Release Notes for Cisco 526 Wireless Express Mobility Controllers and Cisco 521 Wireless Express Lightweight Access Points, 5.2.157.0

December, 2008

These release notes provide an overview, important notes, and caveats software release 5.2.157.0 for Cisco 526 Wireless Express Mobility Controllers and Cisco 521 Wireless Express Access Points, which comprise part of the Cisco Smart Business Communications System. These components are part of Cisco's Wireless Mobility Express Release 1.8.

Contents

These release notes contain the following sections.

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

Overview

The Cisco 526 Wireless Express Mobility Controller and the Cisco 521 Wireless Express Access Point are components of the Cisco Smart Business Communications System. The 526 controller is a network appliance designed to optimize the wireless network of small and medium-sized businesses. Each controller can be used with up to 12 controller-based 521 access points, and up to two controllers are supported per mobility group. The 526 controller provides:

- A cost-effective solution for small and medium-sized business environments
- Standards-based enterprise-class security
- Simplified network deployment and management with automated radio resource features
- Centralized management with the Cisco Configuration Assistant (CCA)
- Advanced mobility services readiness to support secure guest access and optimized voice-over Wi-Fi

The 521 access point is a single-band 802.11g access point that features business-class management, security, and scalability. It offers high performance wireless connectivity in offices and similar environments. The 521 access point is available in two configurations:

- **Controller-based mode**—These 521 access points are connected to the wired infrastructure through a 526 controller. Controller-based 521 access points are also known as *lightweight access points* or *LAPs* because configuration and management are performed through a single interface.
- **Standalone mode**—These 521 access points are directly connected to the wired infrastructure. Standalone 521 access points are also known as *autonomous access points* because configuration and management are performed locally at the individual access point level.

Note This document applies to the 521 controller-based access points. Refer to the *Release Notes for Cisco 521 Wireless Express Standalone Access Point for Cisco IOS Release 12.4(xx)yy* for information on the 521 standalone access points.

The 526 controller and 521 access point work in concert with the Cisco Configuration Assistant (CCA) to provide you with the visibility and centralized control you need to optimize network performance. The CCA is graphical user interface (GUI)-based software that you install on a Windows-based PC. It allows you to configure and manage all the components of the Cisco Smart Business Communications System.

New Features in This Release

The following new features are supported in the Wireless Express 5.2.157.0 release:

- **Managed access points**—The number of supported controller-managed Cisco 521 wireless access points increased from 6 to 12 per controller. Up to 24 total LAPs are supported in a dual-controller configuration.
- **Autonomous access points**—The number of supported autonomous Cisco 521 wireless access points increased from 3 to 10.

Cisco 526 Controller GUI Features

The following new features have been added to the Cisco 526 controller GUI since the 4.2.61.8 release:

- **Country Homologation List**—You can now specify a country of operation (such as FR for France or ES for Spain) for each controller. Configuring a country code ensures that each radio's broadcast frequency bands, interfaces, channels, and transmit power levels comply with country-specific regulations.

  The menu path from the controller GUI Home page is **Wireless** > **Country**.

- **802.11 Authentication Response Timeout**—You can now set the duration the controller attempts to authenticate an access point before it times out.

  The menu path from the controller GUI Home page is **Wireless** > **Timers**.

- **Delivery Traffic Indication Map (DTIM) settings**—You can now configure the DTIM value for buffered broadcast and multicast messages. In 802.11a/n and 802.11b/g/n networks, lightweight access points broadcast a beacon at regular intervals specified by the Delivery Traffic Indication Map (DTIM). After the access point broadcasts the beacon, it transmits any buffered broadcast and multicast frames based on the value set for the DTIM period. This feature allows power-saving clients to wake up at the appropriate time if they are expecting broadcast or multicast data.

  The menu path from the controller GUI Home page is **WLANs** > **Edit** > **Advanced.**

- **Local Extensible Authentication Protocol (EAP)**—You can now use local EAP to allow wireless clients to be authenticated locally. It is designed for use in remote offices that want to maintain connectivity to wireless clients when the backend system becomes disrupted or the external authentication server goes down. When you enable local EAP, the controller serves as the authentication server and the local user database, thereby removing dependence on an external authentication server.

  The menu path from the controller GUI Home page is **Security** > **Local EAP**.

- **Internal Dynamic Host Configuration Protocol (DHCP) server**—The controller now contains an internal DHCP server. This server is typically used in branch offices that do not already have a DHCP server, that contain 10 access points or fewer, and that have their access points on the same IP subnet as the controller. Only lightweight access points are supported. When you want to use the internal DHCP server, you must set the management interface IP address of the controller as the DHCP server.

  The menu path from the controller GUI Home page is **Controller** > **Internal DHCP Server**.

Wireless Protection Policies

- **Rogue policies**—You can now set policies and exclusions to to monitor, control, and protect your network from rogue attacks.

  A rogue device is an unknown access point or client that is detected by managed access points in your network as not belonging to your system. Rogue access points can disrupt wireless LAN operations by posing as legitimate clients and using plain-text or other denial-of-service or man-in-the-middle attacks. That is, a hacker can use a rogue access point to capture sensitive information, such as usernames and passwords. Because rogue access points are inexpensive and readily available, employees sometimes plug unauthorized rogue access points into existing LANs and build ad hoc wireless networks without IT department knowledge or consent. These rogue access points can be a serious breach of network security because they can be plugged into a network port behind the corporate firewall.

The menu path from the controller GUI Home page is **Security** > **Wireless Protection Policies** > **Rogue Policies.**

- **Management Frame Protection (MFP)**—Management frame protection (MFP) provides security for the otherwise unprotected and unencrypted 802.11 management messages passed between access points and clients. The controller supports infrastructure MFP.

  The menu path from the controller GUI Home page is **Security** > **Wireless Protection Policies** > **Management Frame Protection**.

- **Intrusion Detection System (IDS)**—You can now use the Cisco intrusion detection system/intrusion prevention system (CIDS/IPS) to instruct a WE526 controller to prevent certain clients from accessing the wireless network when attacks involving these clients are detected at Layer 3 through Layer 7. This system offers significant network protection by helping to detect, classify, and stop threats including worms, spyware/adware, network viruses, and application abuse.

  The menu path from the controller GUI Home page is **Security** > **Wireless Protection Policies** > **Client Exclusion Policies** and **Security** > **Wireless Protection Policies** > **Standard Signatures**.

Software Release Information

Mobility Express Release 1.8 comprises several software components. These are factory-installed on your controller and access points.

Make sure you have all the latest software components:

- Controller software release 5.2.157.0
- Cisco IOS Release 12.4(10b)JA
- Cisco Configuration Assistant 1.8

If you are a registered user, you can download the latest versions from cisco.com at the following URL:

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

Note To avoid possible problems and to take advantage of the new features of Mobility Express Release 1.8, Cisco recommends that you make sure you have the latest versions of the software listed above.

Note The 5.2.157.0 release does not support the NM-AIR-WLC6 platform.

Registering at Cisco.com

If you are not a registered user, follow these steps to register:

Step 1 Open your browser and browse to the following URL:

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

Step 2 The Cisco.com Registration page appears.

Step 3 Complete the information requested on the page.

Step 4 Click **Submit**.

Additional information about registering is available on cisco.com at the following URL:

http://www.cisco.com/en/US/applicat/cdcrgstr/applications_overview.html

Installation Notes

This section contains important information for installing 526 controllers and 521 access points.

Warnings

This section provides safety warnings for the 526 controller and 521 access point. For translations of these safety warnings, refer to the translated safety warnings document at these URLs:

http://www.cisco.com/en/US/docs/wireless/controller/4400/warnings/reference/guide/440warn.html

http://www.cisco.com/en/US/docs/wireless/access_point/warnings/reference/guide/ap_warn1.html

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.** Statement 1071

These warnings apply to the 526 controller:

Warning **There is the danger of explosion if the battery is replaced incorrectly. Replace the battery only with the same or equivalent type recommended by the manufacturer. Dispose of used batteries according to the manufacturer's instructions.** Statement 1015

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 **Ultimate disposal of this product should be handled according to all national laws and regulations.** Statement 1040

These warnings apply to the 521 access point:

Warning **This product must be connected to a Power-over-Ethernet (PoE) IEEE 802.3af compliant power source or an IEC60950 compliant limited power source.** Statement 353

Warning **In order to comply with FCC radio frequency (RF) exposure limits, antennas should be located a minimum of 7.9 in. (20 cm) or more from the body of all persons.** Statement 332

⚠ Warning **Do not operate your wireless network device near unshielded blasting caps or in an explosive environment unless the device has been modified to be especially qualified for such use.** Statement 245B

⚠ Warning **Do not work on the system or connect or disconnect cables during periods of lightning activity.** Statement 1001

⚠ Warning **Read the installation instructions before you connect the system to its power source.** Statement 1004

⚠ Warning **This product relies on the building's installation for short-circuit (overcurrent) protection. Ensure that the protective device is rated not greater than 20A.** Statement 1005

Safety Information

Follow the guidelines in this section to ensure proper operation and safe use of 526 controllers and 521 access points.

FCC Safety Compliance Statements

526 Controller and 521 Access Point

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving radio or TV antenna.
- Increase the separation between the Cisco equipment and a radio or TV receiver.
- Connect the Cisco equipment to an outlet on a circuit different from that to which the radio or TV receiver is connected.
- Consult an experienced radio/TV technician for help in resolving interference problems to a radio or TV receiver.

521 Access Point

The FCC, 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. Cisco 521 access points 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 document and the installation and configuration guides will result in user exposure substantially below the FCC recommended limits.

- Do not hold any component containing a radio such that the antenna is very close to or touching any exposed parts of the body, especially the face or eyes, while transmitting.
- The use of wireless devices in hazardous locations is limited to the constraints posed by the safety directors of such environments.

Safety Considerations

- Verify that the ambient temperature remains between 32 to 104° F (0 to 40° C), taking into account the elevated temperatures when installed in a rack or enclosed space.
- When multiple 526 controllers are mounted in an equipment rack, be sure that the power source is sufficiently rated to safely run all the equipment in the rack (input: 100–240 VAC, 50/60 Hz; output: 48 VDC, 2.08 A per controller).
- Verify the integrity of the electrical ground before installing the 526 controller.

Installation Instructions

Refer to the appropriate quick start 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.

Important Notes

This section describes important information about the 526 controllers and 521 access points.

Configuring the 526 Controller through the Controller GUI

In addition to configuring the 526 controller through the CCA, you can also configure it by browsing to the controller GUI. Instructions for configuring the 526 controller through the GUI are provided in the *Cisco 500 Series Wireless Express Mobility Controller Configuration Guide*.

Note Configuring the controller using the controller GUI requires that someone who is familiar with the 526 controller GUI and the controller functions.

Note The controller GUI requires the following operating system and web browser: Windows XP SP1 or higher or Windows 2000 SP4 or higher and Internet Explorer 6.0 SP1 or higher, respectively.

Establishing Wireless Connectivity

Follow these guidelines to ensure that the 526 controller and 521 access point can establish wireless connectivity.

- When a 526 controller and 521 access point are connected to a Cisco Catalyst Express 500 Series Switch or Cisco Unified Communications 500 Series Switch managed by the CCA and you use the CCA's Configure tab to select Smartports, you can have the CCA suggest a role for the ports to which the controller and access point are connected. The recommended role for the controller and access point is the Access Point Smartport Role. The CCA also suggests a default VLAN of 1. If you apply the suggested Smartport role, the native VLAN should be set to 1 on all ports connecting to the controller and access point.
- The 526 controller's management and ap-manager interfaces are set by default to the untagged VLAN (or VLAN 0) and it is recommended that VLAN 0 not be changed. The IP addresses for these two interfaces must belong to the subnet associated with this untagged VLAN, and the default SSID created from the controller configuration wizard is associated to this untagged VLAN. You can create dynamic interfaces using any other VLAN (from 2 to 1000) and associate this VLAN to the new SSID, but this VLAN should be different from the native VLAN on the connected port. For example, if you create a dynamic interface using VLAN 25, then you can associate this VLAN to the new SSID.

Converting an Autonomous AP521 Using the CCA

When an autonomous AP521 access point is converted to controller-mode operation using the CCA, the access point properties screen continues to indicate that the access point is an AIR-AP521G-A-K9 after the conversion. This is in agreement with the product label on the access point. However, the CCA displays a small triangle icon next to the converted access point to indicate that the access point is now operating as a controller-mode access point.

Note The CCA conversion process is one-way. Once the conversion takes place, you cannot restore the access point to autonomous operation using CCA.

Caveats

This section lists open caveats for components of the Cisco Smart Business Communications System.

Open Caveats

These caveats are open in this release:

- **CSCsi32505**—The controller CLI does not allow the user to set the controller prompt name.

  Workaround: None.
- **CSCsm22318**—After converting an autonomous access point to controller management using CCA, the device type display does not reflect the change.

  For more information, see the "Converting an Autonomous AP521 Using the CCA" section on page 8

These caveats are open in CCA release 1.8 and affect controller manageability.

- **CSCsh99313**—CCA is using same username and password to access multiple devices.

  A controller with read-only privileges can be added to a read-write community and a controller with read-write privileges can be added to a read-only community. This problem occurs when you add the same username and password pair as read-only for one controller and as read-write for another controller. As a result, the CCA discovers both controllers even though the privilege level of one of them does not match the privilege level of the community. When you manage the read-write community, you can configure the controller with the read-only privilege, but the controller rejects the operation because of insufficient privilege.

  Workaround: Set the same privilege level when configuring one username and password pair for different controllers. Also, provide the read-write username and password pair during controller discovery for the read-write community and provide the read-only username and password pair during controller discovery for the read-only community.

- **CSCsi51896**—The x-launch does not open the window for the desired device.

  When you have more than one controller and you configure controller settings such as SSID, RADIUS servers, interfaces, VLANs, and so on, the selected controller is not carried over from one window to another window.

  Workaround: Be sure to select the correct controller from the Hostname list.

- **CSCsj31198**—When creating a community to discover network devices, the authentication dialog displays only the IP addresses of the devices and not the device types. This situation makes it difficult to provide the correct username and password for each device.

  Workaround: Have a list of device types, their IP addresses, and authorization information available when creating new communities.

Resolved Caveats

This caveat is resolved in this release:

- **CSCsk76218**—It is no longer possible to download the controller configuration file without the encryption key.

Closed Caveats

This caveat was closed in this release:

- CSCsi22823—Undersized frame error on the port connected to wireless LAN controller.

  The following error message may appear on the Cisco Catalyst Express 500 Series Switches (CE500): “Fa10: Detected undersize frames generated by the connected device.” However, there is no impact to controller functionality.

  Workaround: Disconnect the connected device.

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.)

Obtaining Documentation, Obtaining 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