APPENDIX B

Verifying Detection of Asset Tags in WLAN Controllers

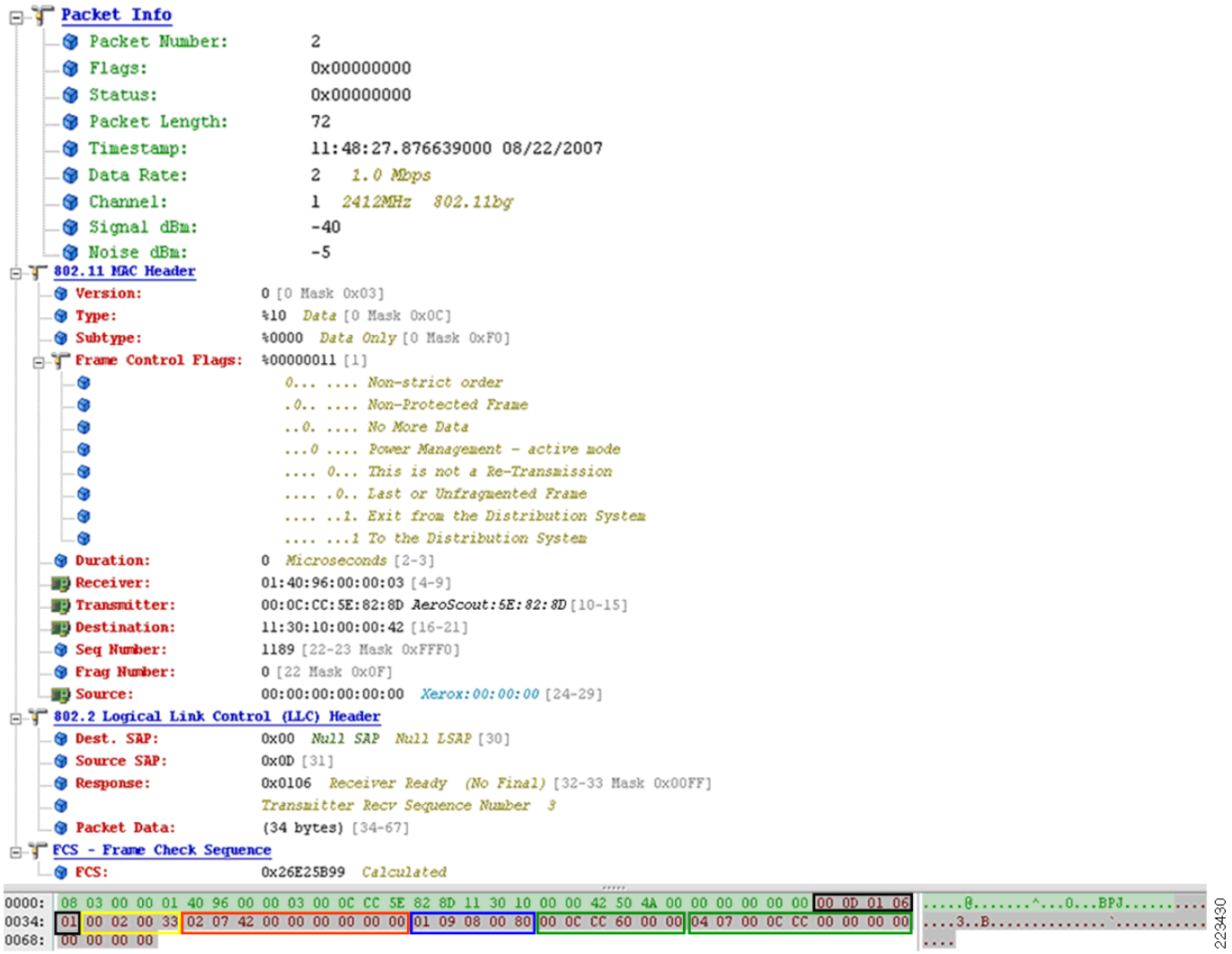
Asset Tags Detection

The protocol analyzer trace in Figure B-1 provides important information with regard to how asset tags compliant with the Cisco Compatible Extensions for Wi-Fi Tags specification are recognized and distinguished from other tracked devices in the network. In this example, we use an AeroScout T2 asset tag with firmware version 4.33. Assets tags that are supplied by other vendors that are also compliant with the Cisco Compatible Extensions for Wi-Fi Tags specification can be expected to be recognized by the Cisco UWN in a similar fashion.

Figure B-1 depicts the layer two multicast frame that is transmitted at the expiration of every tag transmission interval for an AeroScout T2 asset tag configured for a basic set of operational parameters. In Figure B-1, the tag configuration includes:

- Periodic 60 second tag transmission interval across three channels (1, 6, 11)
- Chokepoint out of range indication (indicated by the blue rectangle in Figure B-1)
- Onboard motion and temperature detection sensors disabled

Figure B-1 RF Protocol Analysis of Tag Multicast Frame (Cisco Compatible Extensions for Wi-Fi Tag Compliant)



This asset tag shown in Figure B-1 is not configured to transmit external sensor telemetry. In addition, the RF frame also includes the following information:

- Five byte Cisco Compatible Extensions for Wi-Fi Tags header (black rectangle)
- Tag product type identification (yellow rectangle)
- Optional battery telemetry (red rectangle)
- Optional vendor specific information (green rectangles)

The length of the multicast frames is dependent upon the tag's configuration and the optional features supported by the tag and tag vendor. In this case, the length of the multicast frame shown in Figure B-1 is 72 bytes. If additional features such as on-board temperature sensing were enabled, or if the tag were transmitting a multicast message due to stimulation from a chokepoint trigger, the frame length would be greater. For example, a typical length for tag multicasts transmitted as a result of stimulation from a chokepoint trigger is 88 bytes. The added length in this case comes primarily from the inclusion of the stimulating chokepoint trigger's MAC address and additional vendor-specific information.

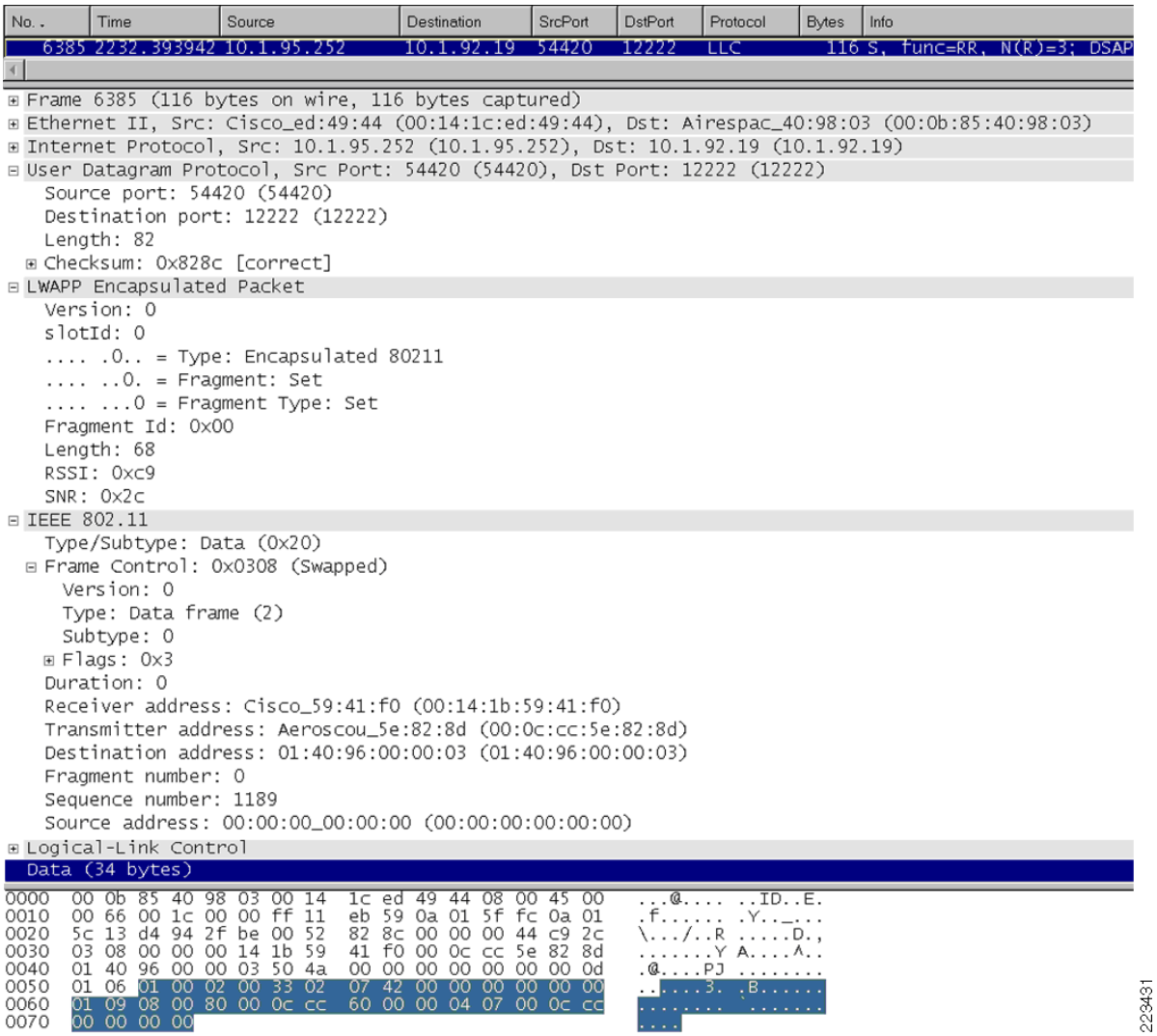
The AeroScout T2 tag initiates Clear Channel Assessment (CCA) for 100 microseconds. If the channel is clear, it then multicasts its payload at 1 Mbps. These frames are sent at 1 Mbps with the To Distribution System (ToDS) and Exit From Distribution System (FromDS) bits in the 802.11 MAC header both set to "1". Note that the Wireless Distribution System (WDS) four-address frame format is being used, indicated by the presence of the receiver and transmitter addresses in Figure B-1.

The transmitter address will always indicate the MAC address of the asset tag responsible for transmitting the frame, whereas the receiver address is a multicast address used by all asset tags compliant with the Cisco Compatible Extensions for Wi-Fi Tags specification, regardless of vendor origin. The destination and source addresses shown within the 802.11 MAC header are not used by the Cisco UWN for asset tags compliant with the Cisco Compatible Extensions for Wi-Fi Tags specification. These are typically set to all zeroes, although vendor-specific usage of the destination address field by tag vendors is possible, as we see with the AeroScout T2 tag shown in Figure B-1.

After the frame shown in Figure B-1 is received by access points, it will be transmitted to the controller(s) to which these access points are registered using the LWAPP protocol, as shown in Figure B-2. Here we see the IP source address associated with the receiving access point, and the IP destination address associated with the AP Manager interface of the controller to which the receiving access point is registered. When comparing the two figures, notice in Figure B-2 that Cisco Aironet access points make two modifications to the frame information prior to dispatching to the controller via LWAPP:

- It copies the access point's base radio MAC address (base BSSID) to the receiver address field in the encapsulated 802.11 header.
- It copies the CCX multicast address of 01:40:96:00:00:03 to the destination address field in the encapsulated 802.11 header.

Figure B-2 LWAPP Capture of Tag Multicast Frame (Cisco Compatible Extensions for Wi-Fi Tag Compliant)



When the tag multicast address is recognized by the controller, the identity and type of sender is established via the payload information contained in the frame. Depending on the type of information contained within the tag payload, it will be passed to the location appliance using either traditional SNMP poll responses or the new LOCP introduced in software Release 4.1.

Note the sequence number (1189) and fragment fields (0) that appear in both the RF as well as the LWAPP frame analysis. This is an important piece of information that can be very useful when matching packets that flow into access points via 802.11 and out of them via LWAPP. The sequence number for a particular tag frame indicates the number of the tag message and is assigned from a single modulo 4096 counter starting at zero, and is incremented by 1 for each tag message cycle. The fragment number specifies the specific frame within a burst of frames transmitted on a single channel. The fragment number should always start from zero even if the burst length is zero. For a packet burst, the fragment number should be set to *n* where *n* is the packet index within the burst starting from 0. For example, if a tag is configured to transmit a burst of length 5, then the fragment number would start at 0 for the first packet in the burst, 1 for the second packet and so on up to 4 for the last packet in the burst.

For example, assume that an asset tag is configured to send a burst length of 3 packets for each of channels 1, 6, and 11. In the case of an AeroScout asset tag, the burst length is configured by using the tag message repetitions transmission parameter. The expected fragment and sequence numbers would be as shown in Table B-1.

Table B-1 Packet Fragment and Sequence Numbers

Packet Instance	Fragment Number	Sequence Number	Channel
0	0	0	1
1	1	0	1
2	2	0	1
3	0	0	6
4	1	0	6
5	2	0	6
6	0	0	11
7	1	0	11
8	2	0	11

Assume a second asset tag is configured to send a single message on each of channels 1, 6, and 11 every 60 seconds. The expected fragment and sequence numbers occurring over the next 120 seconds would be as shown in Table B-2 to Table B-4.

Table B-2 Time+0

Packet Instance	Fragment Number	Sequence Number	Channel
0	0	0	1
1	0	0	6
2	0	0	11

Table B-3 Time+60

Packet Instance	Fragment Number	Sequence Number	Channel
0	0	1	1
1	0	1	6
2	0	1	11

Table B-4 Time+120

Packet Instance	Fragment Number	Sequence Number	Channel
0	0	2	1
1	0	2	6
2	0	2	11

Asset Tags Not Detected

In situations where asset tags are not being detected properly despite configuration of the system in accordance with best practices, re-verification of proper configuration should be performed. It is also recommended that verification of proper asset tag RSSI detection and message forwarding be conducted. The following steps are recommended to accomplish this:

Step 1 Verify if tag is properly detected by WLAN controllers by using the **show rfid summary** command:

```
(Controller) >show rfid summary

Total Number of RFID   : 12
-------------- -------- ------------------ ------ --------------------
  RFID ID      VENDOR       Closest AP      RSSI  Time Since Last Heard
-------------- -------- ------------------ ------ --------------------
00:0c:cc:5d:4c:5e Aerosct  AP0014.6a1b.41f0    -34     24 seconds ago
00:12:b8:00:20:52 G2       AP001a.a10e.2ffa    -61     16 seconds ago
00:14:7e:00:30:a1 Pango    AP0014.6a1b.41f0    -65      2 seconds ago
```

If the controller does not detect the tag, use the command **show rfid config** to verify that RFID tag detection has been enabled on the controller.

```
 (Controller) >show rfid config

RFID Tag data Collection..... Enabled
RFID Tag Auto-Timeout........ Disabled
RFID  timeout................ 1200 seconds
```

Step 2 If the RFID tag detection is not enabled, enable it using the command shown below. Note that starting with the Cisco UWN software Release 4.1, RFID tag detection is enabled by default.

```
config rfid status enable
```

Step 3 Ensure that the RFID tag timeout is set to a recommended minimum of three times (and a recommended maximum of eight times) the longest tag transmission interval found in the tag population, inclusive of stationary as well as any “in-motion” tag transmission intervals. The valid range of values for this parameter is 60 to 7200 seconds and the default value is 1200 seconds.

For example:

```
(Controller) >config rfid timeout 1200
```

Step 4 Check that the RSSI expiry timeout are set as follows:

```
(Controller) >show advanced location summary

Advanced Location Summary :

Algorithm used:                       Average
Client RSSI expiry timeout:            150 sec, half life: 60 sec
Calibrating Client RSSI expiry timeout: 30 sec, half life: 0 sec
Rogue AP RSSI expiry timeout:              1200 sec, half life: 120 sec
RFID Tag RSSI expiry timeout:              1200 sec, half life: 120 sec
```

If the values are different from default as shown above, set them to default using the following configuration commands:

```
config advanced location expiry {calibrating client | client | rogue-aps | tags }
<seconds>
```

config advanced location rssi-half-life {calibrating client | client | rogue-aps | tags} *<seconds>*

Step 5 If asset tags are still not detected by the controller using the **show rfid summary** command, enable the following debugs on the controller:

```
debug mac addr <tag mac addr>
debug dot11 rfid enable
00:0c:cc:5e:82:8d Parsing Cisco Tag RFID packet 68
00:0c:cc:5e:82:8d System group 51
00:0c:cc:5e:82:8d Battery group: status 0x42, days 0, age 0
00:0c:cc:5e:82:8d Chokepoint group, option 0x8, power 0, range 128
00:0c:cc:5e:82:8d Vendor group
00:0c:cc:5e:82:8d  LOCPBuffer 0x133245ec  buffer 0x13324611 msgLen 37 msgId 18 transId
816848706
00:0c:cc:5e:82:8d Notifying LBS of vendor specific data
00:0c:cc:5e:82:8d rfid Aerosct updated by AP 00:14:1B:59:41:F0 (Incoming rssi -47,snr 53),
New saved values rssi -48, snr 49, timestamp 3402186024
```

Note It is recommended that the **debug mac addr** command be used when debugging in this fashion. This will help avoid a flood of debug messages in environments where there are many tags active.

Step 6 If the **debug** command output indicates that packets from this asset tag are not received by the controller, you may want to continue debugging on the console of an access point that is known to be within range of the asset tag. In order to verify the detection of an RFID tag by an access point, perform the following steps:

a. Verify whether RFID tag detection has been enabled on the access point and the channel that the access point is currently configured for. This can be done on the access point console using the following command:

show controller Dot11Radio 0

```
 <snipped capture>
Current Frequency: 2412 MHz  Channel 1
RFID Tag Detection: Enabled
```

If tag detection is found to be disabled on the access point, enable tag detection by issuing the following command on the controller:

config rfid status enable

Note that some access point commands can also be executed remotely from the controller using the access point remote debugging feature:

debug ap enable <Cisco AP>
debug ap command <command> <Cisco AP>

b. If tag detection is enabled and the asset tag is configured to transmit on the channel the access point is configured for, check to see that the access point is forwarding the tag multicast packet to the controller by enabling the following debugs on the access point:

debug dot11 Dot11Radio 0 trace print mcast

Note In software Release 4.1, in order for the output of the `debug` **dot11 Dot11Radio 0 trace print mcast** command to be viewed, the command must be entered directly at the access point console. It cannot be entered remotely from the controller.

```
4A1F8FB0 r  1 60/ 38- 0803 000 m014096 5D33CF m61356B 6D00   000000 173
   0012 0606 0100 0200 3302 0742 0000 0000 0000 0302 0A03 0109 0000 8000
  0CCC 6010 BF04 0800 0CCC 6E10 BF00 0000 019C 917C 00B8 F564 608F FD05 0000
```

- **m014096**—The 3 bytes following the letter "m" represents the first 3 bytes of the multicast address used for asset tags compliant with the Cisco Compatible Extensions for Wi-Fi Tags specification.
- **5D33CF**—This represents the last 3 bytes of the asset tag's MAC address.

If you would like to view the multicast address and tag MAC address in their unabbreviated format, issue the command **no debug dot11 Dot11Radio 0 print short** command at the access point console.

If information similar to that shown above is seen on the debug output, it indicates that the access point is receiving and forwarding asset tag packets to the controller. If the controller still does not show the asset tag packets being received, use an ethernet protocol analyzer capable of decoding LWAPP encapsulated 802.11 frames (such as WireShark or OmniPeek) on the LWAPP ethernet connection between the access point and controller to verify that the asset tag packets are indeed reaching the controller. The format of these packets should similar to that shown in Figure B-2. If these packets are seen on the protocol analyzer trace and the controller still does not indicate that asset tag packets are successfully received, capture all the details collected so far including the protocol analyzer traces and contact the Cisco Technical Assistance Center for further debugging assistance.

c. If the tag multicast messages are not seen in the access point debug output, use an RF protocol analyzer such as OmniPeek or WireShark to verify that asset tags are indeed successfully transmitting packets in the format expected on all three 2.4 GHz channels (or the channels that your infrastructure is configured for) as seen in Figure B-1. If the proper frame formats are not seen on the protocol analyzer trace, this should be addressed via the asset tag configuration or by replacing the asset tag if necessary, especially if the asset tag firmware is out of date. If the proper frames are seen on the RF protocol analyzer, attempt to reset tag detection in the controller by issuing the following commands:

```
config rfid status disable
config rfid status enable
```

If the issue continues to persist despite these suggestions, it is recommended that you capture all the details collected so far including the protocol analyzer traces and contact the Cisco Technical Assistance Center for further debugging assistance.

Verifying Asset Tag Telemetry and Events

In order to verify that WLAN controllers are detecting asset tag telemetry and high-priority events, and forwarding that information to the location appliance using LOCP, the following procedure may be used:

Step 1 Make sure that the asset tag is detected by the WLAN controller using the procedure outlined in the previous section.

Step 2 Verify that the telemetry or high-priority "emergency" event information you are concerned with has been recorded in the RFID database on the controller:

```
show rfid detail <tag mac addr>
```

For example, the following output snippet illustrates that indication of a panic button being depressed on an asset tag has been received, along with vendor specific data pertaining to the event:

```
<snip>
Telemetry Group
===================
Motion Probability.............................  No Motion

!! EMERGENCY !!
===================
Reason.........................................  Panic Button

Vendor Specific
===================
Group Length...................................  8
Vendor OUI:....................................  0x0  0xc  0xcc
Vendor Data: 0x6e  0x13  0xa3  0x0  0x0
```

Step 3 If the notification is not seen above in the controller's RFID database, enable the following debugs on the controller to validate that it is receiving the notifications.:

```
debug mac addr <tag mac addr>
debug dot11 rfid enable

00:0c:cc:5e:82:8d Parsing Cisco Tag RFID packet 62
00:0c:cc:5e:82:8d System group 51
00:0c:cc:5e:82:8d Battery group: status 0x42, days 0, age 0
00:0c:cc:5e:82:8d Chokepoint group, option 0x8, power 0, range 128
00:0c:cc:5e:82:8d Emergency group
00:0c:cc:5e:82:8d  LOCP Buffer 0x133245ec  buffer 0x1332460a msgLen 30 msgId 18 transId
808989330
00:0c:cc:5e:82:8d Notifying LBS of emergency
00:0c:cc:5e:82:8d rfid Aerosct updated by AP 00:14:1B:59:41:F0 (Incoming rssi -49,snr 50),
New saved values rssi -48, snr 49, timestamp 3444175997
```

Step 4 If output similar to that above is not seen, use an RF protocol analyzer to capture the packets being transmitted by the tag during the send of telemetry or high priority events to verify that data is being transmitted in the correct format. You will need the assistance of the Cisco Technical Assistance Center to confirm this. If the packets that the tag transmits over the air are deemed by the Cisco TAC not to be valid, verify that the level of firmware being used in the asset tag is compliant with the Cisco Compatible Extensions for Wi-Fi Tags specification and that it supports the telemetry or high-priority functions desired.

Step 5 If the telemetry or high-priority events are seen in the controller's RFID database, check to see if they are being sent to the location appliance (look for **Notifying LBS of emergency**) in the output above. Issue the following command to verify that the LOCP connection between the controller and the location appliance is up and functioning.

```
(Cisco Controller) >show LOCP status

LocServer IP    TxEchoResp    RxEchoReq    TxData    RxData
--------------  ----------    ---------   --------   -------
10.1.56.21         5300          5300        83597      441
```

Normally, if the LOCP connection is up and running properly, you should see the echo counts regularly increment (based on the settings of the echo interval in the location appliance). In addition, as emergencies and telemetry events occur that require transport via LOCP, you will see the data fields

increment as well. If a controller is rebooted and repeatedly fails to establish a connection to the location appliance, you will fail to see an IP address listed for the location appliance, and the Tx / Rx counts will be blank.

If the TxData fields fail to increment in spite of known emergencies and telemetry data being sent by tags, verify that the LOCP send to the location appliance is successful using the following debug command:

```
debug LOCP event enable
```

The output should look similar to the following:

```
LOCP TX message
Sending LOCP_APP_INFO_NOTIF_MSG to LocServer 0
Tx OK
```

If messages are received indicating that there are LOCP failures, contact the Cisco Technical Assistance Center for further troubleshooting assistance.