Release Notes for the Cisco WAP200 Wireless-G Access Point with PoE and RangeBooster Version 2.0.6.0

January 2013

These release notes describe caveats for the Cisco WAP200 Wireless-G Access Point with PoE and RangeBooster firmware versions. These release notes are updated as needed to describe memory requirements, hardware support, software platform deferrals, microcode or modem code changes, related document changes, and any other changes that are not documented elsewhere.

Contents

New and Changed Information

This version of the release notes contains caveat information for the following software versions:

- 2.0.6.0
- 2.0.4.0
- 2.0.2.4
- 2.0.1.3
- 1.0.22

- 1.0.20
- 1.0.14

Caveats

Caveats describe unexpected behavior or defects in the Cisco software releases. This section contains caveats for the following releases:

- **Open Caveats in Release 2.0.6.0**
- **Resolved Caveats in Release 2.0.6.0**
- **Open Caveats in Release 2.0.4.0**
- **Resolved Caveat in Release 2.0.4.0**
- **Open Caveats in Release 2.0.2.4**
- **Resolved Caveats in Release 2.0.2.4**
- **Open Caveats in Release 2.0.1.3**
- **Resolved Caveats in Release 2.0.1.3**
- **Open Caveats in Release 1.0.22**
- **Resolved Caveats in Release 1.0.22**
- **Open Caveats in Release 1.0.20**
- **Resolved Caveats in Release 1.0.20**
- **Open Caveats in Release 1.0.14**

NOTE If you are upgrading firmware from Version 1.0.14 to Version 1.0.22, it is recommended that you use Internet Explorer 6.0 or Firefox 2.0. If you are using Internet Explorer 7.0 or a later release, it cannot redirect back to its original window after firmware upgrade or device reboot.

Open Caveats in Release 2.0.6.0

- None.

Resolved Caveats in Release 2.0.6.0

- CSCue12148—Added security enhancements for product stability.
- CSCud05594—Fixed issue with mandatory secondary DNS. You can now enter 0.0.0.0 in the secondary static DNS field if no secondary DNS exists.

Open Caveats in Release 2.0.4.0

- The current Administration Guide is not fully compliant with the GUI for this release.
- HTTPS certificate is expired (SSL certificate can be imported and exported using the GUI).

Resolved Caveat in Release 2.0.4.0

- Spanning Tree Protocol (STP) Setup can now be configured in the Basic Setup page.

Open Caveats in Release 2.0.2.4

- An erroneous SNMP inform/trap “SNMPv2-MIB:warmStart inform:SNMPv2c...” and “SNMP2-MIB:warmStart trap:SNMPv2c...” is sent when the WAP200 device renews its IP address upon DHCP expiration as set on the router. This will cause the SNMP daemon to restart. To continue to use the uninterrupted SNMP feature, increase the router’s DHCP expiration timer. Currently, this happens at half the DHCP expiration timer value. For example, if you want to use uninterrupted SNMP for 12 hrs, please set this timer to 24 hrs.
- It is recommended to use either Internet Explorer 7 or later, or Firefox 3.0 or later as your internet browser. Google Chrome is not a fully supported browser. When using Google Chrome, the SSL Certificate extension downloads as "wap200.download." This is an invalid extension and needs to be changed to a “.crt” extension.

Resolved Caveats in Release 2.0.2.4

- When the user chooses another AP mode then returns to the original mode, the MAC fields will be reset.
- When the **Set Bandwidth Utilization Threshold** is set to 1, it will cause a wireless client to be unassociated with the WAP200 device.
- Fixed GUI issues.
- SSL certificate can now be easily imported and exported using the GUI; effective starting with this release.

Open Caveats in Release 2.0.1.3

- The **Content Area** window size will be readjusted after resizing the Internet Explorer 7.0 web browser window.
- HTTPS certificate is expired.
- In the **Basic Wireless Settings** window, when the user adds and modifies multiple SSID names and saves settings, it will take about 7-10 seconds to refresh between windows.

Resolved Caveats in Release 2.0.1.3

This section contains caveat information for the following technologies:

GUI

- The access point's web-based configuration utility has a new user interface based on the Cisco Small Business style.

Time

- Time zones that had been displaying incorrect times, some as the result of in the daylight saving time (DST) errors, now display the correct time.
- When using the Microsoft Vista operating system, the Tbilisi and Tehran time zones were not accurate. This has been corrected by Microsoft. Please refer to the Microsoft article "August 2007 cumulative time zone update for Microsoft Windows operating systems'" at http://support.microsoft.com/kb/933360
- The **Current Time** now includes the number of seconds.

Sendmail

- The time threshold is changed from 600 to 86400 seconds.
- Enabling an E-mail alert is not required to enable the syslog buffer.
- The log message that indicates when a client is unable to connect to a mail server is changed.

Wireless

- **WEP key** fields support all ASCII characters with the exception of the semicolon (;).
- Cell phone roaming is supported.
- The **Client MAC table timeout** parameter has been increased from 5 minutes to 65 minutes.
- The **association timeout** parameter has been increased to 65 minutes.

Load Balancing

- The **loadbalance** statement under class map **B** has been corrected.
- The **Add Bandwidth Utilization** parameter on the **Status > Wireless** window has been corrected.
- The **Load Balancing** parameter on the **Wireless > Advanced Wireless Settings** window has been corrected.

Miscellaneous

- After they have expired, DHCP clients can renew their IP address leases.
- A redirect error that occurred after the device firmware is upgraded has been corrected.
- Users can no longer login without a username and a password after Internet Explorer 6.0 or Internet Explorer 7.0 time out.

Open Caveats in Release 1.0.22

- When the **Wireless Web Access** parameter is set to **disabled**, WLAN clients that are not hosted on the AP Management VLAN are still able to access the Web User interface.
- The **Device Name** parameters on the **SNMP** window and the **Basic Setup** window are not synchronized. The parameter on the Basic Setup cannot be modified by using SNMP.
- While enabling SNMPv3, a user is required to enter the *Get Community*, *Set Community*, and *SNMP Trap-Community* strings. These fields should be grayed out.

Resolved Caveats in Release 1.0.22

- The TCP checksum error that resulted in HTTP session failure when the device was in Repeater or Bridge mode has been corrected.
- WPA-Personal encryption mode error that occurred when the device was in Repeater or Bridge mode has been corrected.
- The device MAC address cannot be overwritten with a default value when SNMP is enabled.
- Unscheduled Automatic Power Save Delivery (U-APSD) errors have been corrected.
- When Repeater mode is configured, wireless isolation is automatically disabled on first SSID.
- WEP encryption now includes ASCII mode support.

Open Caveats in Release 1.0.20

- A WDS Bridge can cause TCP checksum errors on some packets and that might result in HTTP session failures.
- When the **Wireless Web Access** parameter is set to **disabled**, WLAN clients that are not hosted on the AP Management VLAN are still able to access the Web User interface.

Resolved Caveats in Release 1.0.20

- PING floods are no longer observed when multiple access points configured with multiple BSSIDs have been up and running for two or more days.
- When more than two SSIDs are configured, some client cards might exhibit difficulty connecting to an access point.
- When a non-management VLAN is configured, remote management of an access point cannot be accomplished.
- A VLAN filter was added to drop traffic from VLANs that are not mapped to the SSID.

Open Caveats in Release 1.0.14

- When more than two SSIDs are configured, some client cards might exhibit difficulty connecting to an access point. To resolve this issue, reduce the number of SSIDs configured on the access point.

Related Information

Support	
Cisco Small Business Support Community	www.cisco.com/go/smallbizsupport
Online Technical Support and Documentation (Login Required)	www.cisco.com/support
Phone Support Contacts	www.cisco.com/en/US/support/tsd_cisco_small_business_support_center_contacts.html
Software Downloads (Login Required)	Go to tools.cisco.com/support/downloads, and enter the model number in the Software Search box.
Product Documentation	
Cisco WAP200 Access Point	www.cisco.com/en/US/products/ps10048/index.html
Cisco Small Business	
Cisco Partner Central for Small Business (Partner Login Required)	www.cisco.com/web/partners/sell/smb
Cisco Small Business Home	www.cisco.com/smb
Marketplace	www.cisco.com/go/marketplace

78-21113-01 (formerly OL-19150-02)