![Cisco logo]

16. May. 2023

DTS-UNII device declaration letter

To whom it may concern, Cisco Systems, Inc. declares the features below for equipment authorization regarding FCC ID: LDK0401B2757

1. DFS device:
   ☐ Master
   ☐ DFS Client with radar detection capability
   ☒ DFS Client without radar detection capability.

2. Active / Passive scanning – for ad-hoc mode access point capability:

Center frequencies (F$_0$, MHz)	Active scanning (able to select channel and initiate a network)	Passive scanning (not able to initiate a network)	Not applicable
2412 - 2462	☒ Yes ☐ No	☐ Yes ☒ No	☐
5160 – 5240 (UNII-1)	☒ Yes ☐ No	☐ Yes ☒ No	☐
5260 – 5340 (UNII-2A)	☐ Yes ☐ No	☐ Yes ☐ No	☒
5480 – 5720 (UNII-2C)	☐ Yes ☐ No	☐ Yes ☐ No	☒
5745 – 5855 (UNII-3)	☒ Yes ☐ No	☐ Yes ☒ No	☐

Active scanning: The device can transmit a beacon/probe.

Passive scanning: The device does not transmit a beacon/probe.

This device supports ad-hoc mode only on US non-DFS frequencies.

3. Country code selection ability:
   It is not possible for the user to select country code. Country code is factory set in the UI and cannot be changed by end users.

4. Meet 15.202 requirement - ☒ Yes , ☐ No

   ☐ A master device is defined as a device operating in a mode in which it has the capability to transmit without receiving an enabling signal. In this mode it is able to select a channel and initiate a network by sending enabling signals to other devices.

☒ A client device is defined as a device operating in a mode in which the transmissions of the device are under the control of the master. A device in client mode is not able to initiate a network.

(5) 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.

☒ Apply, Yes, please see Software Security Description.

☐ Not apply (If apply, please help to provide an explanation on it was implemented, and how the software was controlled)

Applicant: Cisco Systems, Inc.

Address: 125 West Tasman Drive, San Jose, California 95134-1706, USA

Signature:

Name: Ola Taarud Rømoen

Tel: +47 9949 3443

Email: oromoen@cisco.com