IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
MARSHALL DIVISION

UNILOC 2017 LLC Plaintiff, v. CISCO SYSTEMS, INC., Defendant.	§	Case No. 2:18-cv-00505-JRG Jury Trial Demanded

PLAINTIFF'S FIRST AMENDED COMPLAINT FOR PATENT INFRINGEMENT

COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Uniloc 2017 LLC ("Uniloc"), by and through the undersigned counsel, hereby files this First Amended Complaint and makes the following allegations of patent infringement relating to U.S. Patent Nos. 6,664,891 and 6,285,892 against Defendant Cisco Systems, Inc., ("Cisco") and alleges as follows upon actual knowledge with respect to itself and its own acts and upon information and belief as to all other matters:

NATURE OF THE ACTION

1. This is an action for patent infringement. Uniloc alleges that Cisco infringes U.S. Patent Nos. 6,664,891 (the "'891 patent") and 6,285,892 (the "'892 patent"), copies of which are attached hereto as Exhibits A-B (collectively, "the Asserted Patents").

2. Uniloc alleges that Cisco directly and indirectly infringes the Asserted Patents by making, using, offering for sale, selling and importing devices such as Cisco's Beacon Point and Cisco's Meraki Bluetooth Low Energy ("BLE") solutions. Uniloc further alleges that Cisco induces and contributes to the infringement of others. Uniloc seeks damages and other relief for Cisco's infringement of the Asserted Patents.

THE PARTIES

3. Uniloc 2017 LLC is a Delaware corporation having places of business at 1209 Orange Street, Wilmington, Delaware 19801, 620 Newport Center Drive, Newport Beach, California 92660 and 102 N. College Avenue, Suite 303, Tyler, TX 75702.

4. Uniloc holds all substantial rights, title and interest in and to the Asserted Patents.

5. Upon information and belief, Defendant Cisco Systems, Inc. is a corporation organized and existing under the laws of the State of California, with at least the following regular and established places of business in this District: 2300 E. President George Bush Hwy., Richardson, Texas 75082 and 2260 Chelsea Blvd., Allen, Texas 75013. Cisco may be served

with process through its registered agent for service in Texas: Prentice Hall Corporation System, 211 E. 7th St., Suite 620, Austin, Texas 78701.

6. On information and belief, Cisco's Richardson facility is a multiple building campus with more than 2,000 Cisco employees.

7. On information and belief, Cisco's Allen facility is a 162,000 square foot data center.

8. On information and belief, Cisco's Richardson and Allen facilities were appraised and taxed by the Collin County Appraisal District at values in excess of $300,000,000.

JURISDICTION AND VENUE

9. This action for patent infringement arises under the Patent Laws of the United States, 35 U.S.C. § 1 et. seq. This Court has original jurisdiction under 28 U.S.C. §§ 1331 and 1338.

10. This Court has both general and specific jurisdiction over Cisco because Cisco has committed acts within the Eastern District of Texas giving rise to this action and has established minimum contacts with this forum such that the exercise of jurisdiction over Cisco would not offend traditional notions of fair play and substantial justice. Defendant Cisco, directly and through subsidiaries, intermediaries (including distributors, retailers, franchisees and others), has committed and continues to commit acts of patent infringement in this District, by, among other things, making, using, testing, selling, licensing, importing and/or offering for sale/license products and services that infringe the Asserted Patents.

11. Venue is proper in this district and division under 28 U.S.C. §§ 1391(b)-(d) and 1400(b) because Cisco has committed acts of infringement in the Eastern District of Texas and has multiple regular and established places of business in the Eastern District of Texas.

COUNT I – INFRINGEMENT OF U.S. PATENT NO. 6,664,891

12. The allegations of paragraphs 1-11 of this Complaint are incorporated by reference as though fully set forth herein.

13. The ’891 patent, titled “Data Delivery Through Portable Devices,” issued on December 16, 2003. A copy of the ’891 patent is attached as Exhibit A.

14. Pursuant to 35 U.S.C. § 282, the ’891 patent is presumed valid.

15. Invented by Koninklijke Philips Electronics, N.V., the inventions of the ’891 patent were not well-understood, routine or conventional at the time of the invention. At the time of invention of the ’891 patent, the world was witnessing a great increase in mobile phone subscribers and networks through advances in technology and the addition of functionalities. ’891 patent at 1:11-14. As a result, a mobile information society was developing, with personalised and localised services becoming increasingly more important. *Id*. at 1:14-17. "Context-Aware" (CA) mobile telephones were developed used with low power, short range base stations in places like shopping malls to provide location-specific information. *Id*. at 1:17-20.

16. With Bluetooth communications protocols predicted to become a common technology in mobile communications devices, one possible solution to the problems of establishing a broadcast mode for CA applications considered was using the full current Bluetooth handshaking process to set up a two-way Bluetooth connection for data exchange between mobiles carried by consenting users selecting such a service. *Id*. at 2:4:-13. However, the Bluetooth connection protocol at the time carried the disadvantages of: i) the time required to establish the connection before any data can be exchanged was too long (e.g., 10-30 seconds, by which time the encountering parties may be out of RF range), ii) undesirable power consumption for hand shaking transmissions on behalf of the listening device to establish network connection; iii) limits of number of active listening devices that can be addressed by a broadcasting device; and iv) loss of privacy by the listening device as its device becomes known by the broadcasting

device in the process of establishing the connection. *Id*. at 2:13-34. In many opportunistic situations, the listener to a broadcast wishes their identity and location to remain anonymous and private. This was a major drawback. *Id*. Another potential solution involved a central service that registers those mobile users in proximity to a fixed infrastructure and for example compares web-stored user profiles, alerting users via Bluetooth or the cellular network of matches. *Id*. at 2:35-38. However this also suffered from some of the disadvantages above (especially privacy) and, in addition, restricted the encounters to pre-determined places where a user-locating RF beacon is installed, rather than ad-hoc encounters. *Id*. at 2:38-42.

17. The inventive solution of the claimed inventions of the '891 patent provides a method for portable communication devices to broadcast messages to users of other portable communications devices that overcome the disadvantages of the prior art.

18. A person of ordinary skill in the art reading the ’891 patent and its claims would understand that the patent’s disclosure and claims are drawn to solving a specific, technical problem arising in the field of RF communications between low power portable communications devices, such as portable telephones and suitably equipped PDAs. *Id*. at 1:4-10. Moreover, a person of ordinary skill in the art would understand that the claimed subject matter of the ’891 patent presents advancements in the field of RF communications between low power portable communications devices, such as portable telephones, suitably equipped PDAs and low power beacons, and more particularly, in the field of broadcast communications between these types of devices that improves over the drawbacks of prior art systems. *Id*. at 4:46-63.

19. On information and belief, Cisco makes, uses, offers for sale, and/or sells in the United States and imports into the United States portable communication devices that broadcast message to users of other portable communication devices, such as the Cisco Beacon Point (collectively the “Accused Infringing Devices”).

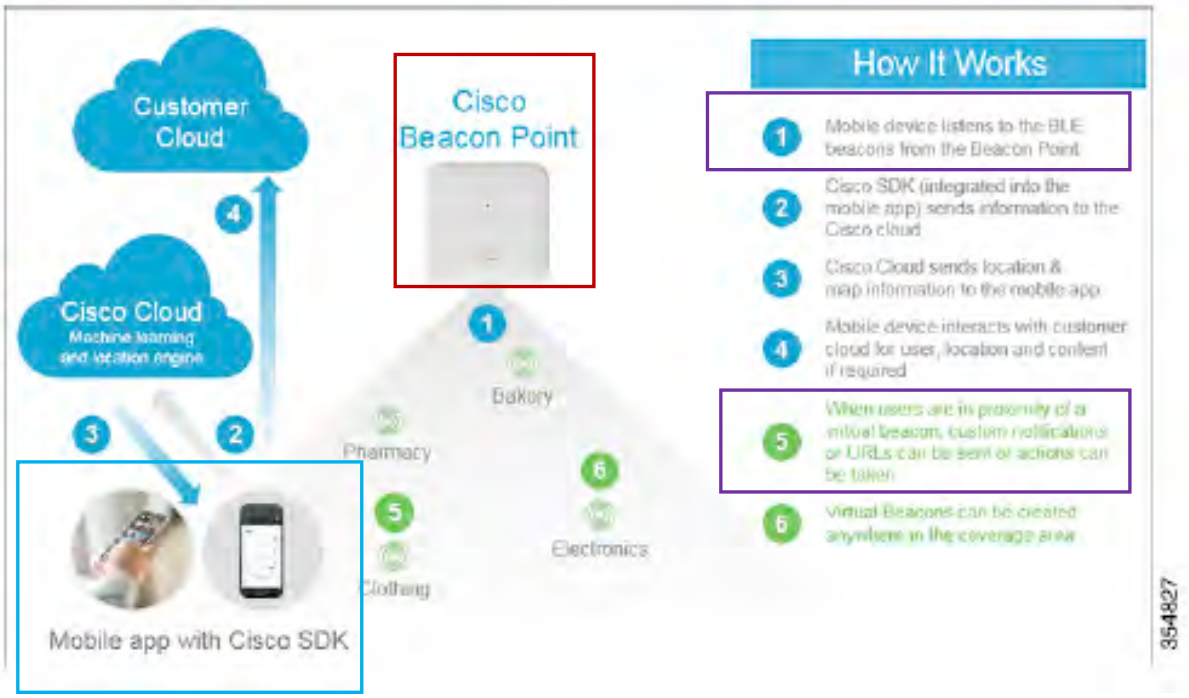
20. Upon information and belief, the Accused Infringing Devices infringe at least claim 14 in the exemplary manner described below.

21. The Accused Infringing Devices are portable communication devices that broadcast messages to users of other portable communication devices. The Accused Infringing Devices broadcast messages, such as custom notifications or URLs, to other devices in proximity.

> As mobile devices enter a Beacon Point coverage area, mobile applications receive multiple beams from the Beacon Points in the area. These BLE Received Signal Strength Indication (RSSI) observations are captured by the mobile client SDK and securely sent to the CMX Cloud Beacon Center over the Wi-Fi network or via 3G/ LTE cellular network.

Source: https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/white-paper-c11-737782.pdf

Figure 2: Cisco Virtual Beacon Architecture



Source: https://www.cisco.com/c/en/us/td/docs/wireless/cmx_cloud/vBLE_SUG/b_cg_Cisco_Beacon_Center/b_cg_Cisco_Beacon_Center_chapter_01.html

22. The Accused Infringing Devices broadcast a series of advertisements (inquiry messages) using Bluetooth beacons. These broadcasts are received by any smart device with Bluetooth in the vicinity of the Accused Infringing Devices.

> When a Cisco Beacon Point is deployed in a facility, any smart device that is enabled with bluetooth, that enters the Cisco Beacon Point coverage area, receives messages from that Cisco Beacon Point. Smart devices are capable of listening to beacons and invoking the mobile SDK app that is specific for the facility. For

Source: https://www.cisco.com/c/en/us/td/docs/wireless/cmx_cloud/vBLE_SUG/b_cg_Cisco_Beacon_Center/b_cg_Cisco_Beacon_Center_chapter_01.html

> Cisco has recently introduced Cisco Beacon Point (AIR-VBLE1-K9), which is an industry-first virtual BLE beacon. Cisco Beacon Point supports beaconing in Apple iBeacon, Google Eddystone, and AltBeacon advertising formats.

Source: https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/white-paper-c11-737782.pdf

23. The Bluetooth advertisements (inquiry messages) as transmitted by the Accused Infringing Devices contain a plurality of predetermined data fields, such as the preamble, Access address, PDU header and Broadcast address.

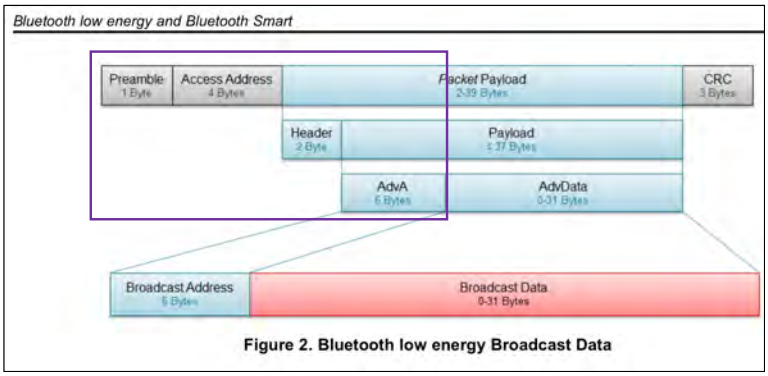


Figure 2. Bluetooth low energy Broadcast Data

Source: http://www.ti.com/lit/an/swra475a/swra475a.pdf

24. The Accused Infringing Devices' advertisements add a broadcast message (e.g.,

UUID, Major, Minor) prior to transmission such that suitably configured other portable devices may receive the transmitted inquiry messages.

The Preamble, Access Address, Header, MAC Address, and CRC will be set as part of the BLE radio's frame construction. The TX Power is a calibrated indicator of the RSSI of the transmitted measured at a 1m distance; this can be used for rough estimation of proximity to the device emitting the Beacons.

UUID, Major, and Minor are fields defined by the Beacon network administrator. Typically, an organization will define a unique identifier for their habitual usage: the UUID. All Beacons deployed throughout their locations would have the same UUID.

To differentiate Beacons at different offices or store locations, and Beacons within different areas of those locations, the Major and Minor fields are used. For example, a chain restaurant might decide that all restaurants within a city will share a Major, and each restaurant within that city will have a different Minor.

Source: https://documentation.meraki.com/MR/Bluetooth/Bluetooth_Low_Energy_(BLE)

Manage a vBeacon

After adding a vBeacon, you can select and edit its parameters.

Step 1 From the **vBeacons** tab, check the appropriate vBeacon check box.

Step 2 In the **Selected vBeacon** panel, click **Edit**.

Step 3 In the **Quick Edit vBeacon** dialog box, edit the following parameters:

- **Name**—Name of the vBeacon.
- **Message**—Message to be displayed.
- **UUID**—The unique identifier, a 16-byte string used to differentiate a large group of related beacons.
- **URL**—URL of the redirect page that the user navigates to when they are near the vBeacon.
- **Transmit Power**—Use the slide bar to adjust the transmit power to increase the proximity ring size. The transmit power details are displayed. Click **Reset to default** to reset the transmit value to default.

Note This parameter also defines the distance at which the user receives the notification on the app. The default is 4 dBM, that is approximately 10 feet. To send a notification to the user at 50 feet, adjust the slider to 18 dBM that corresponds to the 50-feet distance.

- **Major**— A 2-byte string to distinguish a small subset of beacons within the larger group. This value, along with **UUID** and **Minor** value is used to identify the unique beacon. This is as per Apple's iBeacon standard. Currently, you can keep it blank. However, you can use this value to migrate a physical beacon system to Cisco Virtual Beacon, as per a customer's existing physical deployment using iBeacons.
- **Minor**— A 2-byte string to identify individual beacons.

Source: https://www.cisco.com/c/en/us/td/docs/wireless/cmx_cloud/vBLE_SUG/b_cg_Cisco_Beacon_Center/b_cg_Cisco_Beacon_Center_chapter_01.html

25. Cisco provides a SDK to suitably configure other portable devices to receive the transmitted inquiry messages and read the broadcast data from said additional data field.

Cisco Virtual Beacon SDK supports iOS and Android mobile devices. The SDK app receives the BLE beacon messages and sends the client details to the Cisco CMX cloud. The SDK app also displays the client location in real time on the client device.

Source: https://www.cisco.com/c/en/us/td/docs/wireless/cmx_cloud/vBLE_SUG/b_cg_Cisco_Beacon_Center/b_cg_Cisco_Beacon_Center_chapter_01.html

26. Applications using the SDK can read the broadcast data from the said additional field (UUID, Major, Minor) before sending these details back to the Cisco cloud.

> The mobile SDK app receives the BLE beacon signals and gathers data from the mobile device. The app, in turn, sends the beacon details (UUID, Major, Minor, TX, and so on) that is received to the Cisco CMX Cloud location engine.

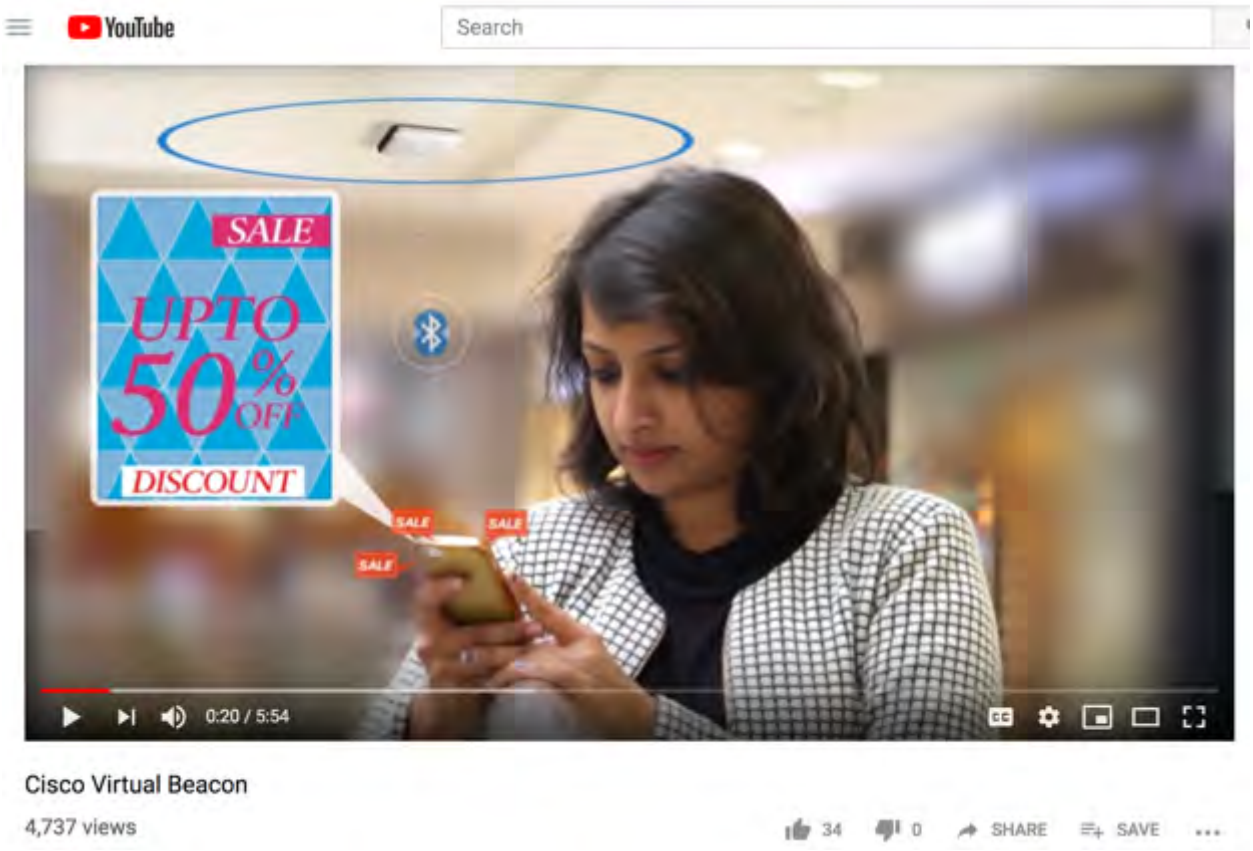
Source:
https://www.cisco.com/c/en/us/td/docs/wireless/cmx_cloud/vBLE_SUG/b_cg_Cisco_Beacon_Center/b_cg_Cisco_Beacon_Center_chapter_01.html

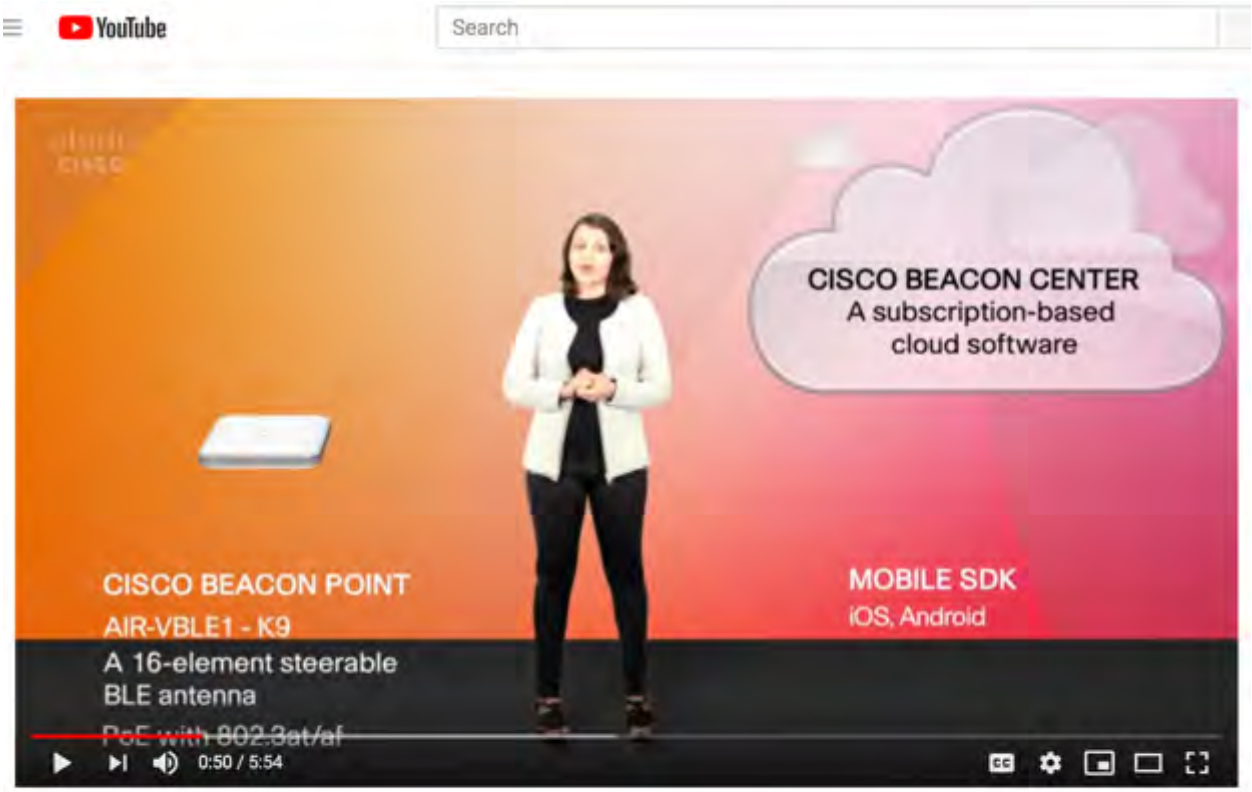
27. Cisco has infringed, and continues to infringe, at least claim 14 of the '891 patent in the United States, by making, using, offering for sale, selling and/or importing the Accused Infringing Devices in violation of 35 U.S.C. § 271(a).

28. Cisco also has infringed, and continues to infringe, at least claim 14 of the '891 patent by actively inducing others to use, offer for sale, and sell the Accused Infringing Devices. Cisco's users, customers, agents or other third parties who use those devices in accordance with Cisco's instructions infringe claim 14 of the '891 patent in violation of 35 U.S.C. § 271(a). Cisco intentionally instructs its customers to infringe through training videos, demonstrations, brochures and user guides, such as those located at: www.cisco.com, https://www.youtube.com/watch?v=JR9V_njq5DI, https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/white-paper-c11-737782.pdf, https://www.cisco.com/c/en/us/td/docs/wireless/cmx_cloud/vBLE_SUG/b_cg_Cisco_Beacon_Center/b_cg_Cisco_Beacon_Center_chapter_01.html, https://www.cisco.com/c/en/us/td/docs/wireless/cmx_cloud/vBLE_SUG/b_cg_Cisco_Beacon_Center/b_cg_Cisco_Beacon_Center_chapter_01.html, https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/white-paper-c11-737782.pdf,

https://www.cisco.com/c/en/us/td/docs/wireless/cmx_cloud/vBLE_SUG/b_cg_Cisco_Beacon_Center/b_cg_Cisco_Beacon_Center_chapter_01.html, https://www.cisco.com/c/en/us/td/docs/wireless/cmx_cloud/vBLE_SUG/b_cg_Cisco_Beacon_Center/b_cg_Cisco_Beacon_Center_chapter_01.html, and https://www.cisco.com/c/en/us/td/docs/wireless/cmx_cloud/vBLE_SUG/b_cg_Cisco_Beacon_Center/b_cg_Cisco_Beacon_Center_chapter_01.html. Cisco is thereby liable for infringement of the '891 patent under 35 U.S.C. § 271(b).

29. For example, Cisco published a video on YouTube to encourage its customers to use the Accused Infringing Devices to infringe claim 14 of the '891 patent:

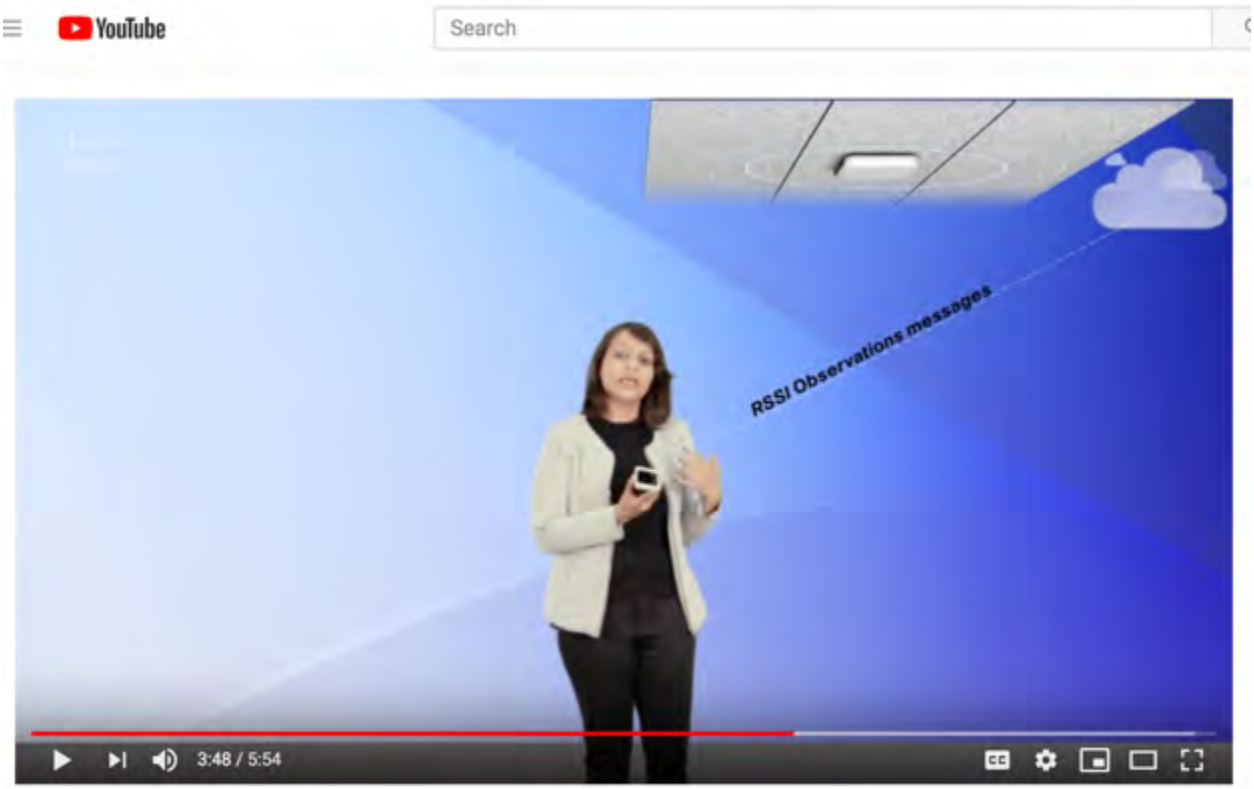


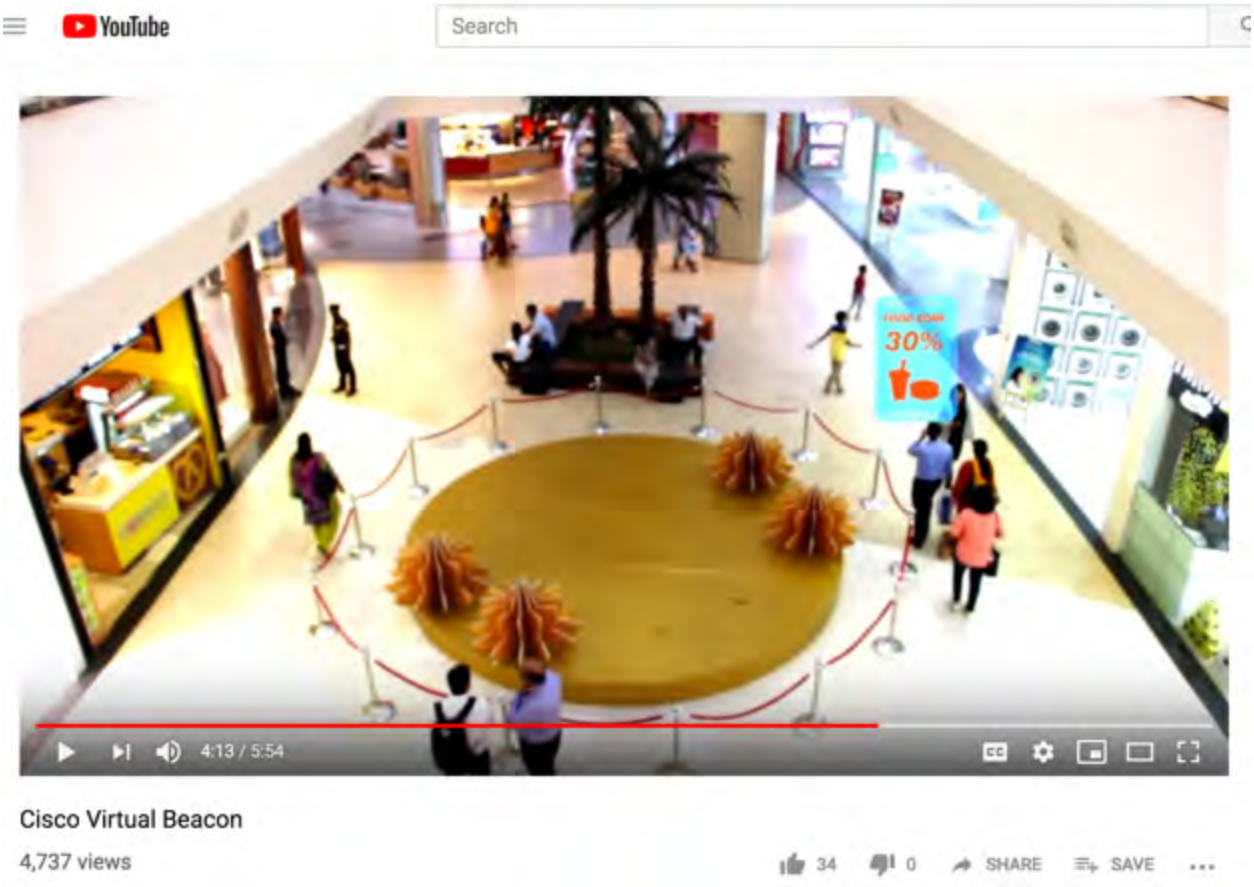


Cisco Virtual Beacon

4,737 views

34 0 SHARE SAVE ...


YouTube
Search
RSSI Observations messages
3:48 / 5:54
Cisco Virtual Beacon
4,737 views
34
0
SHARE
SAVE



https://www.youtube.com/watch?v=JR9V_njq5DI.

30. Cisco also has infringed, and continues to infringe, at least claim 14 of the '891 patent by offering to commercially distribute, commercially distributing, and/or importing the Accused Infringing Devices which devices are used in practicing the processes, or using the systems, of the '891 patent, and constitute a material part of the invention. Cisco knows portions of the Accused Infringing Devices to be especially made or especially adapted for use in infringement of the '891 patent, not a staple article, and not a commodity of commerce suitable for substantial noninfringing use. Cisco is thereby liable for infringement of the '891 patent under 35 U.S.C. § 271(c).

31. Cisco is on notice of its infringement of the '891 patent by no later than September 28, 2018 in a complaint filed in this District detaling Cisco's infringement of the '891

patent. On information and belief, Cisco did not and has not changed its infringing behavior after learning of the infringement allegations. It has not offered to license the '891 patent and has continued its infringement and its inducement of others unabated. On information and belief, since receiving such notice Cisco has known and intended that its continued actions would actively induce and contribute to the infringement of at least claim 14 of the '891 patent. Cisco has had the specific intent to induce and contribute to the infringement of third parties since receiving notice of the '891 patent and has had knowledge of (and/or was willfully blind to) the fact that its actions would induce and/or contribute to the infringement of third parties since receiving notice of the '891 patent. Discovery may prove that Cisco had earlier knowledge of the '891 patent and its infringement of the '891 patent.

32. Upon information and belief, Cisco may have infringed and continues to infringe the '891 patent through other software and devices utilizing the same or reasonably similar functionality, including other versions of the Accused Infringing Devices.

33. Cisco's acts of direct and indirect infringement have caused and continue to cause damage to Uniloc and Uniloc is entitled to recover damages sustained as a result of Cisco's wrongful acts in an amount subject to proof at trial.

COUNT II – INFRINGEMENT OF U.S. PATENT NO. 6,285,892

34. The allegations of paragraphs 1-11 of this Complaint are incorporated by reference as though fully set forth herein.

35. The '892 patent, titled "Data Transmission System For Reducing Terminal Power Consumption In A Wireless Network," issued on September 4, 2001. A copy of the '892 patent is attached as Exhibit B.

36. Pursuant to 35 U.S.C. § 282, the '892 patent is presumed valid.

37. Invented by Philips Electronics North America Corporation, the inventions of the

'892 patent were not well-understood, routine or conventional at the time of the invention. At the time of invention of the '892 patent, power saving features have been incorporated into existing wireless networks, and into wireless asynchronous transfer mode (ATM) networks in particular. '892 patent at 2:29-31. For example, in one conventional system, the base station or the central controller issues a reservation message specifying which wireless terminal is to transmit data to a particular slot, and also which wireless terminal is to receive data from a particular slot. *Id.* at 2:31-34. With this information in hand, the receiving wireless terminals are able to switch between a low-power (i.e., a "power-saving") mode and a higher power (i.e., "data-receiving") mode, during which data from appropriate slots can be received. *Id.* at 2:34-38.

38. While the foregoing conventional systems can result in power conservation in the wireless terminals, those systems also have significant drawbacks. *Id.* at 2:39-41. In particular, they result in an increase in network overhead due to the additional computational effort required on the part of the the base station or the central controller to determine the identities of both the transmitting and receiving wireless terminals. *Id.* at 2:41-44. In addition, since each receiving wireless terminal is switched between modes individually, the reservation message must include switching information for each individual receiving wireless terminals. *Id.* at 2:44-47. Moreover, the additional processing capabilities required to implement the foregoing power-saving scheme, particularly at the wireless terminals, may require additional power, which counters the amount of power actually saved. *Id.* at 2:55-63. Furthermore, there may be problems with controlling the receiving wireless terminals. *Id.* at 2:63-3:2.

39. The inventive solution of the claimed inventions of the '892 patent provides a system and method whereby various ways of switching specific sets of wireless terminals between a low-power mode, during which relatively little power is consumed, and a data-

receiving mode, during which power sufficient to receive and/or process data is consumed. *Id.* at 3:9-14. By switching the wireless in sets, rather than individually as in the prior art, the invention is able to reduce the amount of overhead in the base station or the central controller, the transmitting wirelss terminals, and/or the receiving wireless terminals. *Id.* at 3:14-17.

40. According to one aspect, the present invention is a system (e.g., a method, an apparatus, and computer-executable process steps) for transmitting data among plural wireless terminals in a wireless network. *Id.* at 3:18-21. In this system, the base station or the central controller identifies a transmitter and a set of receivers among the plural wireless terminals (e.g., by examining a message from the transmitter which includes that information). *Id.* at 3:21-24. The base station or the central controller then issues a message to the transmitter and to the set of receivers, the message identifying the transmitter, the set of receivers, and a transmission time at which the transmitter transmits the data to the set of receivers. *Id.* at 3:24-28. At the transmission time, (i) the transmitter transmits the data to the set of receivers identified in the message, and (ii) the set of receivers switch from a low-power mode to a data-receiving mode in order to receive the data from the transmitter identified in the message. *Id.* at 3:28-34.

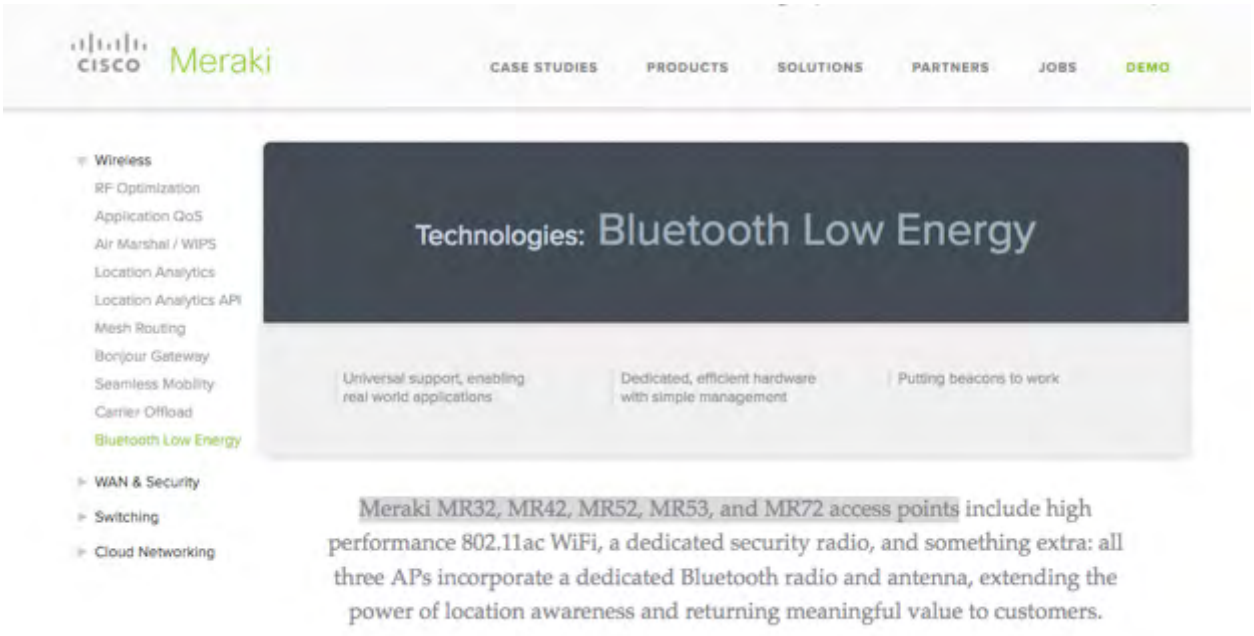
41. A person of ordinary skill in the art reading the ’892 patent and its claims would understand that the patent’s disclosure and claims are drawn to solving a specific, technical problem arising in reducing power consumption of networked wireless terminals. Moreover, a person of ordinary skill in the art would understand that the claimed subject matter of the ’892 patent presents advancements in the field of wireless ATM networks. And, as detailed by the specification, the prior power saving features suffered drawbacks such that a new and novel communications system was required.

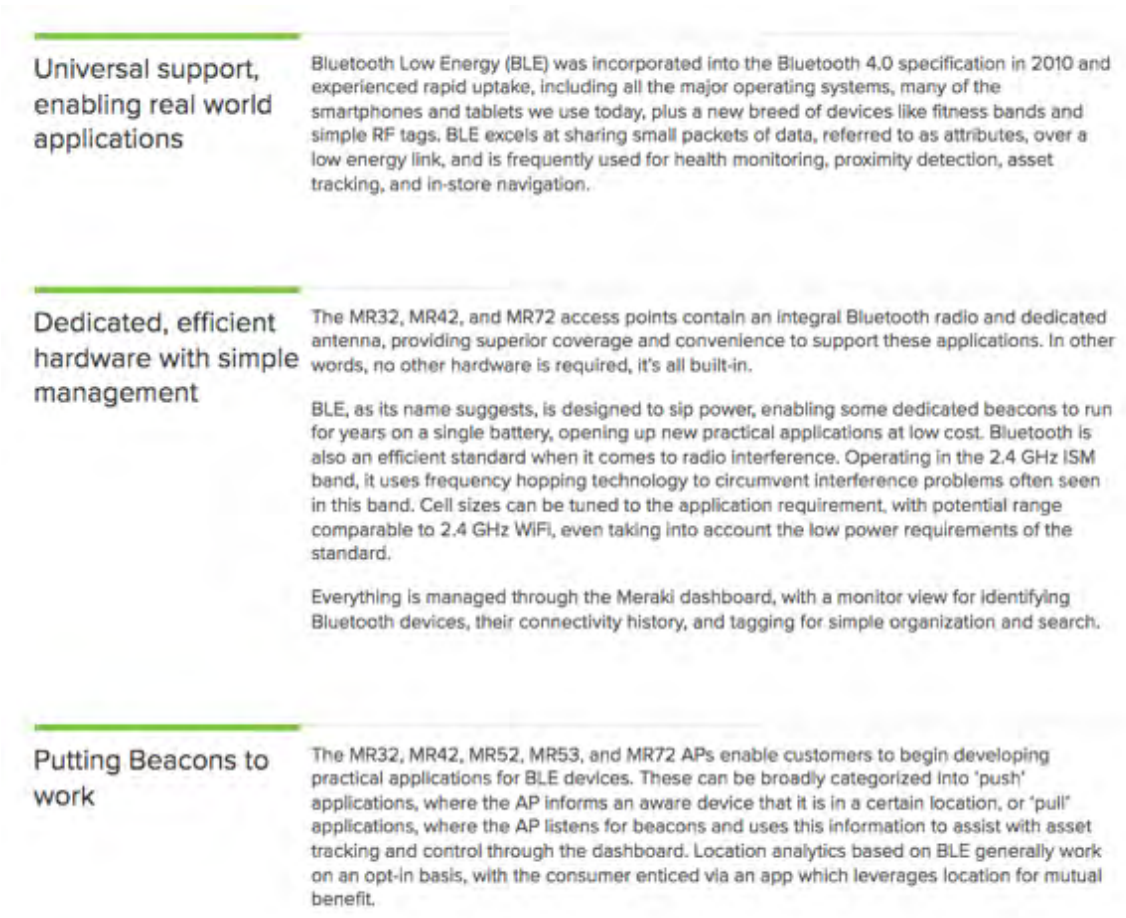
42. On information and belief, Cisco makes, uses, offers for sale, and/or sells in the United States and imports into the United States Meraki Bluetooth Low Energy (“BLE”)

solutions that include BLE enabled hardware and software that incorporate and implement BLE technology, including MR32, MR42, MR52, MR53, MR72, Meraki dashboard and Meraki Location Analytics API (collectively the "Accused Infringing Devices").

43. Upon information and belief, the Accused Infringing Devices infringe at least claim 1 in the exemplary manner described below.

44. The Accused Infringing Devices practice the method of transmitting data among plural terminals in a wireless network.





Universal support, enabling real world applications

Bluetooth Low Energy (BLE) was incorporated into the Bluetooth 4.0 specification in 2010 and experienced rapid uptake, including all the major operating systems, many of the smartphones and tablets we use today, plus a new breed of devices like fitness bands and simple RF tags. BLE excels at sharing small packets of data, referred to as attributes, over a low energy link, and is frequently used for health monitoring, proximity detection, asset tracking, and in-store navigation.

Dedicated, efficient hardware with simple management

The MR32, MR42, and MR72 access points contain an integral Bluetooth radio and dedicated antenna, providing superior coverage and convenience to support these applications. In other words, no other hardware is required, it's all built-in.

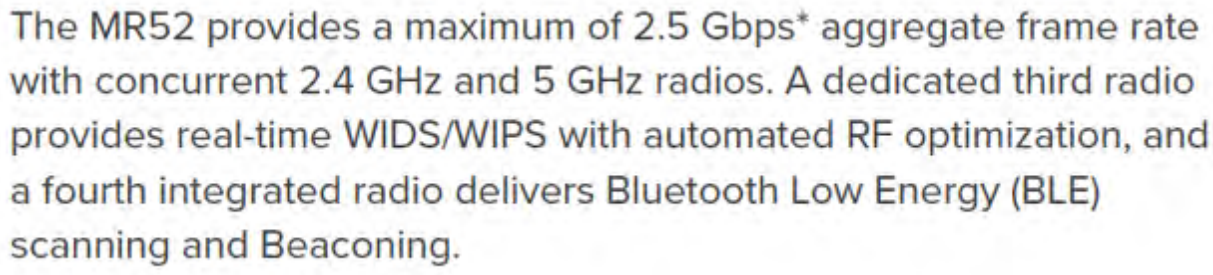
BLE, as its name suggests, is designed to sip power, enabling some dedicated beacons to run for years on a single battery, opening up new practical applications at low cost. Bluetooth is also an efficient standard when it comes to radio interference. Operating in the 2.4 GHz ISM band, it uses frequency hopping technology to circumvent interference problems often seen in this band. Cell sizes can be tuned to the application requirement, with potential range comparable to 2.4 GHz WiFi, even taking into account the low power requirements of the standard.

Everything is managed through the Meraki dashboard, with a monitor view for identifying Bluetooth devices, their connectivity history, and tagging for simple organization and search.

Putting Beacons to work

The MR32, MR42, MR52, MR53, and MR72 APs enable customers to begin developing practical applications for BLE devices. These can be broadly categorized into 'push' applications, where the AP informs an aware device that it is in a certain location, or 'pull' applications, where the AP listens for beacons and uses this information to assist with asset tracking and control through the dashboard. Location analytics based on BLE generally work on an opt-in basis, with the consumer enticed via an app which leverages location for mutual benefit.

Source: https://meraki.cisco.com/technologies/bluetooth-low-energy?dtid=osscdc000283



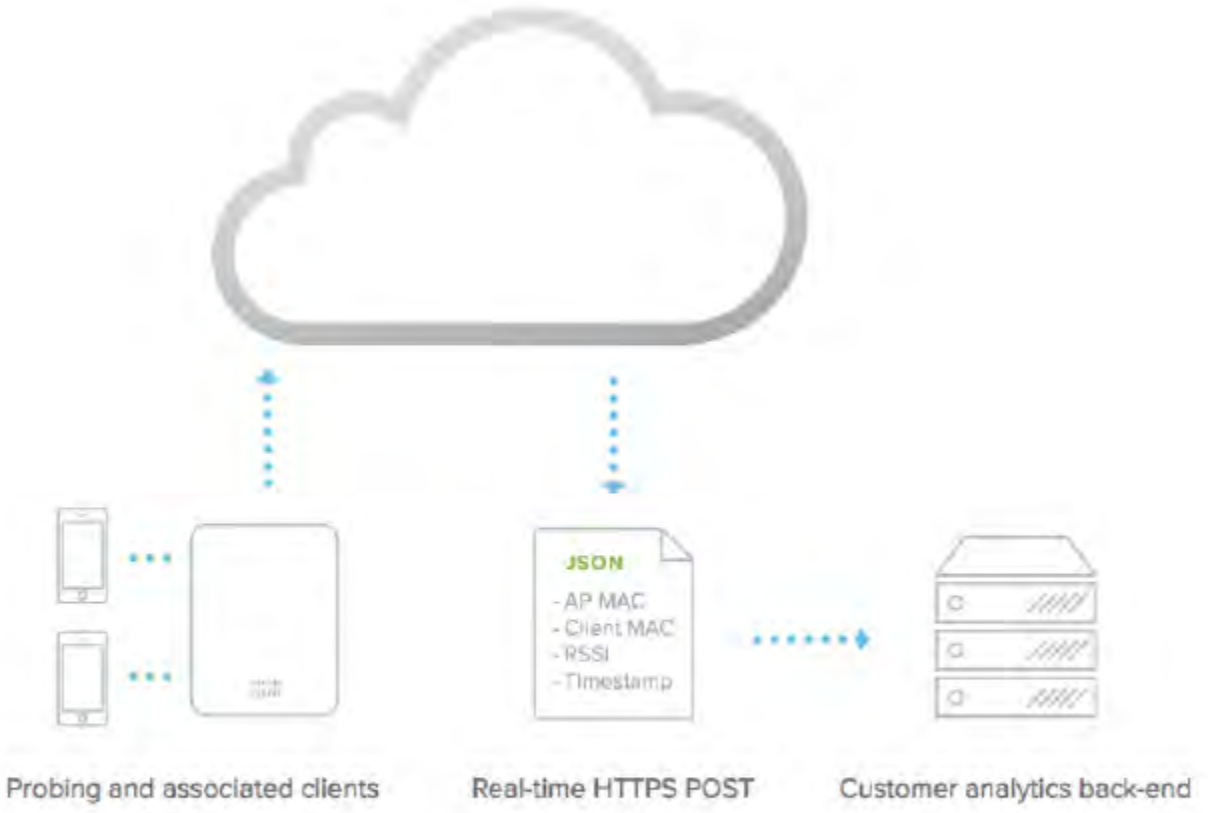
The MR52 provides a maximum of 2.5 Gbps* aggregate frame rate with concurrent 2.4 GHz and 5 GHz radios. A dedicated third radio provides real-time WIDS/WIPS with automated RF optimization, and a fourth integrated radio delivers Bluetooth Low Energy (BLE) scanning and Beaconing.

Source: Cisco Meraki MR52 Datasheet, p. 1.

Bluetooth Low Energy Beacon and scanning radio

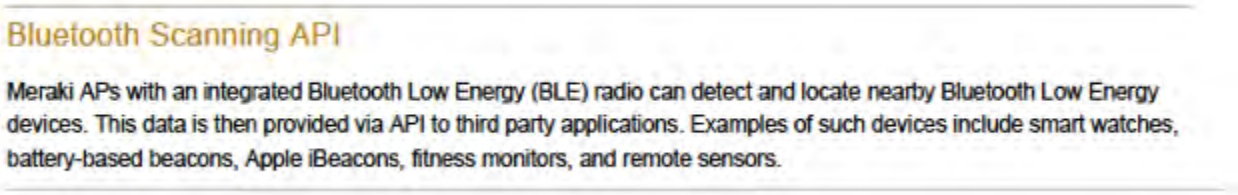
An integrated fourth radio for Bluetooth Low Energy (BLE) provides seamless deployment of BLE Beacon functionality and effortless visibility of BLE devices. The MR52 enables the next generation of location-aware applications while futureproofing your deployment, ensuring it's ready for any new customer engagement strategies.

Source: Cisco Meraki MR52 Datasheet, p. 1.



The Scanning API delivers data in real-time from the Meraki cloud and can be used to detect WiFi (associated and non-associated) and Bluetooth Low Energy (BLE) devices in real-time. The elements are exported via an HTTP POST of JSON data to a specified destination server. The raw data is aggregated from all access points within a network on the Meraki cloud, and sent directly from the cloud to an organization's data warehouse or business intelligence center. The JSON posts occur frequently, typically batched every minute for each AP.

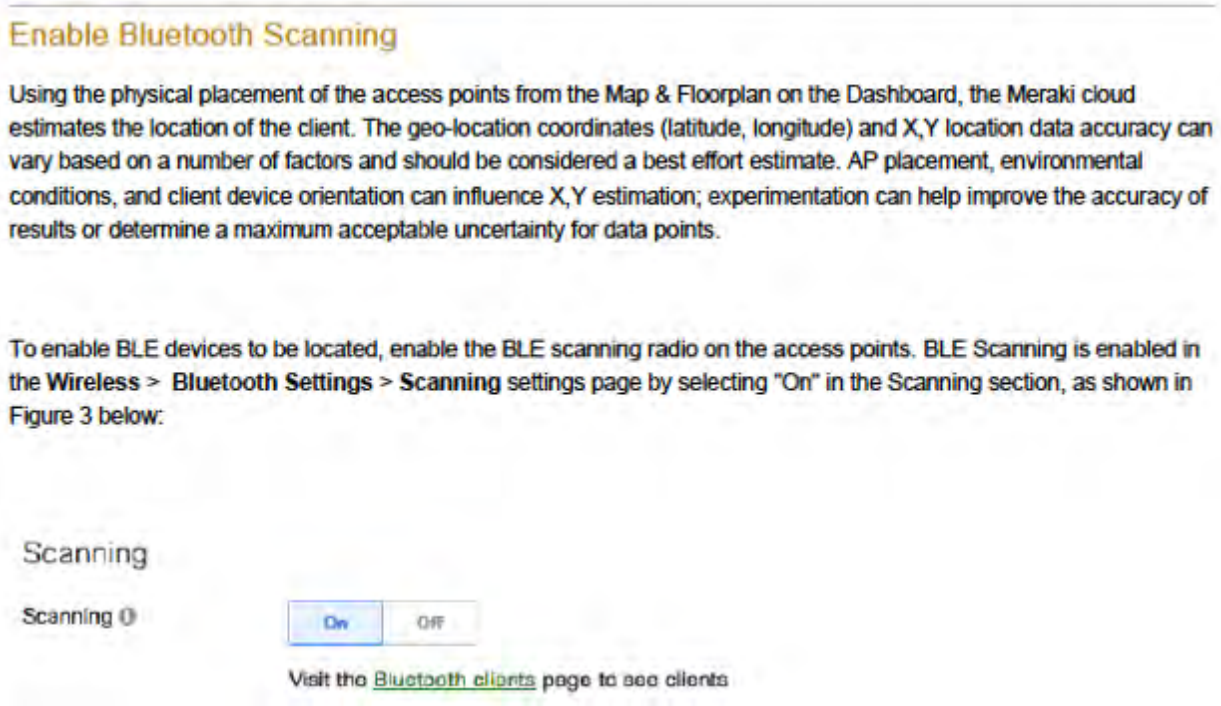
Source: Cisco Meraki Location Analytics Whitepaper, p. 13.



Bluetooth Scanning API

Meraki APs with an integrated Bluetooth Low Energy (BLE) radio can detect and locate nearby Bluetooth Low Energy devices. This data is then provided via API to third party applications. Examples of such devices include smart watches, battery-based beacons, Apple iBeacons, fitness monitors, and remote sensors.

Source: Cisco Meraki Location Analytics Whitepaper, p. 16.



Enable Bluetooth Scanning

Using the physical placement of the access points from the Map & Floorplan on the Dashboard, the Meraki cloud estimates the location of the client. The geo-location coordinates (latitude, longitude) and X,Y location data accuracy can vary based on a number of factors and should be considered a best effort estimate. AP placement, environmental conditions, and client device orientation can influence X,Y estimation; experimentation can help improve the accuracy of results or determine a maximum acceptable uncertainty for data points.

To enable BLE devices to be located, enable the BLE scanning radio on the access points. BLE Scanning is enabled in the **Wireless** > **Bluetooth Settings** > **Scanning** settings page by selecting "On" in the Scanning section, as shown in Figure 3 below:

Scanning

Scanning

On Off

Visit the Bluetooth clients page to see clients

Source: Cisco Meraki Location Analytics Whitepaper, p. 17.

45. A BLE network allows communication among multiple devices over a wireless communication link operating in the unlicensed ISM band at 2.4GHz. The physical channel in BLE network is sub-divided into time units known as events. Data is transmitted between LE devices in packets that are positioned in these events. There are two types of events: Advertising and Connection events. The devices communicating in Advertising events are classified as Advertisers and Scanners. The devices communicating in Connection events are classified as Masters and Slaves.

1.2 OVERVIEW OF BLUETOOTH LOW ENERGY OPERATION

Like the BR/EDR radio, the LE radio operates in the unlicensed 2.4 GHz ISM band. The LE system employs a frequency hopping transceiver to combat interference and fading and provides many FHSS carriers. LE radio operation uses a shaped, binary frequency modulation to minimize transceiver complexity. The symbol rate is 1 Megasymbol per second (Ms/s) supporting the bit rate of 1 Megabit per second (Mb/s).

Source: Specification of the Bluetooth System, v4.0, Page 126

Bluetooth	Bluetooth is a wireless communication link, operating in the unlicensed ISM band at 2.4 GHz using a frequency hopping transceiver. It allows real-time AV and data communications between Bluetooth Hosts. The link protocol is based on time slots.

Source: Specification of the Bluetooth System, v4.0, Page 130

4.1.2 LE Topology

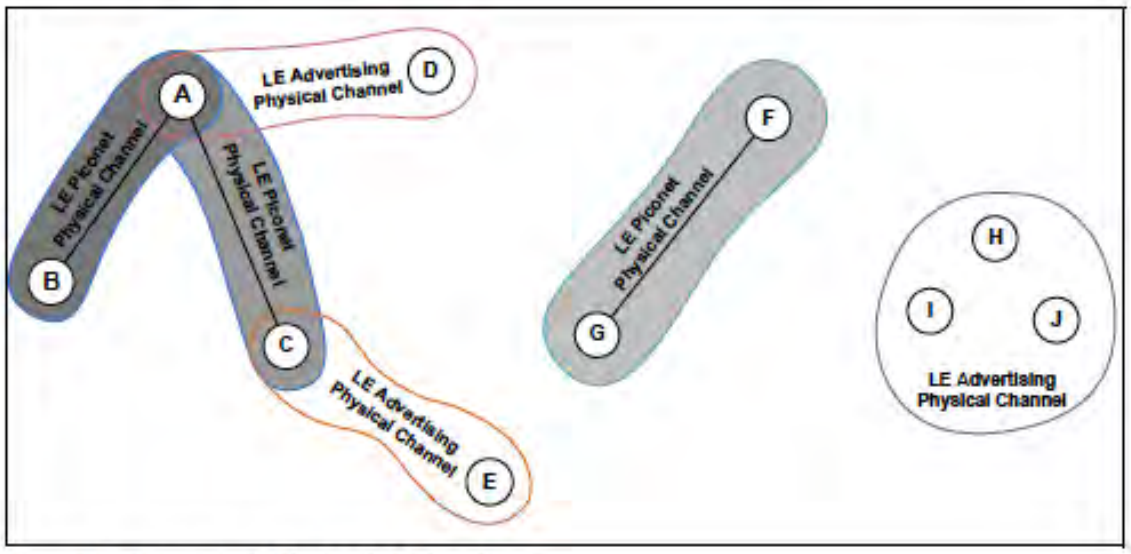


Figure 4.2: Example of Bluetooth LE topology

Source: Specification of the Bluetooth System, v4.0, Page 181

> The physical channel is sub-divided into time units known as events. Data is transmitted between LE devices in packets that are positioned in these events. There are two types of events: Advertising and Connection events.
>
> Devices that transmit advertising packets on the advertising PHY channels are referred to as **advertisers**. Devices that receive advertising on the advertising channels without the intention to connect to the advertising device are referred to as **scanners**. Transmissions on the advertising PHY channels occur in

Source: Specification of the Bluetooth System, v4.0, Page 126

> Devices that need to form a connection to another device listen for connectable advertising packets. Such devices are referred to as **initiators**. If the advertiser is using a connectable advertising event, an initiator may make a connection request using the same advertising PHY channel on which it received the connectable advertising packet. The advertising event is ended and connection events begin if the advertiser receives and accepts the request for a connection be initiated. Once a connection is established, the initiator becomes the **master** device in what is referred to as a **piconet** and the advertising device becomes the **slave** device. Connection events are used to send data packets between the master and slave devices. In connection events, channel hopping occurs at the start of each connection event. Within a connection event, the master and slave alternate sending data packets using the same data PHY channel. The master initiates the beginning of each connection event and can end each connection event at any time.

Source: Specification of the Bluetooth System, v4.0, Page 127
See also, Specification of the Bluetooth System, v5.0, Pages 173, 169-172, 228-229, 234-238

46. The Accused Infringing Devices designate at least one of the plural terminals as a transmitter for outputting data to the wireless network. For example, in a BLE network, the Advertiser is designated as a transmitter for outputting advertising packets to the Scanners in the network. Also, the Master device and the Slave devices transmit data packets to each other in Connection event of a piconet.

4.1.2 LE Topology

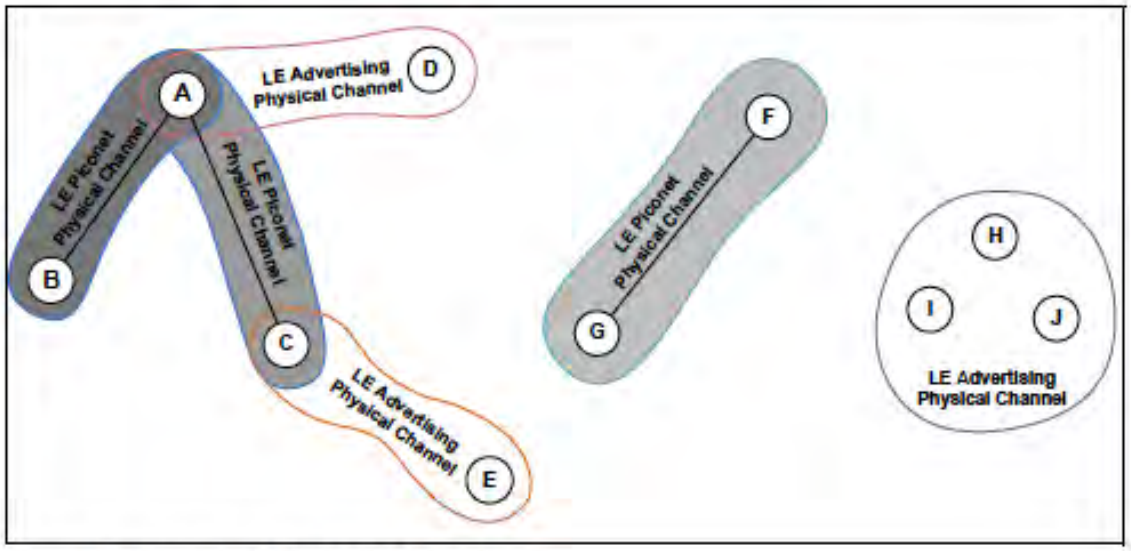


Figure 4.2: Example of Bluetooth LE topology

Source: Specification of the Bluetooth System, v4.0, Page 181

The physical channel is sub-divided into time units known as events. Data is transmitted between LE devices in packets that are positioned in these events. There are two types of events: Advertising and Connection events.

Devices that transmit advertising packets on the advertising PHY channels are referred to as **advertisers**. Devices that receive advertising on the advertising channels without the intention to connect to the advertising device are referred to as **scanners**. Transmissions on the advertising PHY channels occur in

Source: Specification of the Bluetooth System, v4.0, Page 126

> Devices that need to form a connection to another device listen for connectable advertising packets. Such devices are referred to as **initiators**. If the advertiser is using a connectable advertising event, an initiator may make a connection request using the same advertising PHY channel on which it received the connectable advertising packet. The advertising event is ended and connection events begin if the advertiser receives and accepts the request for a connection be initiated. Once a connection is established, the initiator becomes the **master** device in what is referred to as a **piconet** and the advertising device becomes the **slave** device. Connection events are used to send data packets between the master and slave devices. In connection events, channel hopping occurs at the start of each connection event. Within a connection event, the master and slave alternate sending data packets using the same data PHY channel. The master initiates the beginning of each connection event and can end each connection event at any time.

Source: Specification of the Bluetooth System, v4.0, Page 127
See also, Exhibit B - Specification of the Bluetooth System, v5.0, Pages 169-172, 228-229, 234-238.

47. The Accused Infringing Devices designate a set of the plural terminals as able to receive data output to the wireless network by the transmitter. For example, when an advertising device begins advertising, it transmits broadcast control and user data to all scanning devices within close distance in the BLE network (which are plural terminals) over an LE Advertising Broadcast (ADVB) logical transport.

> ***3.5.4.7 LE Advertising Broadcast (ADVB)***
>
> The LE advertising broadcast logical transport is used to transport broadcast control and user data to all scanning devices in a given area. There is no acknowledgment protocol and the traffic is predominately unidirectional from the advertising device. A scanning device can send requests over the logical transport to get additional broadcast user data, or to form an LE ACL logical transport connection. The LE Advertising Broadcast logical transport data is carried only over the LE advertising broadcast link.
>
> The ADVB logical transport is inherently unreliable because of the lack of acknowledgment. To improve the reliability, each packet is transmitted a number of times over the LE advertising broadcast link.
>
> An ADVB is created whenever an advertising device begins advertising. The ADVB logical transport is identified by the advertiser's Bluetooth device address and advertising set.

Source: Specification of the Bluetooth System, v4.0, Page 221
See also, Exhibit B - Specification of the Bluetooth System, v5.0, Pages 221-222.

48. The Accused Infringing Devices issue a first message to the plural terminals identifying the transmitter and the set of plural terminals. For example, when an advertising device begins advertising, it transmits broadcast control and user data to all scanning devices within close distance in the BLE network, over an LE Advertising Broadcast (ADVB) logical transport. The control data and user data are carried in different messages over Advertising Broadcast Control Logical Link (ADVB-C) and Advertising Broadcast User Data Logical Link (ADVB-U), respectively.

3.5.5.2.3 Advertising Broadcast Control Logical Link (ADVB-C)

The LE Advertising Broadcast Control Logical Link (ADVB-C) is used to carry LE LL signaling between unconnected devices in a given area. This signaling is the control commands for gathering additional broadcast user data (scan requests) or connection requests. The control link is only carried on the default LE Advertising Broadcast logical transport.

3.5.5.2.4 Advertising Broadcast User Data Logical Link (ADVB-U)

The LE Advertising Broadcast User Data Logical Link (ADVB-U) is used to carry LE advertisement broadcast user data used between devices without the need for a connection or LE-U between the devices. The user data link is only carried on the default LE Advertising Broadcast logical transport.

Source: Specification of the Bluetooth System, v4.0, Page 177

Broadcast links have no feedback route, and are unable to use the acknowledgement scheme (although the receiver is still able to detect errors in received packets.) Instead, each packet is transmitted several times to increase the probability that the receiver is able to receive at least one of the copies successfully. Despite this approach there are still no guarantees of successful receipt, and so these links are considered unreliable.

Source: Specification of the Bluetooth System, v4.0, Page 150

49. The Advertising Broadcast (ADVB) control and data messages transmitted by an Advertiser to multiple scanning devices conform to the BLE generic packet structure, which include a PDU (Packet Data Unit) header. The PDU header for an ADVB message contains the

advertiser's address which identifies the transmitter. The PDU type for an ADVB message identifies the scanning devices within close distance in the BLE network.

3.2.2 LE Generic Packet Structure

The general structure of the link layer air interface packet closely reflects the architectural layers found in the LE system. The LE packet structure is designed for optimal use in normal operation. It is shown in Figure 3.5.

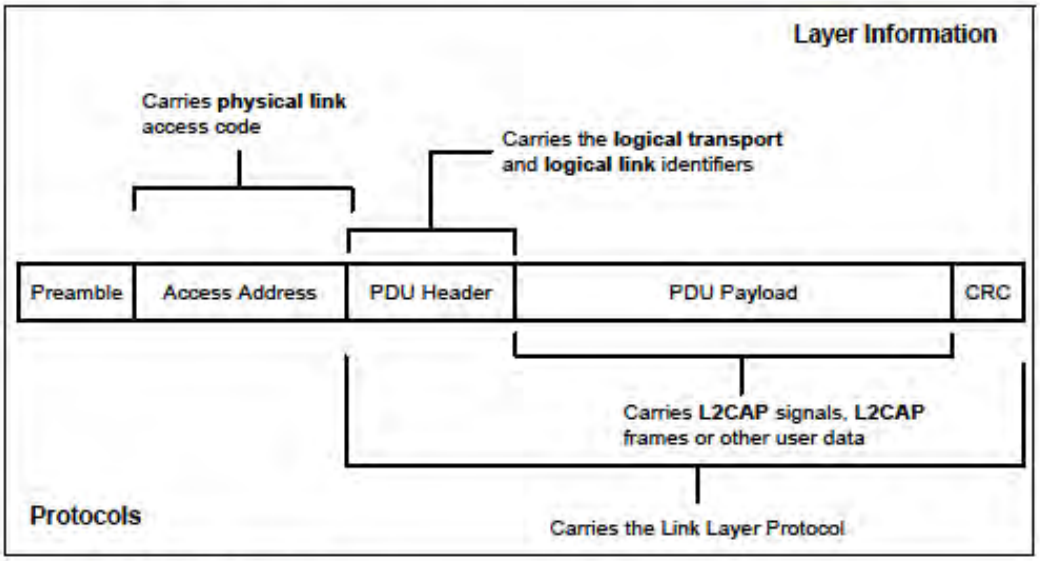


Figure 3.5: LE packet structure

All LE packets include a PDU header. The PDU header determines the type of advertisement broadcast or logical link carried over the physical channel.

For advertising channel PDUs, the PDU header contains the type of advertisement payload, the device address type for addresses contained in the advertisement and advertising channel PDU payload length. Most advertising channel PDU payloads contain the advertiser's address and advertising data. One advertising channel PDU payload only contains the advertiser's device address and the initiator's device address in which the advertisement is directed. Advertising channel PDUs with scan requests payloads contain the scanner's device address and the advertiser's device address. Advertising channel PDUs with scan responses contain advertiser's device address and the scan response data. Advertising channel PDUs with connection request payloads contain the initiator's device address, advertiser's device address and connection setup parameters.

Source: Specification of the Bluetooth System, v4.0, Pages 153-154.

2.3 ADVERTISING CHANNEL PDU

The advertising channel PDU has a 16-bit header and a variable size payload. Its format is as shown in Figure 2.2. The 16 bit Header field of the advertising channel PDU is as shown in Figure 2.3.

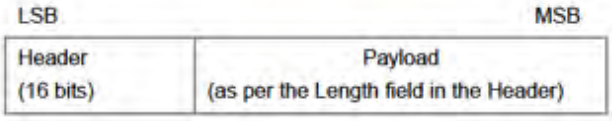


Figure 2.2: Advertising channel PDU

Source: Specification of the Bluetooth System, v4.0, Page 2201.

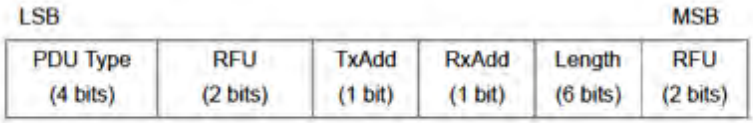


Figure 2.3: Advertising channel PDU Header

The PDU Type field of the advertising channel PDU that is contained in the header indicates the PDU type as defined in Table 2.1.

Source: Specification of the Bluetooth System, v4.0, Page 2202.

PDU Type $b_3b_2b_1b_0$	Packet Name
0000	ADV_IND
0001	ADV_DIRECT_IND
0010	ADV_NONCONN_IND
0011	SCAN_REQ
0100	SCAN_RSP
0101	CONNECT_REQ
0110	ADV_SCAN_IND
0111-1111	Reserved

Table 2.1: Advertising channel PDU Header's PDU Type field encoding

Source: Specification of the Bluetooth System, v4.0, Page 2303.

50. Out of all the possible values for the PDU Type field in Advertising Channel PDU header, at least the ADV_IND value with a bit pattern of "0000," the ADV_NONCONN_IND value with a bit pattern of 0010, and the ADV_SCAN_IND value with a bit pattern of "0110," indicate that the Advertising Channel PDU is a one-to-many Advertising Channel PDU destined for all the scanning devices within close distance of the advertising device in the BLE network. The Advertising device's address "AdvA" is identified at the beginning of the Payload of these three types of Advertising Channel PDUs.

2.3.1.1 ADV_IND

The ADV_IND PDU has the Payload as shown in Figure 2.4. The PDU shall be used in connectable undirected advertising events. The TxAdd in the Flags field indicates whether the advertiser's address in the AdvA field is public (TxAdd = 0) or random (TxAdd = 1).

Payload	
AdvA (6 octets)	AdvData (0-31 octets)

Figure 2.4: ADV_IND PDU Payload

The Payload field consists of AdvA and AdvData fields. The AdvA field shall contain the advertiser's public or random device address as indicated by

Source: Specification of the Bluetooth System, v4.0, Pages 2303-2304.

2.3.1.3 ADV_NONCONN_IND

The ADV_NONCONN_IND PDU has the Payload as shown in Figure 2.6. The PDU shall be used in non-connectable undirected advertising events. The TxAdd in the Flags field indicates whether the advertiser's address in the AdvA field is public (TxAdd = 0) or random (TxAdd = 1).

Payload	
AdvA (6 octets)	AdvData (0-31 octets)

Figure 2.6: ADV_NONCONN_IND PDU Payload

The Payload field consists of AdvA and AdvData fields. The AdvA field shall contain the advertiser's public or random device address as indicated by TxAdd. The AdvData field may contain Advertising Data from the advertiser's Host.

Source: Specification of the Bluetooth System, v4.0, Page 2304.

2.3.1.4 ADV_SCAN_IND[1]

The ADV_SCAN_IND PDU has the Payload as shown in Figure 2.7. The PDU shall be used in scannable undirected advertising events. The TxAdd in the Flags field indicates whether the advertiser's address in the AdvA field is public (TxAdd = 0) or random (TxAdd = 1).

Payload	
AdvA (6 octets)	AdvData (0-31 octets)

Figure 2.7: ADV_SCAN_IND PDU Payload

The Payload field consists of AdvA and AdvData fields. The AdvA field shall contain the advertiser's public or random device address as indicated by TxAdd. The AdvData field may contain Advertising Data from the advertiser's Host.

Source: Specification of the Bluetooth System, v4.0, Page 2305.
See also, Specification of the Bluetooth System, v5.0, Pages 197-199, 221-222, 224, 2566-2575.

51. The Accused Infringing Devices receive a request for transmission from the transmitter. A BLE network implements many requests for transmission from the transmitting devices. For example, an advertising device sends a request to an Attribute Protocol (ATT) server device to understand the properties of the receiving device. As another example, Bluetooth LE Advertising Broadcast Control Logical Link (ADVB-C) is used to carry LE Link Layer (LL) signaling that includes scan requests and connection requests.

2.1.1.4 Attribute Protocol

The Attribute Protocol (ATT) block implements the peer-to-peer protocol between an attribute server and an attribute client. The ATT client communicates with an ATT server on a remote device over a dedicated fixed L2CAP channel. The ATT client sends commands, requests, and confirmations to the ATT server. The ATT server sends responses, notifications and indications to the client. These ATT client commands and requests provide a means to read and write values of attributes on a peer device with an ATT server.

Source: Specification of the Bluetooth System, v4.0, Page 141.

3.5.5.2.3 Advertising Broadcast Control Logical Link (ADVB-C)

The LE Advertising Broadcast Control Logical Link (ADVB-C) is used to carry LE LL signaling between unconnected devices in a given area. This signaling is the control commands for gathering additional broadcast user data (scan requests) or connection requests. The control link is only carried on the default LE Advertising Broadcast logical transport.

Source: Specification of the Bluetooth System, v4.0, Page 177.

Advertising devices may receive scan requests from listening devices in order to get additional user data from the advertising device. Scan responses are sent by the advertising device to the device making the scan request over the same advertising physical channel. Whereas the broadcast user data sent as part of the advertising packets is typically dynamic in nature, scan response data is generally static in nature.

Source: Specification of the Bluetooth System, v4.0, Page 187.

An advertising device may receive connection requests from initiator devices on the advertising broadcast physical channel. If the advertising device was using a connectable advertising event and the initiating device is not being filtered by the device filtering procedure, the advertising device ceases advertising and enters the connected mode. The device can begin advertising again after it is in the connected mode but it can only use non-connected advertising events.

Source: Specification of the Bluetooth System, v4.0, Page 187**.**
See also, Specification of the Bluetooth System, v5.0, Pages 184, 199, 209, 224.

52. The Accused Infringing Devices issue a second message to the plural terminals that identifies the transmitter. For example, when an advertising device begins advertising, it transmits broadcast control and user data to all scanning devices within close distance in the BLE network, over an LE Advertising Broadcast (ADVB) logical transport. The control data and user data are carried in different messages over Advertising Broadcast Control Logical Link (ADVB-C) and Advertising Broadcast User Data Logical Link (ADVB-U), respectively. Furthermore, since the broadcast links have no feedback route for an acknowledgement message or an error message to be returned to the transmitter, each control and data packet is repeated in several messages to increase the probability of its delivery.

3.5.5.2.3 Advertising Broadcast Control Logical Link (ADVB-C)

The LE Advertising Broadcast Control Logical Link (ADVB-C) is used to carry LE LL signaling between unconnected devices in a given area. This signaling is the control commands for gathering additional broadcast user data (scan requests) or connection requests. The control link is only carried on the default LE Advertising Broadcast logical transport.

3.5.5.2.4 Advertising Broadcast User Data Logical Link (ADVB-U)

The LE Advertising Broadcast User Data Logical Link (ADVB-U) is used to carry LE advertisement broadcast user data used between devices without the need for a connection or LE-U between the devices. The user data link is only carried on the default LE Advertising Broadcast logical transport.

Source: Exhibit A - Specification of the Bluetooth System, v4.0, Page 177

Broadcast links have no feedback route, and are unable to use the acknowledgement scheme (although the receiver is still able to detect errors in received packets.) Instead, each packet is transmitted several times to increase the probability that the receiver is able to receive at least one of the copies successfully. Despite this approach there are still no guarantees of successful receipt, and so these links are considered unreliable.

Source: Specification of the Bluetooth System, v4.0, Page 150.

53. The Advertising Broadcast (ADVB) control and data messages transmitted by an Advertiser to multiple scanning devices conform to the BLE generic packet structure, which include a PDU (Packet Data Unit) header. The PDU header for an ADVB message contains the advertiser's address which identifies the transmitter. The PDU type for an ADVB message identifies the scanning devices within close distance in the BLE network.

3.2.2 LE Generic Packet Structure

The general structure of the link layer air interface packet closely reflects the architectural layers found in the LE system. The LE packet structure is designed for optimal use in normal operation. It is shown in Figure 3.5.

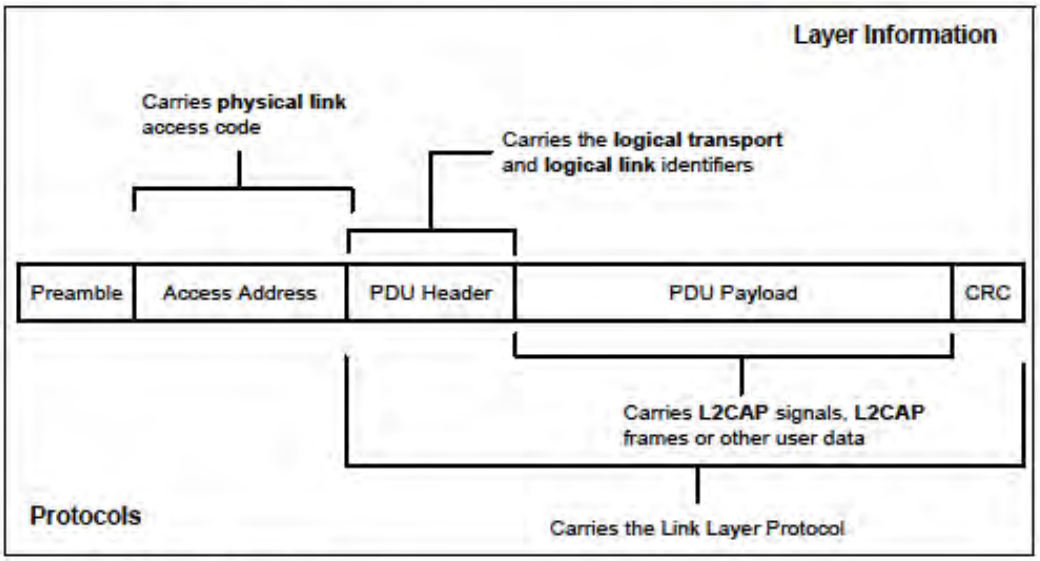


Figure 3.5: LE packet structure

All LE packets include a PDU header. The PDU header determines the type of advertisement broadcast or logical link carried over the physical channel.

For advertising channel PDUs, the PDU header contains the type of advertisement payload, the device address type for addresses contained in the advertisement and advertising channel PDU payload length. Most advertising channel PDU payloads contain the advertiser's address and advertising data. One advertising channel PDU payload only contains the advertiser's device address and the initiator's device address in which the advertisement is directed. Advertising channel PDUs with scan requests payloads contain the scanner's device address and the advertiser's device address. Advertising channel PDUs with scan responses contain advertiser's device address and the scan response data. Advertising channel PDUs with connection request payloads contain the initiator's device address, advertiser's device address and connection setup parameters.

Source: Specification of the Bluetooth System, v4.0, Pages 153-154.

2.3 ADVERTISING CHANNEL PDU

The advertising channel PDU has a 16-bit header and a variable size payload. Its format is as shown in Figure 2.2. The 16 bit Header field of the advertising channel PDU is as shown in Figure 2.3.

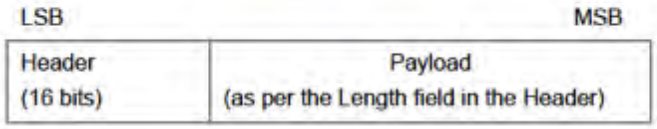


Figure 2.2: Advertising channel PDU

Source: Specification of the Bluetooth System, v4.0, Page 2201.

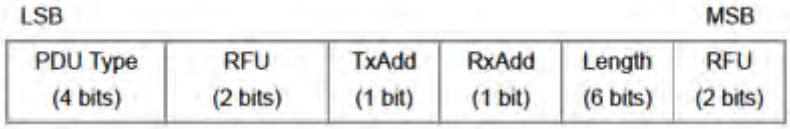


Figure 2.3: Advertising channel PDU Header

The PDU Type field of the advertising channel PDU that is contained in the header indicates the PDU type as defined in Table 2.1.

Source: Specification of the Bluetooth System, v4.0, Page 2202.

PDU Type $b_3b_2b_1b_0$	Packet Name
0000	ADV_IND
0001	ADV_DIRECT_IND
0010	ADV_NONCONN_IND
0011	SCAN_REQ
0100	SCAN_RSP
0101	CONNECT_REQ
0110	ADV_SCAN_IND
0111-1111	Reserved

Table 2.1: Advertising channel PDU Header's PDU Type field encoding

Source: Specification of the Bluetooth System, v4.0, Page 2303.

54. Out of all the possible values for the PDU Type field in Advertising Channel PDU header, at least the ADV_IND value with a bit pattern of "0000," the ADV_NONCONN_IND value with a bit pattern of 0010, and the ADV_SCAN_IND value with a bit pattern of "0110," indicate that the Advertising Channel PDU is a one-to-many Advertising Channel PDU destined for all the scanning devices within close distance of the advertising device in the Bluetooth LE network. The Advertising device's address "AdvA" is identified at the beginning of the Payload of these three types of Advertising Channel PDUs.

2.3.1.1 ADV_IND

The ADV_IND PDU has the Payload as shown in Figure 2.4. The PDU shall be used in connectable undirected advertising events. The TxAdd in the Flags field indicates whether the advertiser's address in the AdvA field is public (TxAdd = 0) or random (TxAdd = 1).

Payload	
AdvA (6 octets)	AdvData (0-31 octets)

Figure 2.4: ADV_IND PDU Payload

The Payload field consists of AdvA and AdvData fields. The AdvA field shall contain the advertiser's public or random device address as indicated by

Source: Specification of the Bluetooth System, v4.0, Pages 2303-2304.

2.3.1.3 ADV_NONCONN_IND

The ADV_NONCONN_IND PDU has the Payload as shown in Figure 2.6. The PDU shall be used in non-connectable undirected advertising events. The TxAdd in the Flags field indicates whether the advertiser's address in the AdvA field is public (TxAdd = 0) or random (TxAdd = 1).

Payload	
AdvA (6 octets)	AdvData (0-31 octets)

Figure 2.6: ADV_NONCONN_IND PDU Payload

The Payload field consists of AdvA and AdvData fields. The AdvA field shall contain the advertiser's public or random device address as indicated by TxAdd. The AdvData field may contain Advertising Data from the advertiser's Host.

Source: Specification of the Bluetooth System, v4.0, Page 2304.

2.3.1.4 ADV_SCAN_IND[1]

The ADV_SCAN_IND PDU has the Payload as shown in Figure 2.7. The PDU shall be used in scannable undirected advertising events. The TxAdd in the Flags field indicates whether the advertiser's address in the AdvA field is public (TxAdd = 0) or random (TxAdd = 1).

Payload	
AdvA (6 octets)	AdvData (0-31 octets)

Figure 2.7: ADV_SCAN_IND PDU Payload

The Payload field consists of AdvA and AdvData fields. The AdvA field shall contain the advertiser's public or random device address as indicated by TxAdd. The AdvData field may contain Advertising Data from the advertiser's Host.

Source: Specification of the Bluetooth System, v4.0, Page 2305.
See also, Specification of the Bluetooth System, v5.0, Pages 197-199, 221-222, 224, 2566-2575.

55. For claim limitations 1(f)-(h), a BLE network implements a device filtering procedure to restrict devices from receiving advertising packets from certain advertising devices. The Link Layer (LL) of the BLE controller in the scanning devices employs a white list that enumerates the remote devices that are allowed to communicate with the local device. When a white list is in effect, transmissions from devices that are in the white list will be allowed and transmissions from devices that are not in the white list will be ignored. This filtering procedure allows the scanning device to enter a low-power mode commonly referred to as a standby state.

4.2.2 LE Procedures

4.2.2.1 Device Filtering Procedure

The device filtering procedure is a method for controllers to reduce the number of devices requiring communication responses. Since it is not required to respond to requests from every device, it reduces the number of transmissions an LE Controller is required to make which reduces power consumption. It also reduces the communication the controller would be required to make with the host. This results in additional power savings since the Host does not have to be involved.

An advertising or scanning device may employ device filtering to restrict the devices in which it receives advertising packets, scan requests or connection requests. In LE, some advertising packets received by a scanning device require that the scanning device send a request to the advertising device. This advertisement can be ignored if device filtering is used and the advertising device is being filtered. A similar situation occurs with connection requests. Connection requests must be responded to by initiators unless a device filter is used to limit the devices the initiator is required to respond. Advertisers can also use device filters to limit the devices in which it will accept a scan request or connection request.

This device filtering is accomplished through the use of a "White List" located in the LL block of the controller. A white list enumerates the remote devices that are allowed to communicate with the local device. When a white list is in effect, transmissions from devices that are not in the white list will be ignored by the

LL. Since device filtering occurs in the LL it can have a significant impact on power consumption by filtering (or ignoring) advertising packets, scan requests or connection requests from being sent to the higher layers for handling.

Source: Specification of the Bluetooth System, v4.0, Pages 186-187.
See also, Specification of the Bluetooth System, v5.0, Page 234.

4.4.1 Standby State

The Standby State is the default state in the Link Layer. The Link Layer shall not send or receive packets in the Standby State. The Link Layer may leave the Standby State to enter the Advertising State, Scanning State or Initiator State.

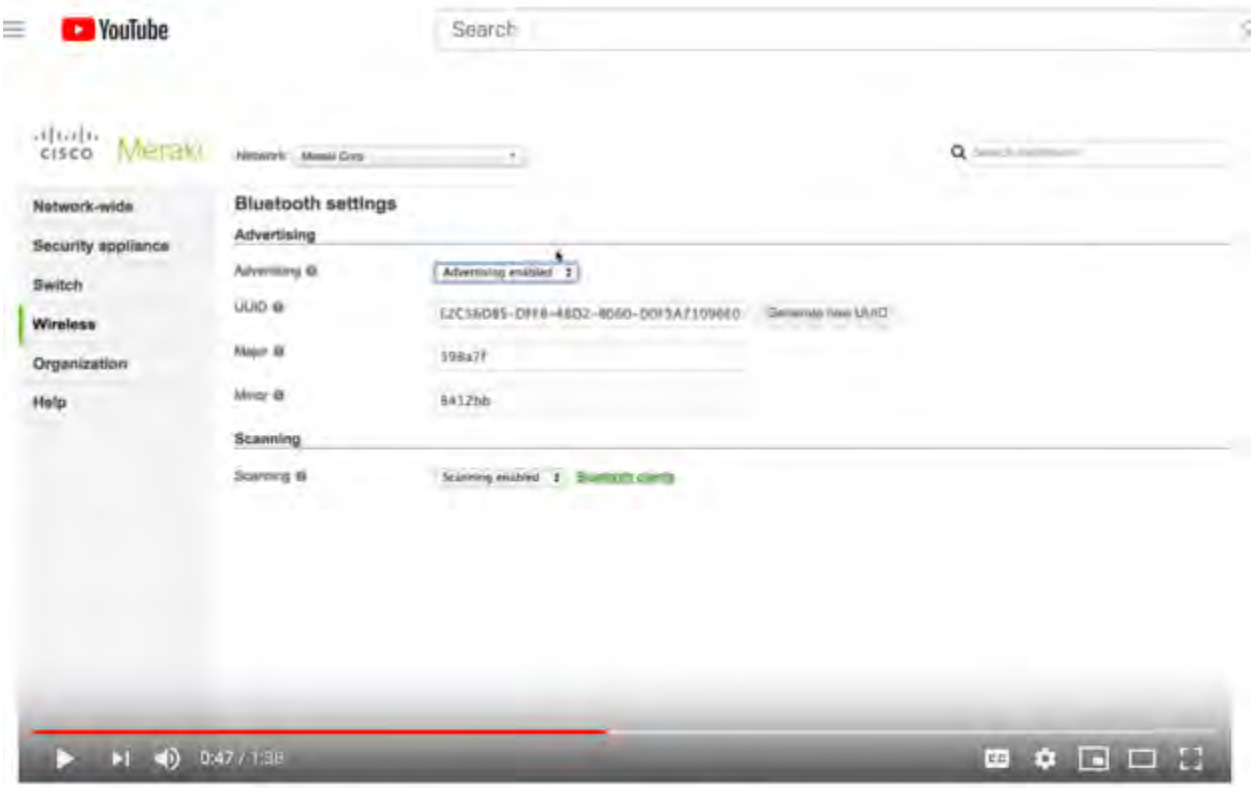
Source: Specification of the Bluetooth System, v4.0, Page 2221.
See also, Specification of the Bluetooth System, v5.0, Pages 234, 2608.

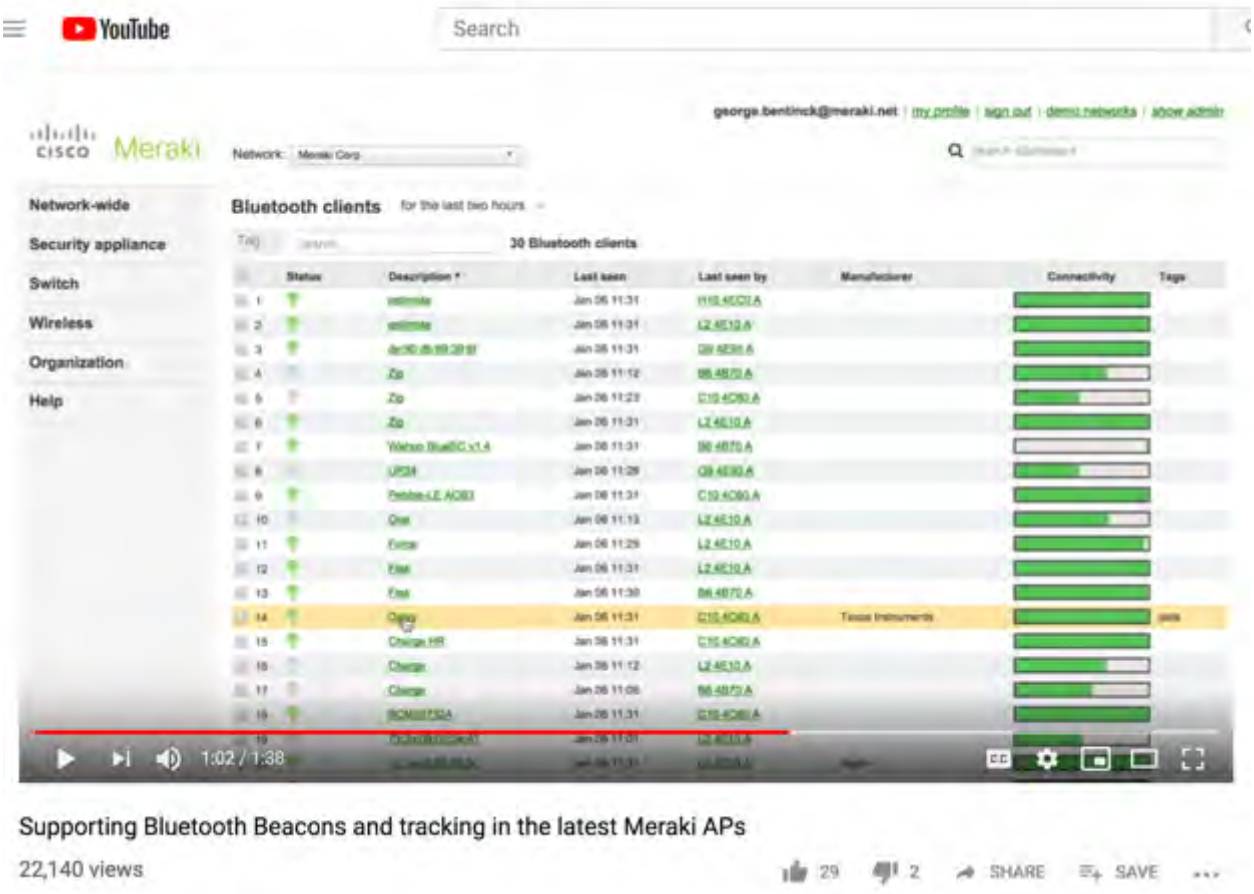
56. Cisco has infringed, and continues to infringe, at least claim 1 of the '892 patent in the United States, by making, using, offering for sale, selling and/or importing the Accused Infringing Devices in violation of 35 U.S.C. § 271(a).

57. Cisco also has infringed, and continues to infringe, at least claim 1 of the '892 patent by actively inducing others to use, offer for sale, and sell the Accused Infringing Devices. Cisco's users, customers, agents or other third parties who use those devices in accordance with Cisco's instructions infringe claim 1 of the '892 patent in violation of 35 U.S.C. § 271(a). Cisco intentionally instructs its customers to infringe through demonstrations, brochures and user guides, such as those located at: https://meraki.cisco.com/, https://www.youtube.com/watch?v=5BWcxO66UQM, https://www.youtube.com/watch?v=XEMno9_pwBw, https://meraki.cisco.com/webinars, https://meraki.cisco.com/technologies/bluetooth-low-energy?dtid=osscdc000283, https://meraki.cisco.com/lib/pdf/meraki_datasheet_location_analytics.pdf, https://meraki.cisco.com/solutions/location_analytics and https://meraki.cisco.com/lib/pdf/meraki_datasheet_MR52.pdf. Cisco is thereby liable for infringement of the '892 patent under 35 U.S.C. § 271(b).

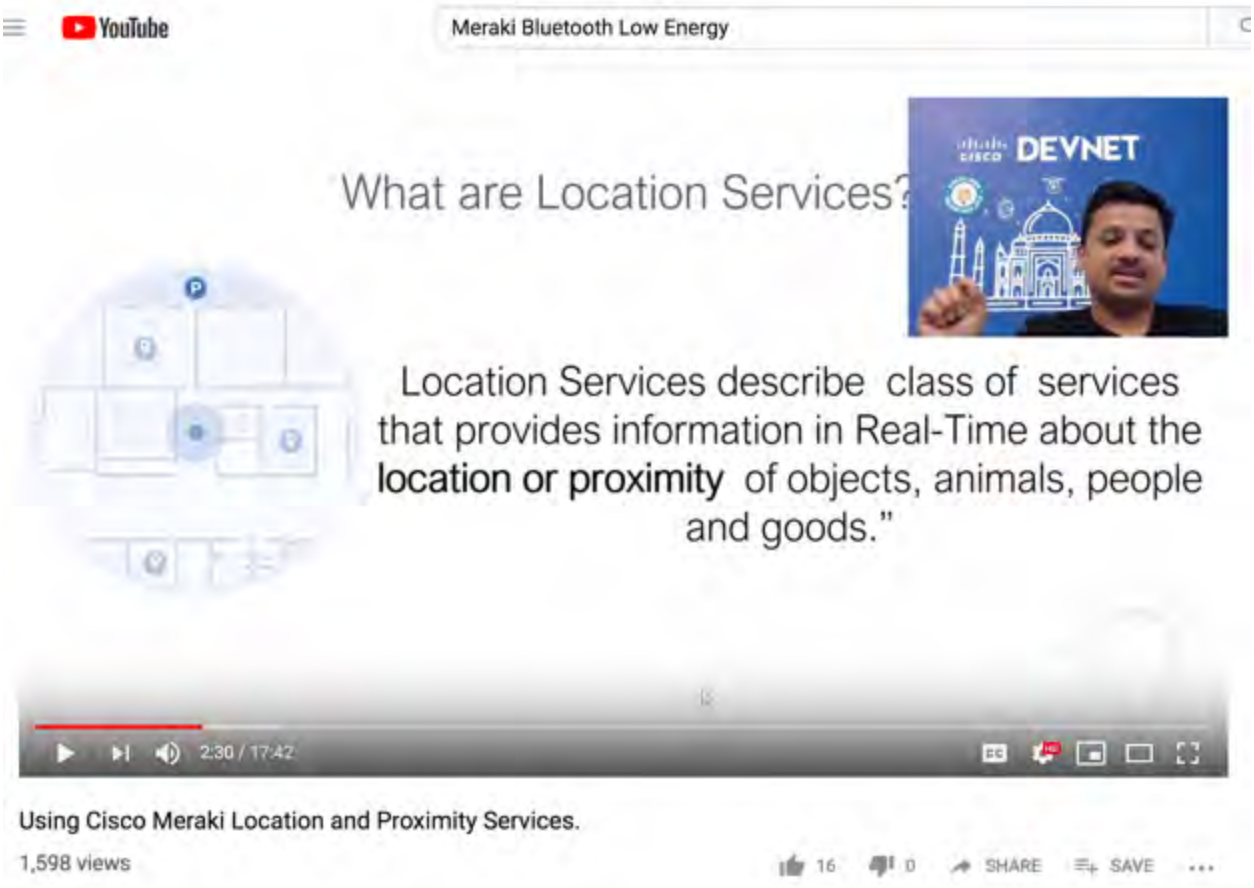
58. For example, Cisco published videos on YouTube to encourage its customers to use the Accused Infringing Devices to infringe claim 1 of the '892 patent:

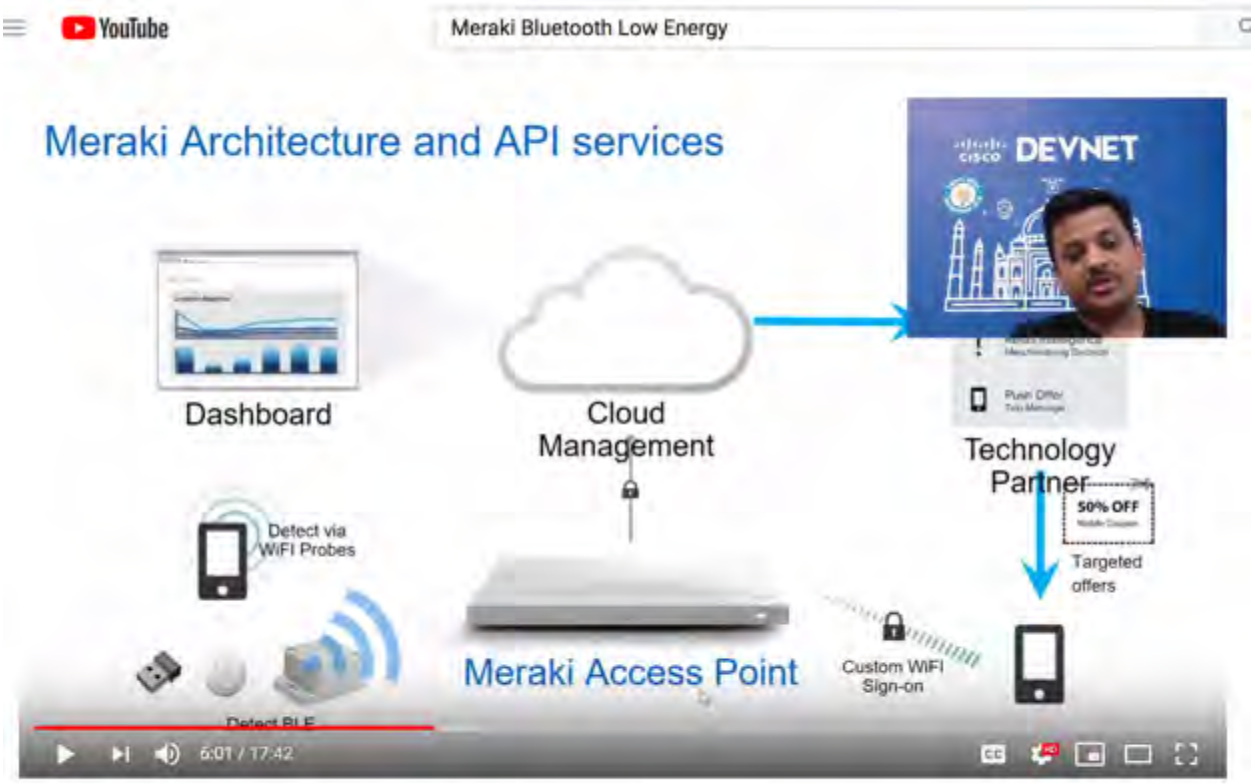

YouTube
Search
cisco
Meraki MR32
0:21 / 1:38
Supporting Bluetooth Beacons and tracking in the latest Meraki APs
22,140 views
29
2
SHARE
SAVE


YouTube
Search
Meraki
Network-wide
Security appliance
Switch
Wireless
Organization
Help
Bluetooth settings
Advertising
Scanning
0:47 / 1:38
Supporting Bluetooth Beacons and tracking in the latest Meraki APs
22,140 views
29
2
SHARE
SAVE



https://www.youtube.com/watch?v=5BWcxO66UQM.

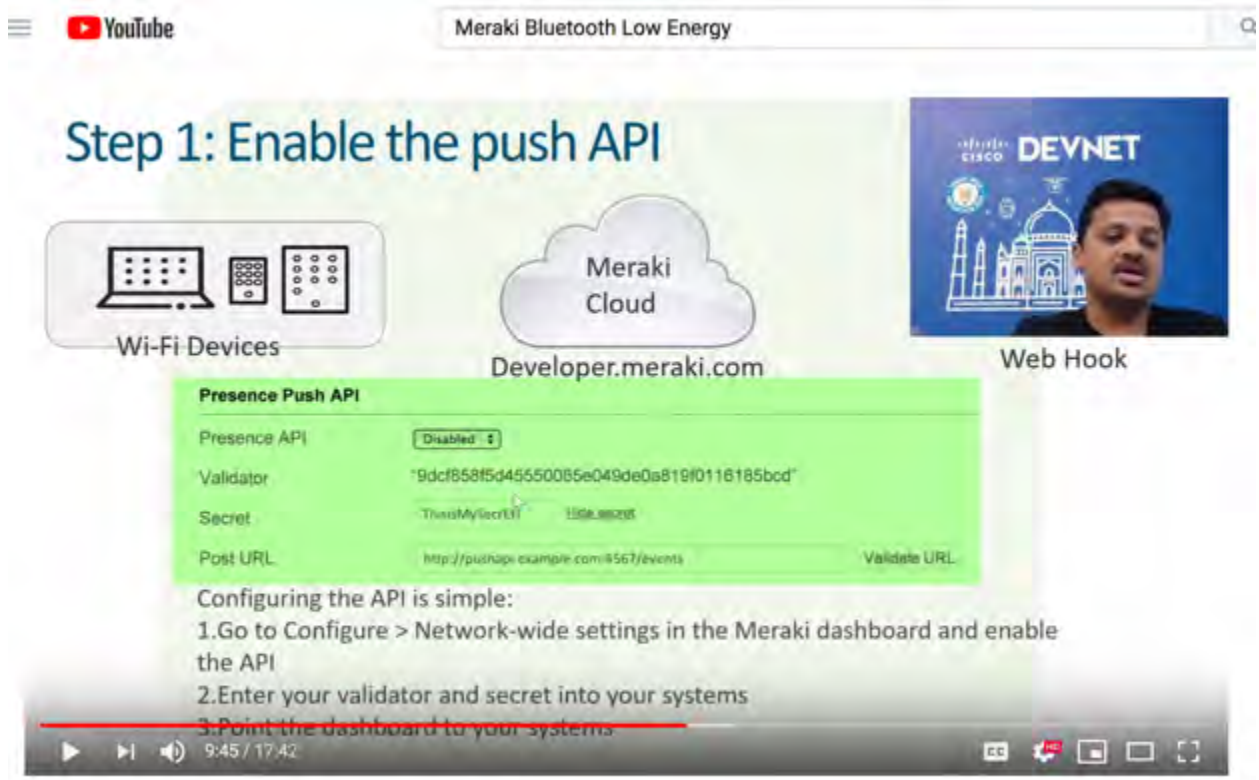

YouTube
Meraki Bluetooth Low Energy
What are Location Services?
DEVNET
Location Services describe class of services that provides information in Real-Time about the location or proximity of objects, animals, people and goods."
2:30 / 17:42
Using Cisco Meraki Location and Proximity Services.
1,598 views
16
0
SHARE
SAVE



Using Cisco Meraki Location and Proximity Services.

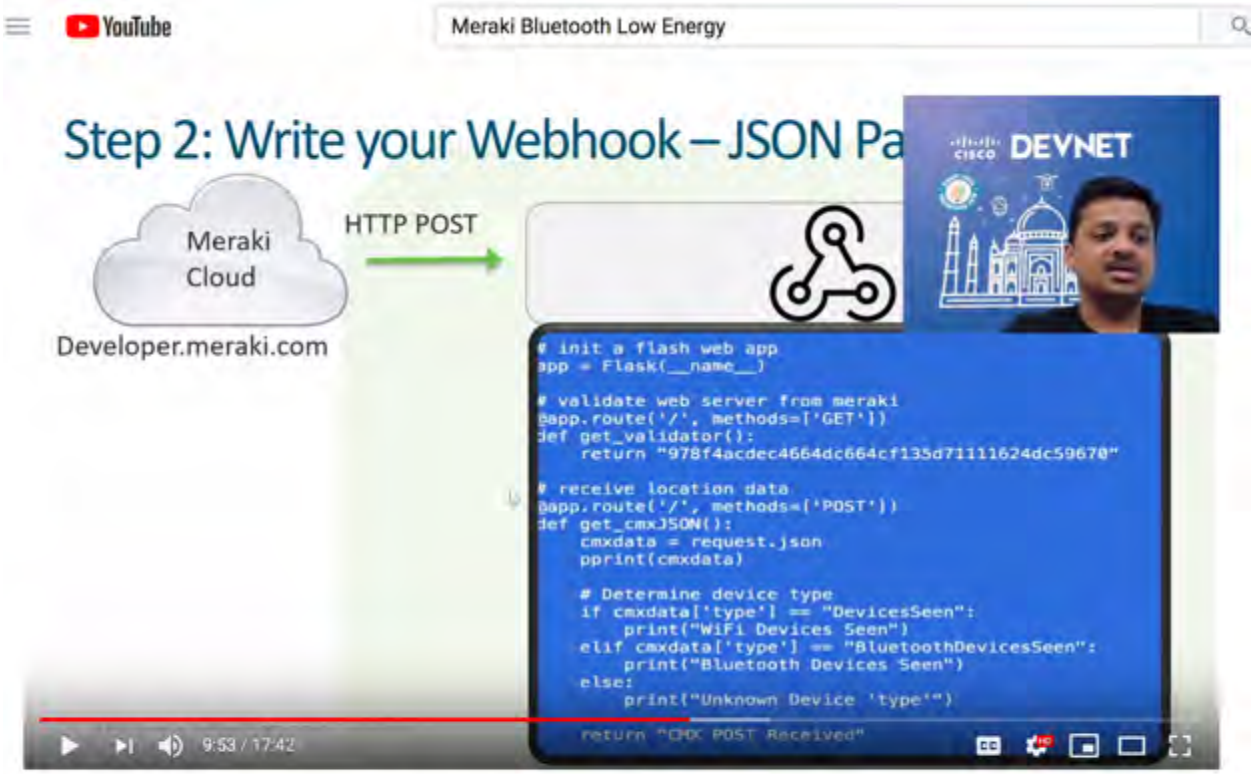
1,598 views

16 0 SHARE SAVE ...



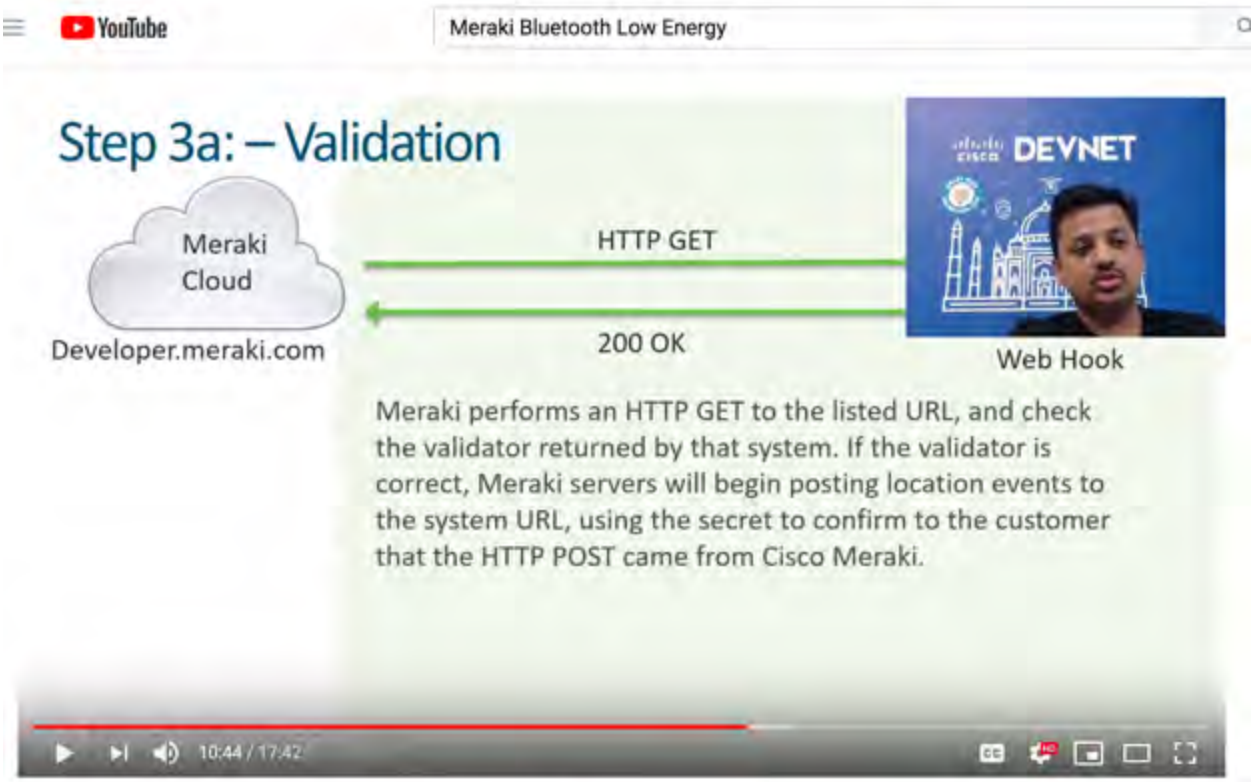
Using Cisco Meraki Location and Proximity Services.

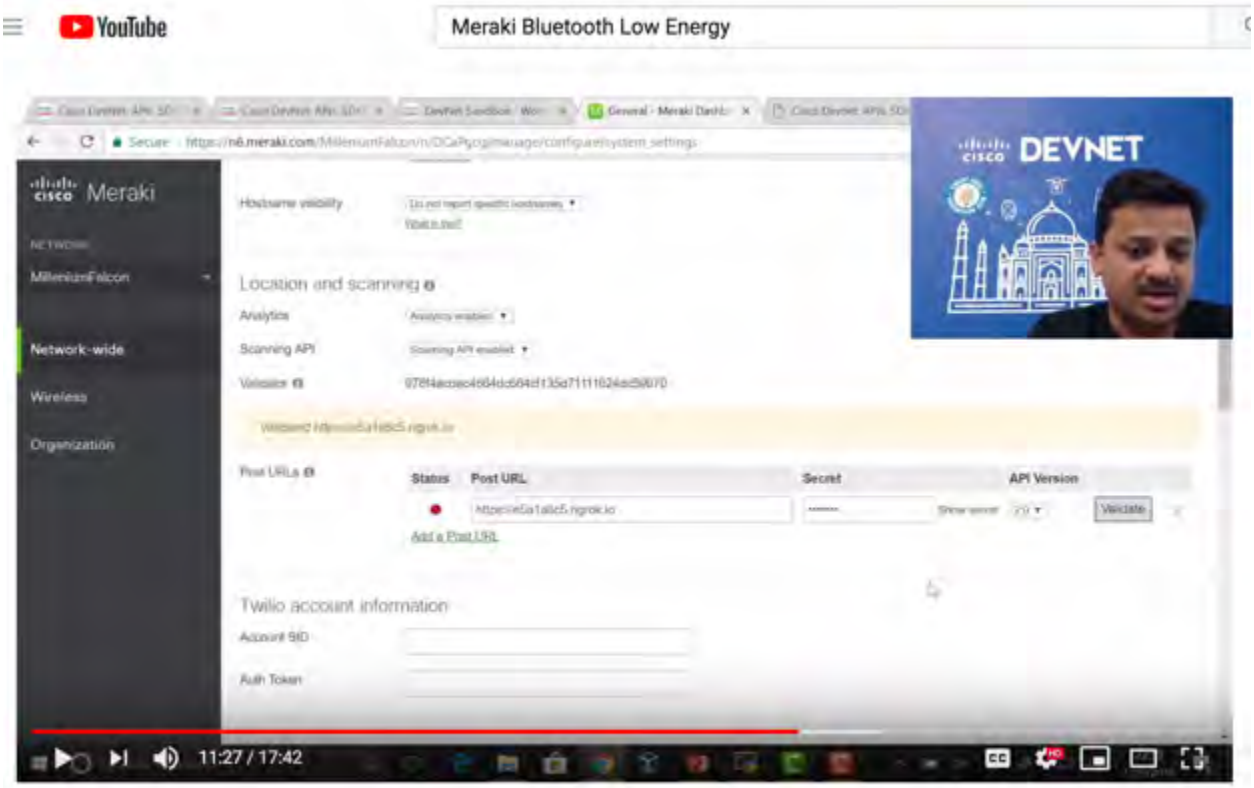
1,598 views 16 0 SHARE SAVE ...



Using Cisco Meraki Location and Proximity Services.

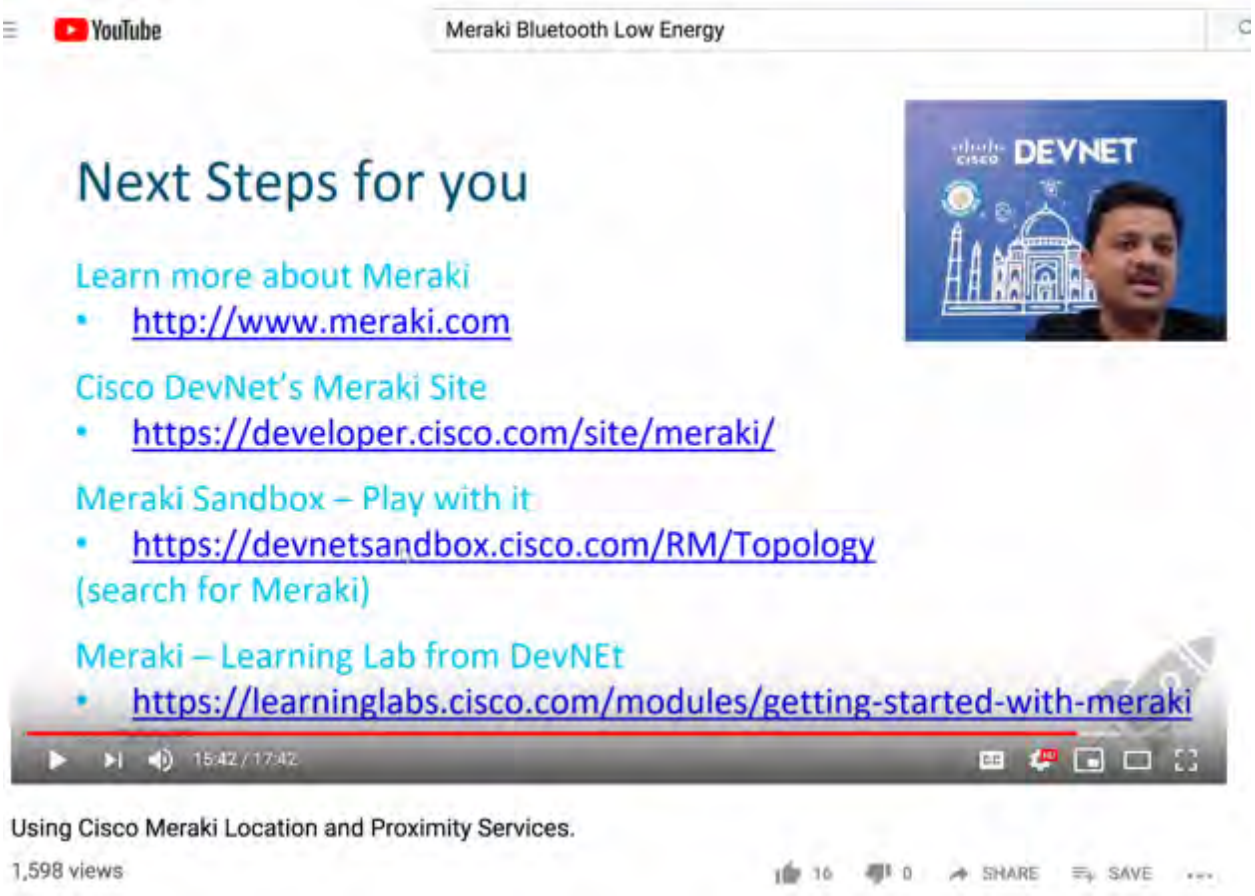
1,598 views 16 0 SHARE SAVE ...


YouTube
Meraki Bluetooth Low Energy
Step 3a: – Validation
Meraki Cloud
Developer.meraki.com
HTTP GET
200 OK
DEVNET
Web Hook
Meraki performs an HTTP GET to the listed URL, and check the validator returned by that system. If the validator is correct, Meraki servers will begin posting location events to the system URL, using the secret to confirm to the customer that the HTTP POST came from Cisco Meraki.
10:44 / 17:42
Using Cisco Meraki Location and Proximity Services.
1,598 views
16
0
SHARE
SAVE



Using Cisco Meraki Location and Proximity Services.

1,598 views 16 0 SHARE SAVE ...



https://www.youtube.com/watch?v=XEMno9_pwBw.

59. Cisco also has infringed, and continues to infringe, at least claim 1 of the '892 patent by offering to commercially distribute, commercially distributing, and/or importing the Accused Infringing Devices which devices are used in practicing the processes, or using the systems, of the '892 patent, and constitute a material part of the invention. Cisco knows portions of the Accused Infringing Devices to be especially made or especially adapted for use in infringement of the '892 patent, not a staple article, and not a commodity of commerce suitable for substantial noninfringing use. Cisco is thereby liable for infringement of the '892 patent under 35 U.S.C. § 271(c).

60. Cisco is on notice of its infringement of the '892 patent by no later than September 28, 2018 in a complaint filed in this District detaling Cisco's infringement of the '892

patent. On information and belief, Cisco did not and has not changed its infringing behavior after learning of the infringement allegations. It has not offered to license the '892 patent and has continued its infringement and its inducement of others unabated. On information and belief, since receiving such notice Cisco has known and intended that its continued actions would actively induce and contribute to the infringement of at least claim 1 of the '892 patent. Cisco has had the specific intent to induce and contribute to the infringement of third parties since receiving notice of the '892 patent and has had knowledge of (and/or was willfully blind to) the fact that its actions would induce and/or contribute to the infringement of third parties since receiving notice of the '892 patent. Discovery may prove that Cisco had earlier knowledge of the '892 patent and its infringement of the '892 patent.

61. Upon information and belief, Cisco may have infringed and continues to infringe the '892 patent through other software and devices utilizing the same or reasonably similar functionality, including other versions of the Accused Infringing Devices.

62. Cisco's acts of direct and indirect infringement have caused and continue to cause damage to Uniloc and Uniloc is entitled to recover damages sustained as a result of Cisco's wrongful acts in an amount subject to proof at trial.

PRAYER FOR RELIEF

WHEREFORE, plaintiff Uniloc 2017 LLC respectfully prays that the Court enter judgment in its favor and against Cisco as follows:

a. A judgment that Cisco has infringed one or more claims of the '891 patent literally and/or under the doctrine of equivalents directly and/or indirectly by inducing infringement and/or by contributory infringement;

b. A judgment that Cisco has infringed one or more claims of the '892 patent literally and/or under the doctrine of equivalents directly and/or indirectly by inducing

infringement and/or by contributory infringement;

c. That for each Asserted Patent this Court judges infringed by Cisco this Court award Uniloc its damages pursuant to 35 U.S.C. § 284 and any royalties determined to be appropriate;

d. That this be determined to be an exceptional case under 35 U.S.C. § 285;

e. That this Court award Uniloc prejudgment and post-judgment interest on its damages;

f. That Uniloc be granted its reasonable attorneys' fees in this action;

g. That this Court award Uniloc its costs; and

h. That this Court award Uniloc such other and further relief as the Court deems proper.

DEMAND FOR JURY TRIAL

Pursuant to Rule 38(b) of the Federal Rules of Civil Procedure, Uniloc demands a trial by jury for all issues so triable.

Dated: February 1, 2019

By: */s/ M. Elizabeth Day*
M. Elizabeth Day

M. Elizabeth Day (SBN 177125) *Admitted to Practice in Texas*
eday@feinday.com
David Alberti
dalberti@feinday.com
Sal Lim
slim@feinday.com
Marc Belloli (SBN 244290)
mbelloli@feinday.com
FEINBERG DAY ALBERTI LIM & BELLOLI LLP
1600 El Camino Real, Suite 280
Menlo Park, CA 94025
Tel: 650.618.4360
Fax: 650.618.4368

Attorneys for Plaintiff
Uniloc 2017 LLC