CISCO

Date: December 5, 2012

FCC IC: Q87-WES610NV2 Channel plan and software operational info

Question 1
Submit a channel/frequency plan for this device showing the channels that have active scanning or passive scanning. Active scanning is where the device can transmit a probe (beacon) and passive scanning is where the device is can listen only with no probes.
<Reply>
No active scan, only passive scan on following DFS bands.
Chanel 52, 56, 60, 64, 100, 104, 108, 112, 116, 132, 136 & 140.

Question 2
Verify that this device does not have ad-hoc mode.
<Reply>
This device does not support ad-hoc mode on all channels (include DFS channels.)

Question 3
Verify that this application contains a complete User's Manual and/or Professional Installers Manual. If the manual is not complete, upload an updated User's Manual exhibit.
<Reply>
The submitted manual is the latest full version for client.

Question 4
Can this device act as an access point on the non-DFS legacy frequencies (5.15-5.25 GHz)
<Replay>
No, this device does not act as an access point.

Question 5
Verify that this device meets the frequency requirements of Section 15.202
<Reply>
This device doesn't support 802.11d. It listens on DFS channels to look for access point without sending probe request.

Question 6
For client devices that have software configuration control to operate in different modes (active scanning in some and passive scanning in others) in different bands (devices with multiple equipment classes or those that operate on non-DFS frequencies) or modular devices which configure the modes of operations through software, the application must provide software and operations description on how the software and / or hardware is implemented to ensure that proper operations modes cannot be modified by end user or an installer.
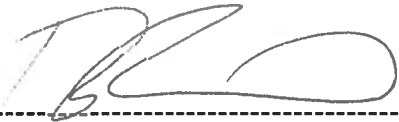
<Reply>
This device scans actively on non-DFS channels and passively on DFS channel. Ad-hoc mode isn't supported by this device.

As part of the DFS functionality in the WLAN driver, software is implemented to react to radar detection messages and move to a new channel. The control of this functionality is not accessible to anyone under any conditions. Furthermore, the firmware is locked by special signature, CRC checksum and cannot be changed or modified by end user. The firmware is protected by special signature and CRC checksum. Signature and CRC checksum will be calculated and verified before firmware upgrade. Unauthorized modification to firmware will lead the failure of verification thus firmware upgrade is not allowed.

Sincerely yours,

Darrell Tennis / Manager Compliance
Cisco Consumer Products LLC
Phone: 949-910-7048
Fax: 949-823-3002
E-mail: dtennis@cisco.com