Release Notes for Cisco Wireless LAN Controllers and Mesh Access Points for Release 4.1.190.5

Last revised: April 09, 2009

These release notes describe features, enhancements, and caveats in Release 4.1.190.5 and IOS version AP 12.4(3g)JMA1.

Release 4.1.190.5 is supported on the following Cisco Wireless LAN controller platforms: 2100 series, 4400 series and Wireless Service Module (WiSM) for the Catalyst 6500; and is compatible with the Cisco Wireless Control System (WCS), Release 4.1 and greater.

Release 4.1.190.5 is compatible with Release 4.1.91.0 of the Cisco Wireless Control System (WCS).

Release 4.1.190.5 supports the following outdoor mesh access points:

- Cisco Aironet 1500 Series (AP1505, AP1510, AP1520)

Note AP1520 is only supported in the United States in Release 4.1.190.5.

Caution If your network is operating with 1520s or you plan to install 1520s in your network, you must set the boot variable on the 1520 before upgrading from release 4.1.190.5 to 4.1.191.24M (or greater release). This ensures the 1520 joins correctly (CSCsl70218). Refer to "Mandatory Boot Variable Update for Networks with 1520s" section on page 10 for specific configuration details.

Caution Please see the "Software Images" section on page 7 for important software upgrade and compatibility details prior to upgrading to this release.

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

Note Release 4.1.190.5 does not support the following indoor Cisco Lightweight Access Points:

- 1000 series, 1100 series, 1130 series, 1200 series, 1230 series, 1240 series and 1300 series
- Although indoor access points are not supported in this release, controllers operating with Release 4.1.190.5 can interoperate with indoor access points that are connected to separate controllers operating with releases such as 4.1.185.0 and earlier that support the relevant indoor (standard) access points.

Note Refer to the *Cisco Aironet 1500 Series Outdoor Mesh Access Point Hardware Installation Guide* and *Cisco Aironet 1520 Series Outdoor Mesh Access Point Hardware Installation Guide* for details on the physical installation and initial configuration of the mesh access points at http://www.cisco.com/en/US/products/ps8368/tsd_products_support_series_home.html

Note Refer to the *Cisco Wireless LAN Controller Configuration Guide, Release 4.1*for details on the Release 4.1.190.5 features and their configuration at http://www.cisco.com/en/US/products/ps6366/products_installation_and_configuration_guides_list.html

Contents

These release notes contain the following sections:

Overview of Features

Release 4.1.190.5 provides extended wireless mesh features beyond that offered in the main Cisco Unified Wireless Network (CUWN) release base. From this release on, mesh-specific features will only be available in the mesh release series until it is merged back into the main CUWN sequence at a future date.

Note Feature support varies depending on the mesh access point. See ***Table 3*** for a detailed summary of feature support by model.

Although a controller installed with Release 4.1.190.5 does not support configuration and management of indoor (standard) access points (1000, 1100, 1130, 1200, 1230, 1240 and 1300 series), it does support interoperability of outdoor mesh access points with indoor access points and client roaming between indoor and outdoor access points, when the indoor access points are associated with a separate controller. Additionally, any controller dedicated to indoor access points must have software that supports the relevant indoor access points.

A single interface, Cisco WCS, is available for configuration and management of those controllers that manage indoor and outdoor access points separately.

RAP versus MAP Functionality

Access points within a mesh network operate as either a *root access point (RAP)* or a *mesh access point (MAP)*. All AP1500 (AP1505, AP1510, AP1520) outdoor access points are by default configured as MAPs. At least one access point within a mesh network must be configured to function as a RAP.

Note Refer to the "Configuring Bridging Parameters" section in Chapter 7 of the *Cisco Wireless LAN Controller Configuration Guide, Release 4.1* for details on configuring an access point as a RAP. This information is available online at the following link: http://www.cisco.com/en/US/products/ps6366/products_configuration_guide_chapter09186a008082d707.html#wp1115408

RAPs within the network have a wired connection to the controller and MAPs communicate among themselves and back to the RAP using wireless connections over the backhaul. MAPs use the AWPP protocol to determine the best path through the other mesh access points to the controller. All the possible paths between the MAPs and RAPs form the wireless mesh that is used to carry traffic from wireless LAN clients connected to MAPs and to carry traffic from devices connected to MAP Ethernet ports.

Table 1 details interoperability of AP1505, AP1510 and AP1520 in Release 4.1.190.5.

Table 1 Root Access Point and Mesh Access Point Interoperability Platform

RAP and MAP Interoperability	AP1505 MAP	AP1510 MAP	AP1520 MAP
AP1505 RAP	Yes	No	No
AP1505 MAP	Yes	No	No
AP1510 RAP	No	Yes	No
AP1510 MAP	No	Yes	No
AP1520 RAP	No	Yes	Yes
AP1520 MAP	No	No	Yes

Hardware Features

Release 4.1.190.5 supports the following outdoor wireless access points:

- The AP1505 which is equipped with a single 2.4-GHz radio that provides client access and data backhaul to other AP1500s.
- The AP1510 which is equipped with two simultaneously operating radios: a 2.4-GHz radio used for client access and a 5-GHz radio used for data backhaul to other AP1500s.
- The AP1520 (1522) which is equipped with two simultaneously operating radios: a 2.4-GHz radio used for client access and a 5-GHz radio used for data backhaul to other AP1500s.

Table 2 Hardware Features by Platform

Feature/Platform	AP1505	AP1510	AP1520
2.4 GHz Band	X	X	X
4.9 GHz Band	–	X	X
5.47 GHz Band	–	X[1]	–
5.8 GHz Band	–	X[2]	X
DOCSIS 2.0 Cable Modem (Optional)	–	–	X
Fiber Module (Optional)	–	–	X
External Battery Status	X	X	–
Internal Battery Status	–	–	X
LED Indicator[3]	X	X	X

1. The 5.47 GHz band is used by the -E and -K regulatory domains.
2. The 5.8 GHz band is used by the -A, -C, -N and -S regulatory domains.
3. A detachable, removable Cisco LED indicator is available to detect power for the AP1505 and AP1510.

Cisco Aironet 1520 Access Point (NEW)

The Cisco Aironet 1520 like the AP1505 and AP1510 employs Cisco's Adaptive Wireless Path Protocol (AWPP) to form a dynamic wireless mesh network among mesh access points, and wireless access to any Wi-Fi-compliant client device.

The Cisco Aironet 1520 series lightweight outdoor mesh access point has a dual-radio configuration (802.11a and 802.11b/g). Communication between the outdoor mesh access points (MAPs) is over the 802.11a radio backhaul. Client traffic is generally transmitted over the 802.11b/g radio.

- Uplinks support includes: Gigabit Ethernet (1000BaseT), and small form-factor pluggable (SFP) slot for fiber (100BaseBX) or cable modem interface.
- Power options include: 90 to 480VAC Streetlight Power, 12VDC, cable power, Power over Ethernet (POE), and internal battery backup power.

Key Features on the Cisco Aironet 1520 series include:

- Improved 802.11b/g radio sensitivity and range performance on the three-channel Maximal Ratio Combining (MRC)
- 802.3af-compliant Power over Ethernet out to connect powered device (PD) IP devices
- LED status indicators
  - Status (AP and software)
  - Uplink (Ethernet, Cable or Fiber)
  - RF-1 (802.11b/g radio status)
  - RF-2 (802.11a radio status)
- NEMA 4X certified enclosure, certifiable for hazardous locations (Class 1, Division 2 / Zone 2. Group B,C,D - United States/Canada/EU)
- Paintable enclosure

Software Features

A summary of the software features supported by each access point is provided in Table 3.

Table 3 Cisco AP 1500 Series Feature Support Matrix for 4.1.190.5

Feature/Platform	AP1505	AP1510	AP1520
Mesh Network Functionality			
Passive scanning–Access point searches for an alternative parent on its current backhaul.	X	X	X
Background Scanning–Access point searches for an alternative parent on any possible backhaul channel.	X	X	–
Optimal Parent Selection–Access point joins the best available parent.	X	X	X
Exclusion Listing–Access point avoids selecting as parent those access points which have a pattern of failing.	X	X	X

Table 3 Cisco AP 1500 Series Feature Support Matrix for 4.1.190.5 (continued)

Feature/Platform	AP1505	AP1510	AP1520
Radar-free Coordinated Sector–Access point notifies parent when radar is detected on the channel so an alternative channel can be employed by the sector.	X	X	–[1]
Dynamic Frequency Selection–Alternative channel is selected when radar is detected in regulated bands.	–	–	–[1]
Synchronized Channel Change–Parent advises children of intended channel change.	X	X	–
Reliable Link Layer, Extended Retries–Transmissions that do not succeed will extend the number of retry attempts in an effort to improve reliability.	X	X	X
Reliable Link Layer, Secondary Backhaul Radio–A secondary backhaul radio is utilized as a temporary path for traffic that cannot be sent on the primary backhaul due to intermittent interference.	–	X	–
Passive Beaconing–Log messages from an access point that cannot connect are relayed through other access points to the controller.	X	X	–
Network Services Functionality			
Ethernet Bridging–Traffic is bridged from hosts connected to a wired port.	X	X	X
Containment of Bridged Multicast Traffic–Multicast traffic (e.g. video camera broadcasts) from a MAP Ethernet port is contained on a RAP Ethernet network and no forwarding occurs (In mode Multicast). This ensures that: (1) Non-LWAPP multicasts received by the RAP are not transmitted back to the MAP Ethernet networks within the mesh network (their point of origin). (2) MAP-to-MAP multicasts do not occur because they are filtered out.	X	X	–
Universal Access–Radio used for backhaul traffic provides access for client traffic	X	X	–
Support for Workgroup Bridges–Allows multiple wired hosts to connect to the wireless network through a workgroup bridge.	X	X	–
Multiple Queues for Backhaul Traffic–Extends client traffic prioritization to the backhaul traffic.	X	X	X
Static Call Admission Control (CAC)–Ensures sufficient bandwidth is available in a mesh sector before serving new T-SPEC client call requests.	–	X	–

Table 3 Cisco AP 1500 Series Feature Support Matrix for 4.1.190.5 (continued)

Feature/Platform	AP1505	AP1510	AP1520
Mesh Security			
EAP Authentication–Restricts mesh node access to approved, authenticated access points. EAP-FAST authentication provides secure authentication and encryption key management.	X	X	X
Applications			
High-speed Roaming–Roam speeds of up to 70 mph are supported for Cisco Compatible Extension v4 clients.	–	X	–
Location–Client location is identified by closest access point.	X	X	–

1. The AP1520 is only supported in the US in Release 4.1.190.5.

Software Images

Table 4 lists the names of the images associated with this release.

Table 4 Software Images Associated with Release 4.1.190.5

Products	4.1.190.5 and Related Software Images		
Access Point		**Image**	**Boot Image**
	1505	VxWorks	VxWorks
	1510	VxWorks	VxWorks
	1520	c1520-k9w9-tar.124-3g.JMA1	c1520-boot-m.124-3g.JMA1
WLC-4400	AIR-WLC4400-K9-4-1-190-5-MESH.aes		
WLC-2100	AIR-WLC2100-K9-4-1-190-5-MESH.aes		
WiSM	SWISMK9-4-1-190-5-MESH.aes		
WCS	WCS-STANDARD-K9-4.1.91.0.exe **Note** For release 4.1.190.5, Cisco WCS is only supported on Windows Server 2003.		
WCS Navigator	NAVIGATOR-K9-1.0.91.0.exe **Note** For release 4.1.190.5, Cisco WCS Navigator is only supported on Windows Server 2003.		

System Requirements

You can install this software release on the following Cisco Wireless LAN controller platforms: 2100 series, 4400 series and Wireless Service Module (WiSM) for the Catalyst 6500.

Release 4.1.190.5 is the first standalone mesh release for controllers.

Note

- You must install Release 4.1.190.5 to operate AP1520s in your mesh network. Any release other than that release will not support an AP1520.
  - If an AP1520 is already connected in the network, and you downgrade the software release within your network, the 1520 will not connect and might become stranded.
- If the AP1520 is going to be installed in a mesh network that is also operating with AP1510s, note the following:
  - The network must first be upgraded to a version of 4.1.18x.x before upgrading to Release 4.1.190.5.
  - The AP1520 should not be added to the network until Release 4.1.190.5 is running on the network to ensure proper communication between the AP1510 and AP1520.
  - Mobility groups functionality is supported when operating with 4.1.190.5 and all 4.1.x versions of non-mesh controller software.
- Refer to the "Upgrading to this Software Release" section on page 10 for detailed upgrade information.

Compatibility Matrix

Table 5 outlines compatibility of controller non-mesh releases with controller mesh releases and indicates the intermediate software releases required as part of the upgrade path. A summary of upgrade path requirements is noted in the "Upgrading to this Software Release" section on page 10.

Table 5 Compatibility Matrix for Controller Mesh and Non-Mesh Releases

Upgrade to / Upgrade from	4.1.190.5	4.1.185.0	4.1.171.0	4.0.219.0	4.0.217.204	4.0.217.0	4.0.216.0	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	3.1.59.24
4.1.190.5	–																						
4.1.185.0	Y[1]	–																					
4.1.181.0	Y[1]	Y[1]																					
4.1.171.0	Y[1]	Y[1]	–																				
4.0.219.0		Y[1]	Y[1]	–																			
4.0.217.204		Y[1]	Y[1]	Y[1]	–																		
4.0.217.0		Y[1]	Y[1]	Y[1]	Y[2]	–																	
4.0.216.0		Y[1]	Y[1]	Y[1]	Y[2]	Y	–																
4.0.206.0		Y[1]	Y[1]	Y[1]	Y[2]	Y		–															
4.0.179.11						Y		Y[3]	–														
4.0.179.8						Y		Y[3]	Y	–													
4.0.155.5						Y		Y[3]	Y	Y	–												
4.0.155.0						Y		Y[3]	Y	Y	Y	–											
3.2.195.10						Y		Y[3]	Y	Y	Y		–										
3.2.193.5						Y		Y[3]	Y	Y	Y		Y	–									
3.2.171.6						Y		Y[3]	Y	Y	Y		Y		–								
3.2.171.5						Y		Y[3]	Y	Y	Y		Y		Y	–							
3.2.150.10						Y		Y[3]	Y	Y	Y		Y		Y		–						
3.2.150.6						Y		Y[3]	Y	Y	Y		Y		Y		Y	–					
3.2.116.21						Y		Y[3]	Y	Y	Y		Y		Y		Y		–				
3.2.78.0						Y		Y[3]	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. CUSTOMERS THAT 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.
2. Release 4.0.217.204 provides fixes for DFS. This functionality is only needed in countries where DFS rules apply.
3. 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).

Upgrading to this Software Release

For instructions on downloading software to the controller using either Cisco WCS or the controller GUI or CLI, refer to the release 4.1 versions of the *Cisco Wireless Control System Configuration Guide and* the *Cisco Wireless LAN Controller Configuration Guide*.

Click this link to access those documents:

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

Upgrade Path to Release 4.1.190.5

Details for upgrading your network to Release 4.1.190.5 from earlier releases of 3.1, 3.2, 4.0 and 4.1 are described below.

- If your controller is installed with release 4.0.2xx software, you must upgrade to a version of release 4.1 (4.1.171.0, 4.1.185.0 or later) prior to upgrading to Release 4.1.190.5.
- If your controller is installed with release 4.0.1.xx or 3.2.xx, you must upgrade with two intermediate releases prior to installing Release 4.1.190.5.
  - First, upgrade to 4.0.217.0
  - Secondly, upgrade to 4.1.18x.x
  - Thirdly, upgrade to Release 4.1.190.5
- If your controller is installed with release 3.1.x, you must upgrade with three intermediate releases prior to installing Release 4.1.190.5.
  - First, upgrade to 3.2.195.10
  - Secondly, upgrade to 4.0.217.0
  - Thirdly, upgrade to 4.1.18x.0
  - Fourthly, upgrade to Release 4.1.190.5

Mandatory Boot Variable Update for Networks with 1520s

If your network is operating with 1520s or you plan to install 1520s in your network, you must set the boot variable on the 1520 BEFORE upgrading from release 4.1.190.5 to 4.1.191.24M (or greater mesh release). Updating the boot variable ensures the 1520 joins correctly.

Note You should check the boot variable setting before updating the boot.

- If the boot system image is visible, then no boot variable update is required.
  - For release 4.1.190.5, the system image should read: flash:/c1520-k9w9-mx.124-3g.JMA1/c1520-k9w9-mx.124-3g.JMA1
- If the boot system image is missing, then you must update the boot variable.

Checking the Boot Variable Setting

To check the setting of the boot variable, do the following:

Step 1 On the controller, enter the following commands for each mesh access point (MAP):

debug ap enable *AP_Name*

debug ap command "more flash:/env_vars" *Cisco_AP*

A display similar to the following appears:

```
Tue Jan 15 00:00:15 2009: SLT-HCAB-MAP-01-fe.bb.6f: 5G_RADIO_CARRIER_SET=0020
Tue Jan 15 00:00:15 2009: SLT-HCAB-MAP-01-fe.bb.6f: 5G_RADIO_ENCRYPTION_CONFIG=02
Tue Jan 15 00:00:15 2009: SLT-HCAB-MAP-01-fe.bb.6f: 5G_RADIO_MAX_TX_POWER=65535
Tue Jan 15 00:00:15 2009: SLT-HCAB-MAP-01-fe.bb.6f:
BOOT=flash:/c1520-k9w9-mx.124-3g.JMA1/c1520-k9w9-mx.124-3g.JMA1
Tue Jan 15 00:00:15 2009: SLT-HCAB-MAP-01-fe.bb.6f: DEFAULT_ROUTER=11.200.9.20
Tue Jan 15 00:00:15 2009: SLT-HCAB-MAP-01-fe.bb.6f: DEVIATION_NUM=0
Tue Jan 15 00:00:15 2009: SLT-HCAB-MAP-01-fe.bb.6f: DOT11G_RADIO_MODE=255
Tue Jan 15 00:00:15 2009: SLT-HCAB-MAP-01-fe.bb.6f: DOT11_DEVICE_TYPE=4C
Tue Jan 15 00:00:15 2009: SLT-HCAB-MAP-01-fe.bb.6f: DOT11_ENCRYPTION_CONFIG=02
Tue Jan 15 00:00:15 2009: SLT-HCAB-MAP-01-fe.bb.6f: DOT11_MAX_ASSOCIATION_NUM=2007
Tue Jan 15 00:00:15 2009: SLT-HCAB-MAP-01-fe.bb.6f: ENABLE_BREAK=yes
Tue Jan 15 00:00:15 2009: SLT-HCAB-MAP-01-fe.bb.6f: FAB_PART_NUM=800-28909-02
Tue Jan 15 00:00:15 2009: SLT-HCAB-MAP-01-fe.bb.6f: IP_ADDR=11.200.9.99
Tue Jan 15 00:00:15 2009: SLT-HCAB-MAP-01-fe.bb.6f: MAC_ADDR=00:1d:e5:e8:aa:00
Tue Jan 15 00:00:15 2009: SLT-HCAB-MAP-01-fe.bb.6f: MAC_ADDR_BLOCK_SIZE=256
Tue Jan 15 00:00:15 2009: SLT-HCAB-MAP-01-fe.bb.6f: MANUAL_BOOT=no
Tue Jan 15 00:00:15 2009: SLT-HCAB-MAP-01-fe.bb.6f: NETMASK=255.255.0.0
Tue Jan 15 00:00:15 2009: SLT-HCAB-MAP-01-fe.bb.6f: NEW_IMAGE=yes
Tue Jan 15 00:00:15 2009: SLT-HCAB-MAP-01-fe.bb.6f: PCA_ASSY_NUM_800=03 20 00 70 ED 02
Tue Jan 15 00:00:15 2009: SLT-HCAB-MAP-01-fe.bb.6f: PCA_PART_NUM_73=49 2A A6 02
Tue Jan 15 00:00:15 2009: SLT-HCAB-MAP-01-fe.bb.6f: PCA_REVISION_NUM=A0
Tue Jan 15 00:00:15 2009: SLT-HCAB-MAP-01-fe.bb.6f: PCA_REVISION_NUM_800=A0
Tue Jan 15 00:00:15 2009: SLT-HCAB-MAP-01-fe.bb.6f: PCB_SERIAL_NUM=FHH1101007F
Tue Jan 15 00:00:15 2009: SLT-HCAB-MAP-01-fe.bb.6f: PEP_PRODUCT_ID=AIR-LAP1521AG-A-K9
Tue Jan 15 00:00:15 2009: SLT-HCAB-MAP-01-fe.bb.6f: PEP_VERSION_ID=V01
Tue Jan 15 00:00:15 2009: SLT-HCAB-MAP-01-fe.bb.6f: PRODUCT_MODEL_NUM=AIR-LAP1521AG-A-K9
Tue Jan 15 00:00:15 2009: SLT-HCAB-MAP-01-fe.bb.6f: RADIO_CARRIER_SET=00FF
Tue Jan 15 00:00:15 2009: SLT-HCAB-MAP-01-fe.bb.6f: RADIO_MAX_TX_POWER=65535
Tue Jan 15 00:00:15 2009: SLT-HCAB-MAP-01-fe.bb.6f: SYSTEM_REVISION_NUM_800=A0
Tue Jan 15 00:00:15 2009: SLT-HCAB-MAP-01-fe.bb.6f: TOP_ASSY_NUM_800=03 20 00 71 22 02
Tue Jan 15 00:00:15 2009: SLT-HCAB-MAP-01-fe.bb.6f: TOP_ASSY_SERIAL_NUM=SJC1101007F
Tue Jan 15 00:00:15 2009: SLT-HCAB-MAP-01-fe.bb.6f: param-any=
```

Step 2 To turn off debug access, enter **debug ap disable** *AP_Name.*

Note You do not need to turn off the debug access at this point if a boot update is required. Continue to the "Updating the Boot Variable" section on page 12.

Updating the Boot Variable

To update the boot variable on a 1520 prior to a software upgrade, do the following:

Step 1 On the controller, enter the following commands for each mesh access point (MAP):

debug ap enable *AP_Name*

debug ap command "debug lwapp con cli" *AP_Name*

debug ap command "test mesh enable telnet" *AP_Name*

show ap config general *AP_Name*

Note Find the IP address for the access point in the **show ap config general** *AP_Name* command and continue to Step 2.

Step 2 Telnet to the access point using the IP address identified in Step 1 by entering the following command:

telnet *IP_address*

Step 3 From the AP console, enter the following:

enable

debug lwapp console cli

show version

Look for the system image as noted in the example below:

```
System image file is "flash:/c1520-k9w9-mx.124-3g.JMA1/c1520-k9w9-mx.124-3g.JMA1"
```

Enter the image name (enclosed within quotes) into the **boot system**... command below.

config term

boot system flash:/c1520-k9w9-mx.124-3g.JMA1/c1520-k9w9-mx.124-3g.JMA1

Note The system image entered in the **boot system** *image-name* command must match the version identified in the **show version** command.

exit

Enter the following command to verify you typed the image string correctly.

more flash:/env_vars *Cisco_AP*

Step 4 Disconnect Telnet.

Important Notes

This section describes information about changes to the controller CLI and GUI, and operational notes for Release 4.1.190.5.

Operational Notes

The following operational notes are relevant to this release.

Battery Charge Information is not Available for AP1510s with Power Supply 1.01d Firmware

An AP1510 with an *Alpha FlexNet MPS30-48C-SL* power supply must have firmware version 1.02d or greater to supply information about its remaining charge to the controller and Cisco WCS. Otherwise, the controller and WCS display incorrect battery information.

To upgrade your power supply to 1.02d (or greater) firmware, return the power supply to an Alpha service center (Argus).

> To arrange return of power supply call or email:

> US and Canada: 1 888 GO ARGUS (462-7487), International: 1 604 436 5547

> Email: support@argusdcpower.com

> For additional Alpha service centers, see:

> http://www.alpha.com/Contacts/Service-Centers/

Monitoring Port LED Status on an AP1520

When physically disconnecting a cable from an AP1520, the port LED associated with that connection might remain lit for up to 3 seconds.

AP1520 Support for Four Gigabit Ethernet Ports

The AP1520 supports four Ethernet interfaces (g0–PoE in, g1–PoE out,g2–Cable, g3–Fiber). Refer to the "Controller GUI and CLI Changes" section on page 13 for details how the CLI and GUI displays are modified to report status on the four Ethernet ports.

Parent Selection Differences Between AP1520 and AP1510

When operating as a MAP, the AP1520 generally prefers to select a parent that shares the same bridge group name (BGN), rather than a wired interface (uplink) to the controller. This approach is different from the AP1510 which always places a higher priority on selecting a parent with a wired connection.

Additionally, when an AP1520 connects to a parent with a default (null) BGN, the AP1520 disables the Ethernet Bridging feature to prevent a potential bridge loop. An AP1510 does not disable Ethernet Bridging.

To ensure smooth operation, configure a bridge group name for the AP1520 and verify that the mesh access point is connecting to a parent on the same bridge group to allow Ethernet bridging.

Controller GUI and CLI Changes

The following changes can be seen in the controller GUI and CLI interfaces.

- The **config mesh linkdata** A*P_Name* command is not supported on the AP1520 (CSCsj73871). It prints out link test statistics for each second and is used to troubleshoot RF links.

AP1520 Support for Four Gigabit Ethernet Ports

The AP1520 supports four Ethernet interfaces: g0–PoE in, g1–PoE out, g2–Cable and g3–Fiber. Both the controller CLI and GUI show the state for each of the four Gigabit Ethernet ports as noted below.

- The **show mesh environment summary** command displays the Up or Down status for four Ethernet interfaces for the AP1520.

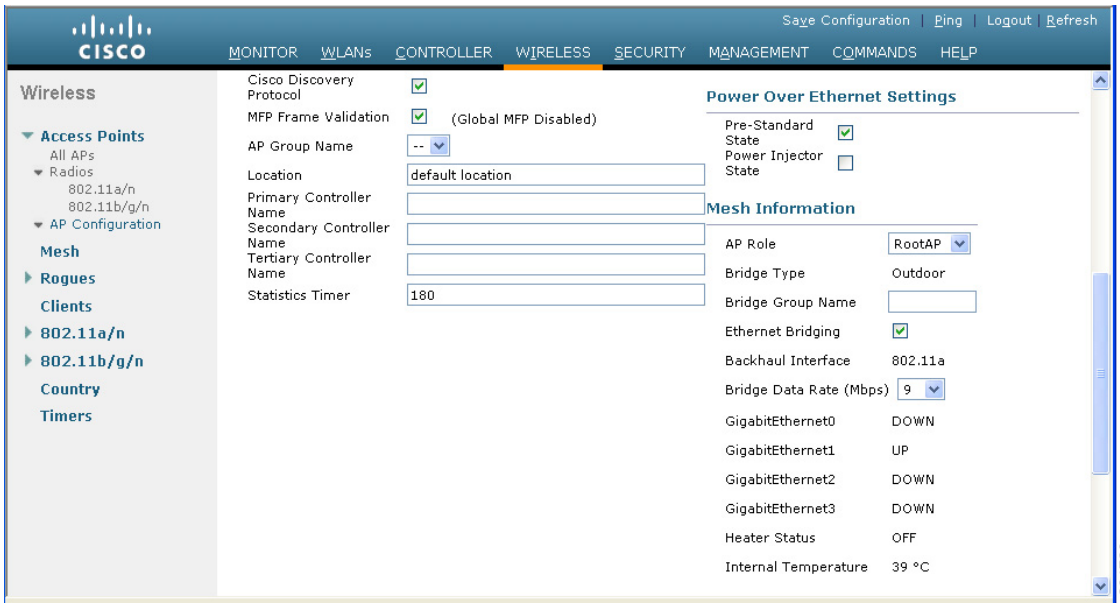
Note

- For the four AP 1520 Ethernet ports, the *Down* state is noted as *Dn*.
- The Up or Down (Dn) status of the four Ethernet ports is reported in the following format: port0:port1:port2:port3. For example, *UpDnDnDn* indicates that port0 is Up and ports 1, 2, and 3 are Down (Dn).
- The AP1510 only reports for one Ethernet port and the Down state is reported as *Down*.

```
(controller)>show mesh env summary
AP Name      Temperature(C/F) Heater Ethernet Battery
--------     ---------------- -------- ------- -------
rap1242.c9ef    N/A             N/A     UP       N/A
rap1522.a380    29/84           OFF     UpDnDnDn N/A
rap1522.4da8    31/87           OFF     UpDnDnDn N/A
map1522.4dcc    28/82           OFF     DnDnDnDn N/A
lap1510.2320    33/91           OFF     DOWN     N/A
map1522.d4af    29/84           OFF     DnDnDnDn N/A
```

- The **Wireless** > *AP Name* > *Details* window displays the state of the four Gigabit Ethernet ports in the Mesh Information section.

Figure 1 Wireless > AP1520 > Details



Caveats

This section lists open, resolved and closed caveats in Release 4.1.190.5.

Open Caveats

The following caveats are open (unresolved) in this release:

- CSCsj48044—In some cases, public safety information might not display accurately in Cisco WCS.

  Workaround: Query the information using the controller GUI or CLI, where applicable.

- CSCsj48049—The Custom options for the TX Power Level Assignment parameter (Configure > Access Point > *Radio)* in Cisco WCS do no reflect the correct dBm values; however, the correct values are resident in the software.

  Workaround: Select the Tx Power Level Assignment based on the values 1 (high) to 5 (low) and ignore the dBm values associated with those numbers.

- CSCsj67716—When AP1520 and AP1510 are operating in the same network, public safety channels for the AP1510 might display (**show mesh neigh summary** *Cisco_AP*) the public safety channel values of 190 or 196 rather than 20 and 26, if the AP1510 is operating with a release earlier than 4.1.181.0. Channels 20 and 26 were adopted for public safety transmissions in release 4.1.181.0. Previous releases use channels 190 and 196 for public safety transmission.

  Workaround: None. This is a display issue only. It is not service affecting.

- CSCsj73871—The **config mesh linkdata** A*P_Name* command which provides link test data is not supported on the AP1520.

  Workaround: None.

- CSCsj77654—The current packet error rate (PER) displayed in Cisco WCS reflects a cumulative value for control and data packets rather than distinct values.

  Workaround: None.

- CSCsj95524–In some cases, a higher than expected number of parent exclusion events might be generated during an extended join period for an AP1520.

  Workaround: Verify that the Bridge Group Name (BGN) for the AP1520 joining the network is properly configured to limit the number of potential parents.

- CSCsk07157–When operating as a MAP, the AP1520 generally prefers to select a parent that shares the same bridge group name (BGN), rather than a wired interface (uplink) to the controller. This approach is different from the AP1510 which always places a higher priority on selecting a parent with a wired connection.

  Additionally, when an AP1520 connects to a parent with a default (null) BGN, the AP1520 disables the Ethernet Bridging feature to prevent a potential bridge loop. This behavior also differs from that of the AP1510.

  Workaround: Configure a bridge group name for the AP1520 and verify that its parent is on the same bridge group to allow Ethernet Bridging.

- CSCsk07319–The txpkts rate for the neighboring mesh node always displays a value of 5000 in the text of the **show mesh adjacency all** command for the AP1520.

  Workaround: None.

- CSCsk08657–In the controller GUI, entry of an antenna gain greater than the highest allowed antenna gain threshold value is allowed with no resulting error message.

  Workaround: Verify that the entered antenna gain is within the FCC limit.

- CSCsk32623–When Bridge Group Names (BGN) are not employed in a mesh network, access points might flap between the Ethernet and 802.11a backhaul uplinks.

  Workaround: Always configure and use Bridge Group Names in the network.

- CSCsl70218–The BOOT bootloader environment variable is not set on some early shipments of 1520 mesh access points. Any image download that fails during upgrade might cause a partial image to be written on the1520. Without the BOOT variable, the bootloader might attempt to boot the partial image rather than the original complete image, causing the 1520 to get stuck and not join the controller.

  This is seen when a controller is upgraded from mesh release 4.1.190.5 to 4.1.191.24M and the 1520 has a wireless connection to the controller. It might also happen when a controller is upgraded from 4.1.190.5 to other future mesh releases.

  Workaround: To recover from an incomplete 1520 boot up due to a 4.1.190.5 to 4.1.191.24M upgrade, enter the following bootloader commands in the AP console:

  ```
  delete flash:/update/c1520-k9w9-mx.124-3g.JMB/c1520-k9w9-mx.124-3g.JMB
  set BOOT flash:/c1520-k9w9-mx.124-3g.JMA/c1520-k9w9-mx.124-3g.JMA
  boot
  ```

  To verify the configuration, enter

  ```
  set
  ```

  Note For details on connecting to the AP console, refer to the "Connecting to the Access Point Locally" section of the *Cisco Aironet 1520 Series Outdoor Mesh Access Point Hardware Installation Guide* found at: http://www.cisco.com/en/US/docs/wireless/access_point/1520/installation/guide/1520_ch3.html#wp1099247

  Note To prevent the 1520 boot up problem, a change in the boot variable must be made prior to 4.1.190.5 from a compatible non-mesh release or any upgrade from 4.1.190.5 to 4.1.191.24M (or greater mesh release). Refer to the "Mandatory Boot Variable Update for Networks with 1520s" section on page 10 for configuration details.

Closed Caveats

- CSCsj70714–When an AP 1520 radio was trying to back off to send a beacon, it did not acknowledge (ACK) receipt of a packet. This condition could cause an increase in packet retry events when a large size packet was sent at low rate.

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:

http://tools.cisco.com/Support/BugToolKit/

(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, refer to the Cisco TAC website at:

http://www.cisco.com/tac

Click **Troubleshooting.** Then choose your product and then select the **Troubleshoot and Alerts** heading on the product page to find information on the problem you are experiencing and other service advisories.

For additional suggestions on troubleshooting mesh networks, refer to the *Troubleshooting Mesh Networks* document at the following Cisco.com URL:

http://www.cisco.com/en/US/products/ps6548/prod_troubleshooting_guides_list.html

Related Documentation

The following documents are related to mesh networks:

- *Cisco Aironet 1500 Series Outdoor Mesh Access Point Hardware Installation Guide*
- *Cisco Aironet 1520 Series Outdoor Mesh Access Point Hardware Installation Guide*
- *Cisco Aironet 1520 Series Outdoor Mesh Access Point Getting Started Guide*
- *Cisco Aironet Series Power Injector Installation Instructions*
- *Cisco Aironet Series 1500 Access Point LED Indicator Installation Instructions*
- *Cisco Aironet 8-dBi Omnidirectional Antenna (AIR-ANT5180V-N)*
- *Cisco Aironet 5-dBi Omnidirectional Antenna (AIR-ANT2450V-N)*
- *Cisco Wireless LAN Controller Configuration Guide*
- *Cisco Wireless LAN Controller Command Reference*
- *Cisco Wireless Control System Configuration Guide*
- *Troubleshooting a Mesh Network*

Note You can view the latest online versions of these documents at the following link: http://www.cisco.com/en/US/products/hw/wireless/tsd_products_support_category_home.html

Obtaining Documentation, Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, 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/en/US/docs/general/whatsnew/whatsnew.html

---

This document is to be used in conjunction with the documents listed in the Related Documents section.

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