

Response to Questions Posed by Mr. Andrew Leimer,
FCC Application Processing Branch
July 6, 2005

Re: FCC ID: LDK102056
Applicant: Cisco Systems, Inc.
Correspondence Reference Number 29134
731 Confirmation Numbers EA458806 and EA88290

1) Submit an internal photos exhibit. You can cut/paste them from the external photos exhibit. A file is required or the system will lock out the Grant feature.

An internal photos exhibit has been uploaded.

2) Explain how this device meets the unique antenna connector requirements of Section 15.203.

This device uses reverse polarity TNC connectors for external antenna connections to comply with the unique antenna connector requirement of 15.203.

3) Submit a new Theory of Hardware Operation file. Figure 1 is unreadable. Please view the file before resubmission.

A new Hardware Theory of Operation has been uploaded.

3) Submit an MPE exhibit the RF Exposure exhibit. Once again, you can cut/paste it from the Test Report exhibit.

An RF exposure exhibit has been uploaded.

4) **“Submit a letter explaining how this device meets the definition and requirements for SDR.”**

47 U.S.C. Section 2.1 Terms and Definitions.

* * * * *

(c) * * *

Software Defined Radio. A radio that includes a transmitter in which the operating parameters of frequency range, modulation type or maximum output power (either radiated or conducted), or the circumstances under which the transmitter operates in accordance with Commission rules, can be altered by making a change in software without making any changes to hardware components that affect the radio frequency emissions.

The hardware and firmware architecture allows alteration of the frequency range and output power in a conducted sense under software control. The “circumstances under which the transmitter operates in accordance with Commission rules,” in particular, will apply to future software releases enacting approved DFS operation in the 5.47-5.725 GHz band. This and any other future operational changes will be implemented completely in software without any hardware component changes “that affect the radio frequency emissions.” The access point has been designed and characterized in advance for compliant operation in the 5.47-5.725 GHz band. Said operation will be made available to customers by Cisco’s future release and controlled distribution of software updates under the allowance of a Class III permissive change.

2.944 Software Defined radios.

- (a) Manufacturers must take steps to ensure that only software that has been approved with a software defined radio can be loaded into the radio. The software must not allow the user to operate the transmitter with operating frequencies, output power, modulation types or other radio frequency parameters outside those that were approved. Manufacturers may use means including, but not limited to the use of a private network that allows only authenticated users to download software, electronic signatures in software or coding in hardware that is decoded by software to verify that new software can be legally loaded into a device to meet these requirements and must describe the methods in their application for equipment authorization.

Future software releases which allow new operational parameters, particularly approved operation in the 5.47-5.725 GHz band, will be released in a conventional manner to Cisco customers. New units shipping from the factory, as well as units already in the field, have unalterable firmware configurations which define the radio’s regulatory domain. These configurations will interact with the new software to restrain the operation within the original regulatory domain.

- (b) Any radio in which the software is designed or expected to be modified by a party other than the manufacturer and would affect the operating parameters of frequency range, modulation type or maximum output power (either radiated or conducted), or the circumstances under which the transmitter operates in accordance with Commission rules, must comply with the requirements in paragraph (a) of this section and must be certified as a software defined radio.

Cisco neither has provided for or expects any third party alteration of software. This includes software installed on existing units as well as future software updates.

- (b) Applications for certification of software defined radios must include a high level operational description or flow diagram of the software that controls the radio frequency operating parameters.

Such descriptions and diagrams are attached to the original filing. See attachments *Cisco AP Software Theory of Operation*.

2.1043 Changes to certificated equipment.

* * * * *

(b) * * *

(3) A Class III permissive change includes modifications to the software of a software defined radio transmitter that change the frequency range, modulation type or maximum output power (either radiated or conducted) outside the parameters previously approved, or that change the circumstances under which the transmitter operates in accordance with Commission rules. When a Class III permissive change is made, the grantee shall supply the Commission with a description of the changes and test results showing that the equipment complies with the applicable rules with the new software loaded, including compliance with the applicable RF exposure requirements. The modified software shall not be loaded into the equipment, and the equipment shall not be marketed with the modified software under the existing grant of certification, prior to acknowledgement by the Commission that the change is acceptable. Class III changes are permitted only for equipment in which no Class II changes have been made from the originally approved device.

NOTE TO PARAGRAPH (b)(3):

Any software change that degrades spurious and out-of-band emissions previously reported to the Commission at the time of initial certification would be considered a change in frequency or modulation and would require a Class III permissive change or new equipment authorization application.

Cisco will supply complete descriptions and test reports covering all transmitter and unintentional emission measurements under the new operational parameters. These will be included in our submission for a Class III permissive change.

5) Please provide more information/clarification about Regulatory Domain compliance. Taking an example of upgrading the device with a Class III permissive change to a new band (i.e. the new 5.5 GHz UNII bands) , please describe how the Class III permissive change will enable new capabilities without changing the hardware and how would the regulatory compliance be assured. Please note, that we need a better understanding of some of the following:

a) Does the hardware that is shipped already have the capability to operate on the new DFS band?

Yes, the access point does have DFS band capability.

If so, are there plans to ship, provide or make available user downloadable software to the end user to enable new capability?

Yes this is our plan.

If yes, would the hardware have capability to operate in multiple regulatory domains ? If yes, how do you restrict someone from downloading software for different regulatory domain to modify the operational parameters?

No, the hardware would be constrained to remain in the original regulatory domain it was shipped under.

If the hardware does not have the new channels already in the hardware, how would the new channels be added?

The new DFS channel capabilities are already designed into the hardware, but are not currently activated by software.

If the regulatory domain controls the capability of the downloaded software, how are new regulatory domain compliance achieved ?

The unit's original firmware constrains the operational software to operate in the proper regulatory domain. New features or operational parameters for the individual regulatory domains are contained in the ongoing software releases, but only those features corresponding to the unit's permanent domain setting may be invoked. Any software feature or operational change for the U.S. regulatory domain will be released only after an authorized Class III permissive change is obtained from the FCC.

b) We need to understand what aspect of regulatory compliance is changed with regard to the example above as part of this SDR.

Cisco plans to activate 11 new DFS channels after receiving authorization via a Class III permissive change. This authorization, we anticipate, will occur after the product begins shipping with approved operation in the 12 conventional UNII channels.

6) Additional information on authentication of the software is needed. When different drivers are available, how does the device ensure that the provided driver to the end user will be compliant. The end user must not be able to install drivers that can operate the device with unapproved radio parameters or modes.

"Different drivers" will not be available. A single AP software release will cover all hardware SKUs and will not require authentication, per se. The

Cisco software structure ensures only authorized features for the corresponding permanent domain settings (installed in the radio firmware during manufacture) are activated in the field. Please see the a Cisco AP Software Theory of Operation attached to the original filing.

7) Indicate how the software updates are implemented, distributed and controlled. Describe how the unit meets the overall requirements of 2.932 (e) for software download and authentication, and as appropriate, the following questions need to be addressed.

For example, are only new units modified/updated prior to shipment?

No. Later software releases are intended to be available to end users after receipt of their units.

Are units that which are already sold updated through the installation of a new end user installed driver for the new configuration?

Yes.

If the end user updates the new configuration with a new driver, how do you ensure that only authorized driver is used with the proper device?

The permanent domain settings installed in the radio at manufacture prevent unauthorized operation because these settings dictate which features in the new software load are allowed for its particular regulatory domain.

8) Describe what means exist to prevent the end user modifying the software, driver or memory through a patch mechanism or other means which may modify the approved software?

Cisco takes numerous steps to ensure the security of its software and, unlike "open systems" structures, provides inherent resistance to "hacking" and "patching." The AP software releases also contain radio Media Access Controller (MAC) firmware which implements radio control settings in accordance with the permanent domain setting of the radio. The MAC is based on a proprietary RISC architecture and is programmed in low-level assembly language. It is impossible for a third party to create an object file or executable for the MAC without intimate knowledge of the hardware, memory map, and the proprietary op codes of the processor. See "AP Software Theory of Operation," Section 3.0 "Security Against Unauthorized Firmware Images."

9) What authentication or security system measures are there to ensure that no third party can modify the software portion that controls the RF parameters?

The permanent domain settings control the RF parameters and are stored in a protected area of the non-volatile memory map. Only the proprietary test utilities possessed and administered by Cisco Manufacturing may install these settings.

Indicate how the software access is controlled and what 3rd party changes are permitted which may change the RF characteristics of the device.

No changes may be made by a third party to alter the device's RF characteristics.

How does the hardware or existing software verify that only authenticated software is operating in the system?

Authentication is not necessary due to the overriding control of the permanent domain settings.

If the hardware with software control has the ability to operate in multiple regulatory domains, what control exists that while in US only the authorized software is capable of operating? (i.e. how does the system prevent a European version of the software running in US?)

Cisco controls this by configuring the permanent domain settings within the radio hardware at ordering, configuration, and shipping, and applies a domain-specifying label to each unit which contains model number and serial number of the unit.

10) How can the FCC verify, in the field, that correct version of the software is running in the device?

Aside from direct measurement or observation of operation, the domain setting can be positively identified by inspection of the label. The software version number is accessible via the normal console interface to the access point, accessible by serial port (command line interface), web page interface, or telnet session via TCP/IP.

Submit a description of this capability and instructions for the FCC to use in the field to verify that proper software is operating in the device.

The FCC may inspect the unit's serial number/domain setting label. Alternately, the console interface may be manipulated to display the individual radio domain settings.

To identify regulatory settings in Command Line Interface for the 5GHz radio, starting at the ap> prompt:

```
ap>show cont d1
!  
interface Dot11Radio1  
Radio AIR-AP1131A, Base Address 0012.44b4.7b60, BBlock version 0.00,  
Software ve  
rsion 5.65.3  
Serial number: ALP084810T6  
Number of supported simultaneous BSSID on Dot11Radio1: 8  
Carrier Set: China (UNI3) (CN )  
DFS Required: No  
Current Frequency: 5805 MHz Channel 161  
Allowed Frequencies: 5745(149) 5765(153) 5785(157) 5805(161)  
Current Power: 17 dBm  
Allowed Power Levels: -1 2 5 8 11 14 15 17
```

To identify regulatory domain setting in GUI for the 5GHz radio:

- 1) In a web browser, type the access point IP address (10.0.0.1 by default) into the web browser address bar.
- 2) Enter Cisco as the user name and password.
- 3) Select Network Interfaces on the left column.
- 4) Select Radio1-802.11A on the right column.

Are there any means by which software version numbers can be related to any future Class III permissive changes?

Cisco plans to disclose to the FCC in our Class III permissive change application(s) the software version number which will first enact the proposed changes. In addition, Cisco will refer to the authorized Class III changes in software release notes available to the field.