point 1240 Memory leak in CAPWAP capwap_ap_add function
CSCtl98648	WCS 6.X fails to download 7.X image for the MSE
CSCtn13199	Access Point 1140 crashes in dot11_driver_fwd_ba_pak
CSCtn14126	ARP client protection breaks DHCP address reuse
CSCtn17195	NM-WLC6 upgrade from 6.0 to 7.0 is not supported.
CSCtn17501	Access Point 1130 crashing in "check heaps" with MFP enabled
CSCtn21868	WCS fail to add WiSM due to Table too large, possible agent loop
CSCtn40435	The access point's middle packet pool is constantly grown and trimmed
CSCtn59116	Failed to run report on the Client TSM Report
CSCtn80024	When J4 country code is enabled, 3500-Q fails to join
CSCtg09159	Radio may get stuck in RESET or DOWN state.

If You Need More Information

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

https://tools.cisco.com/bugsearch/

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

Troubleshooting

For the most up-to-date, detailed troubleshooting information, see the Cisco Support and Documentation website at:

http://www.cisco.com/c/en/us/support/index.html

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

Documentation Updates

This section lists updates to user documentation that has not yet been added to either printed or online documents.

Omissions

The Package Contents section in the *Quick Start Guide: Cisco 4400 Series Wireless LAN Controllers* should be updated to include this item, which is included with the 4400 series controller:

- DB-9-to-DB-9 null modem cable

Related Documentation

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

- *The quick start guide or installation guide for your particular controller or access point*
- *Cisco Wireless LAN Controller Configuration Guide*
- Cisco Wireless LAN Controller Command Reference
- *Cisco Wireless Control System Configuration Guide*

Click this link to browse to the Cisco Support and Documentation page:

http://www.cisco.com/c/en/us/support/index.html

Obtaining Documentation and Submitting a Service Request

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

http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html

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