Release Notes for the Cisco WAP4400N Wireless-N Access Point with PoE

February, 2009

OL-18984-02

These release notes describe caveats for the Cisco WAP4400N Wireless-N Access Point with PoE 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 information for version 1.2.17, version 1.2.14, and version 1.2.11.

Limitations and Restrictions

If you are upgrading firmware from Version 1.2.11 to Version 1.2.14, 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 page after firmware upgrade or device reboot.

Caveats

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

Resolved Caveats in Release 1.2.17

This sections contains caveat information for the following technologies:

GUI

- Interoperability Mode (IOT) mode is removed.

- When using Internet Explorer version 7.0, the user interface cannot redirect the browser back to the index page after a firmware upgrade.

- The **Security monitor account** field does not accept the colon (:) character.

Security

- In Security WPA Modes, users can not associate to an access point (AP) when the AP is configured to use WPA2-Mixed modes and the client is configured to use WPA-AES.

SNMP

- The AP object identifier (OID) is changed to 3955.6.32.4000.1.

- The SNMPv3 security issue is resolved.

- If the ro-community and rw-community strings are the same, use the rw-community.

Sendmail

- The time threshold is changed from 600 to 86400 seconds.

- The log message that indicates when a client is unable to connect to a mail server is changed.

Wireless

- The WEP key supports ASCII characters.

- Attempts by a 802.11b client to associate with an AP set to N only mode are rejected.

- Errors experienced when an AP receives a python script edited by the user have been corrected.

- The wireless driver is changed to align with Draft 2.0.

Miscellaneous

- Errors in the daylight saving time (DST) for the Jerusalem time zone have been corrected.

- When the AP is running DHCP, the udhcpc daemon does keep alive.

Resolved Caveats in Release 1.2.14

This sections contains caveat information for the following technologies:

All issues have been resolved, unless indicated otherwise.

GUI

- The Channel Bandwidth default is changed to 20MHz from auto on the Advanced Wireless Settings page.

- Do not check any field if ACL is disabled.

- The word **W** is not correct on Wireless Security page, the others **W** is correct.

- Changed the SNMP behavior on GUI:

  - Get Community and Set Community fields are grayed out in a SNMPv3 configuration.

  - SNMP v.3 Username, Authentication Password, and Privacy Password fields are grayed out in SNMP v1 and v2 configurations.

  - Modified the description of Trusted Host and SNMP Trap-Destination on the Help page.

  - SNMP Trusted Host and SNMP Trap-Destination can be set to 0.0.0.0.

  - The Device Name on the **Basic Setup** page and the **Management** page are synchronized with the sysName of MIB Browser.

- The user is not allowed to enter a colon (:) in the user name field on Management page.

- When a user enters an invalid character, such as a backslash ("\"), in Host Name and Device Name fields on the **Basic Setup** page the application does not terminate abnormally.

- **Basic Setup Time Zone** GMT+06:00 Rangoon is GMT+06:30.

- The hardware version is changed from Rev.01 to 1.0.

HTTPD

- Users can no longer login without a username and a password after timeout.

- The error dialog that displayed an unknown IP address when trying to connect to the AP, no longer shows the incorrect IP address.

Wireless

- Site survey no longer shows an incorrect SSID after changing the SSID to **vetgat**.

- Wireless Connection Control no longer prevents users from being able to set the same MAC. This issue was also seen in the GUI.

- WEP 64/128 bit can no longer connect with the WAP4400N open system when the WAP4400N setting shared key is activated.

- WEP 128 bit: Gray out is no longer seen in non-default Transmit Key fields.

Miscellaneous

- Authorized Login and unAuthorized Login log messages (syslog) are added.

- SNMP does work after the user clicks **Save Setting** twice on the **Management** page.

- Fixed the TCP checksum error.

- Packets shorter than 64 bytes are prevented.

Resolved Caveats in Release 1.2.11

- 802.11n interoperability with Linksys WPC300N (& WMP300N) on WPA2 is resolved. We recommend that you download the latest driver for the WPC300N (v4.100.15.5). If using Microsoft Windows XP zero config for WPA2, download the Microsoft Windows hotfix KB893357.