Cisco Small Business AP541N Access Point Release Notes for Versions 1.7.2 through 2.0.4

October 2012

78-19182-09

Upgrading the Firmware

We recommended that you backup the device configuration to a file on another device before upgrading the firmware.

If you upgraded from firmware version 1.7.2 to 1.8.0, 1.9.0, 1.9.1, 1.9.2, 2.0.0, 2.0.1, or 2.0.2 you *must* reset the device to factory defaults by pressing and holding the **Reset** button for 10 seconds or more. You should *manually* reconfigure the device for your network. If you reload the configuration file created by using firmware version 1.7.2 and attempt to run it on firmware version 1.8.x, 1.9.x, or 2.0.x, the results are unpredictable.

Version 2.0.3 was not released.

Caveats for Version 2.0.4

Closed Caveats

CSP #535465—A client wireless station was continually requesting a DHCP address. The server sent responses, but they were not seen on the wireless interface.

In the 2.0.1 release, the TX FIFO that handles multicast traffic when the AP goes off channel to scan for other APs was disabled. However, it is necessary to disable all the TX FIFOs when the AP goes off channel to scan for other access points. If the AP submits packets to the TX FIFOs when the AP has hopped to another channel to scan for beacons, the wireless chip microcode can stop outputting packets.

The AP regularly scans for access points when clustering is enabled or when rogue AP detection is enabled. When Clustering or Rogue AP detection is not used, the AP does not hop off channel to detect other Access Points. The AP541N does do aggressive channel scanning during the first two minutes after the AP boots up to quickly generate a table of potential rogue APs, but only does this at boot time and then does not perform another scan unless the Rogue AP or Clustering feature is enabled.

CSCub73520—Resolved the issue of DHCP handling between the access point and the DHCP server when Clustering or Rogue AP Detection is enabled.

Caveats for Version 2.0.2

Open Caveats

CSCty56257—Switching firmware versions might take a long time and when complete, the login page might not automatically come up in certain browsers, such as Internet Explorer 8.

Workaround: Wait two minutes and refresh the screen. The login screen should appear. If it does not appear, power cycle the device. If you are using Internet Explorer 8, you can also go to **Tools > Internet Options > Security > Custom** and set **Prompt for user name and password**. This setting can help avoid the problem.

CSCtg90061—The sysUpTime object ID (OID) does not match the actual system up time. The sysUpTime OID is currently tied to when SNMP is enabled. So each time SNMP is enabled, the sysUpTime OID is initialized to 0.

Workaround: Check **GUI Status > Device Information > System Uptime**. Or, if an SNMP query must be made, as long as SNMP is manually enabled after the device is rebooted AND is not disabled, the sysUpTime will be close to actual up time.

Closed Caveats

CSCtn81839—The device sends only one gratuitous ARP for an IP address instead of two or three when disabling or enabling DHCP.

CSCts45126—In Google Chrome 13, the About page does not display correctly.

CSCtn81981—The device does not broadcast a Goodbye message and sends only one gratuitous ARP for an IP address instead of of two or three.

CSCtn82389—Error checking for disabled SSIDs is not consistent.

CSCtn82420—Duplicate MAC address should not be allowed in MAC filtering.

CSCtn82500—Administration Access Control should not accept invalid source IP addresses.

Caveats for Version 2.0.1

Open Caveats

CSCts45075—When using Google Chrome, and the user sets an http redirect address on on the **Wireless** tab and saves the settings, a space is added before the "http://," causing the feature not to work.

Workaround: Firefox and Internet Explorer are the only fully supported browsers. Chrome is not a fully supported browser. If you still wish to use Chrome, delete the leading space in the URL address bar, and then save the settings.

CSCts45092—Firefox 4, 5 and Google Chrome sometimes experience problems opening the GUI pages (hung session). This issue is only seen if there are multiple WAPs connected to the same router as standalone WAP or in a cluster configuration.

Workaround: Google Chrome is not a fully supported browser. Later versions of Firefox such as 4.x and 5.x are not fully supported. Use Internet Explorer or clear your browser cookies, history, and cache.

Closed Caveats

CSCti77839—RF Scan works properly, shows all access points (APs).

CSCts51824—Unable to see all neighboring APs in the UI Neighbor list (**Status > Rogue AP Detection**).

CSCts51821—Unable to receive a DHCP address.

Caveats for Version 2.0.0

Open Caveats

CSCtn81665—No Bonjour startups for hot plug-in

Workaround: Remove and reconnect the Ethernet cable (non-PoE). Perform a reboot.

CSCtn82461—Hostname starting with numeric should be accepted

Hostname containing all numerics is not allowed. However, hostname with leading numeric and trailing with additional numeric and non-numeric should be accepted but is currently rejected.

Workaround: Leading character should not be a numeric value.

CSCtn84775—IPv6 is not supported with Bonjour

Workaround: There is not a workaround at this time.

Closed Caveats

CSCth14132—Station Isolation is Sporadic

CSCth12675—MAC Filtering Set To **Block** Fails to Block Access

Caveat for Version 1.9.2

WARNING Invalid XML configuration file updates might cause an unrecoverable device crash. When making updates directly to the configuration file (for example, by using a text editor) use the string values described in the Cisco Small Business AP541N Dual-band Single-radio Access Point Administration Guide. Any deviation from the allowed values or typographical errors might cause the access point to fail to operate. In some cases, recovery from such a failure cannot be accomplished by resetting the device to factory default values.

Up to the date of this release note, all devices shipped are with hardware version ID (VID) V01; in the future, due to the potential EOL of a flash component, there is a possibility that we may ship with new hardware version (VID) V02 for accommodating the new flash component. In that case, devices with hardware version ID (VID) V02 must run on firmware version 1.9.2 or higher, i.e. not to be downgraded to earlier version of firmware.

Caveats for Version 1.9.1

Open Caveats

CSCth14132—Station Isolation is Sporadic

Occasionally when Station Isolation (local LAN communication) is set to **Disabled auto**, the device reverts to a **Blocking** state. The configuration continues to indicate that the feature is **Disabled**. As a result, computers cannot access local devices, such as printers. Access to remote devices (outside the local AP LAN) can be accessed (for example, access to an external Web site).
Workaround: Reboot or restart the device.

CSCth12675—MAC Filtering Set To **Block** Fails to Block Access

If you set MAC Filtering to block specified addresses, the device fails to prevent association and authentication.
Workaround: None

Closed Caveats

CSCth09954—CCA Fails Due to an Incorrectly Propagated Device Name

The device name **AP 541NA-K9** was propagated by CDP advertisements received by UC520 devices. The name should have been **AP541N-A-K9** (no space). The space between **AP** and **541NA-K9** prevented Cisco Configuration Assistant (CCA) from accessing the AP 541N for configuration.

Caveats for Version 1.9.0

Open Caveats

CSCtg53062—Configuration Interface Allows More Than 10 Cluster Members

The configuration interface allows more than 10 cluster members, but adding more than 10 cluster members degrades the performance of the device. This includes the Network Neighborhood sometimes showing NULL signal strength.
Workaround: We recommend that a cluster not exceed 10 members.

Closed Caveats

The following caveats have been resolved in version 1.9.0:

CSCtg28316—WL Driver Multicast Queue Freezes

After a period of time, the access point stops forwarding Multicast or Broadcast frames. Also, the last frame on the MCast queue is not always cleared.

CSCtg28338—WPA Key Refresh Freezes

If during disassociation the access point is refreshing a client broadcast key, that client is not accounted for and the WPA key state machine freezes.

CSCtg28357—Error Message on MIB walk: Must Define the apRadioStationIsolation Instance in CISCO-WLAN-ACCESS-POINT-MIB

The following MIBs are added in the MIB repository net-SNMP—(C:\usr\share\snmp\mibs):

```
CISCO-WLAN-ACCESS-POINT-MIB.txt
CISCO-WLAN-ACCESS-POINT-REF-MIB-A-SKU.txt
CISCO-WLAN-ACCESS-POINT-REF-MIB-E-SKU.txt
CISCO-WLAN-ACCESS-POINT-REF-MIB-N-SKU.txt
```

The MIB names are C:\usr\etc\snmp (snmp.conf). For example:

```
mibdirs C:/usr/share/snmp/mibs
persistentDir C:/usr/snmp/persist
tempFilePattern C:/usr/temp/snmpdXXXXXX
mibs +OLD-CISCO-CHASSIS-MIB
mibs +CISCO-WLAN-ACCESS-POINT-REF-MIB
mibs +CISCO-WLAN-ACCESS-POINT-REF-MIB
mibs +CISCO-WLAN-ACCESS-POINT-REF-MIB
mibs +CISCO-WLAN-ACCESS-POINT-MIB
```

If there is anything wrong with the added MIBs, running a **MIB walk** at a command prompt generates an error message. For example:

```
C:\Documents and Settings\tdobrovo\Desktop>snmpwalk -v 2c -c public 172.25.144.155
sysObjectID

Undefined OBJECT (apRadioStationIsolation): At line 3670 in C:/usr/share/
snmp/mibs/CISCO-WLAN-ACCESS-POINT-MIB.txt
SNMPv2-MIB::sysObjectID.0 = OID: CISCO-SMI::ciscoProducts.1135.1.28
```

To avoid this error, define **apRadioStationIsolation** in **CISCO-WLAN-ACCESS-POINT-MIB**.

CSCtg28364—Standalone AP EDCA: Misreported Values for the TxOP Burst Queue Attributes

The **EDCA Max Burst** parameter should be in units of **32us** periods, but it is not converted correctly by the access point.

CSCtg28367—Cisco AP541N MIB sysObjectId Does Not Return the Correct Number

The wrong OID is returned by the object in the access point code.

CSCtg28374—CDP Show Neighbor Displays Only Four CDP Entries

When the **`cdh show neighbor`** command is executed on console, it displays only four neighbor entries.

Caveats for Version 1.8.0

Open Caveats

There are no open caveats in version 1.8.0:

Closed Caveats

The following caveats have been resolved in version 1.8.0:

CSCtd63549—Time Parameter Does Not Allow Setting the Time Zone

CSCtd63503—Wireless IP Phones are Frequently De-registering

CSCtd63487—Some Pages Render Very Slowly

CSCtd62176—Voice Packets are Dropped on RX on the 7921 Clients

CSCtd62146—Primary Image Corrupted After 10 Days

CSCtd62123—System Time Cannot be Set by using the GUI

CSCtd62096—Remove IPV6 References, as it is not Supported

CSCtd62087—WPA-PSK-AES Fails If There are Two Open SSID With the Same Name at Different Security Levels

CSCtd62084—Station Isolation Settings are Not Propagating When Clustering is Enabled

CSCtd62071—Management and Untagged VLAN Field Values Cannot be Changed

Caveats for Version 1.7.2

Open Caveats

The following caveats are open in version 1.7.2:

CSCtd63549—Time Parameter Does Not Allow Setting the Time Zone

NTP configuration in the Setup window does not allow for time zone configuration.

CSCtd63503—Wireless IP Phones are Frequently De-registering

The IP phones are able to successfully register with the call manager and make successful calls. However, the phones de-register after 5 minutes, sometimes in the middle of a call. The wireless association is maintained. It is possible that the keepalives (heart beat messages) sent by the phone are not reaching the CME and the CME de-registers the phones.

CSCtd63487—Some Pages Render Very Slowly

Some configuration GUI pages render very slowly in the AP541N-1.2(1) image when the Advanced tab is selected.

CSCtd62176—Voice Packets are Dropped on RX on the 7921 Clients

Voice packets are dropped on RX on 7921 clients. Call manager uses G.711 codec by default. Tx and RX on both sides should be 50 pps (packets per second). The TX on the 7960 is 50 pps (equal to Rx on 7921) but the Rx on the 7960 is only about 40 - 43 pps, about 14% packet drops on the RTP stream from the 7921 to the 7960.

CSCtd62146—Primary Image Corrupted After 10 Days

The primary image is corrupted after 10 days of use. After multiple reboots of a 1.4(0) image it, suddenly was reported as being corrupted and the device booted of the secondary image.

CSCtd62123—System Time Cannot be Set by using the GUI

The system time parameter cannot be set manually by using the GUI.

CSCtd62096—Remove IPV6 References, as it is not Supported

There are references to IPV6, which is not supported.

CSCtd62087—WPA-PSK-AES Fails If There are Two Open SSID With the Same Name at Different Security Levels

The Cisco device allows two SSIDs to have same name, if they have different security levels. However, most client devices cannot tell the difference and see them as one BSSID. If two SSIDs have the same name, one with WPA-PSK-AES and one without, the network will fail to pass traffic.

CSCtd62084—Station Isolation Settings are Not Propagating When Clustering is Enabled

Station isolation settings for VAPs are not propagating when clustering is enabled.

CSCtd62071—Management and Untagged VLAN Field Values Cannot be Changed

The Management VLANid and Untagged VLANid fields in the GUI accept user input; however, the changes are not accepted and the values in the device configuration remain at the default setting of 1.

Related Information

Support	
Small Business Support Community	www.myciscocommunity.com/community/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.
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

78-19182-09