Understanding Over–the–Air Provisioning (OTAP)

Document ID: 100516

Contents

Introduction

Lightweight Access Points (LAPs) can discover the management IP address of the controller through Over–the–Air Provisioning (OTAP) technique. This feature is supported by Cisco 5500 and 4400 Series Controllers. This document explains some of the details of this process.

Prerequisites

Requirements

Cisco recommends that you have basic knowledge of LWAPP/CAPWAP.

Components Used

This document is not restricted to specific software and hardware versions.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

OTAP Process

During the LAP boot process, the LAP uses different mechanisms in order to discover controllers that it can join. The LAP keeps each of the controller that IP addresses it learned through the different methods in different lists in order to reflect how the LAP learned about them. For example, the LAP can learn management IP addresses of multiple controllers through the DNS entry for CISCO–LWAPP–CONTROLLER.localdomain, DHCP option 43, through broadcasts on the local subnet, locally stored controller IP address discovery, and through OTAP. Once the access point has completed the LWAPP WLC Discovery steps, it chooses a WLC from the candidate WLC list and sends that WLC an LWAPP Join Request.

Lightweight AP (LAP) Registration to a Wireless LAN Controller (WLC) discusses the different methods the LAP use to discover controllers.

This document provides information about the OTAP process.

The OTAP feature is enabled on the controller GUI from the controller **General** page or through the CLI with the **config network otap−mode {enable | disable}** command.

Note: This feature is disabled by default and should remain disabled when all access points are installed.

The OTAP process begins when the LAP momentarily brings the radio interfaces up before the Discovery phase and scans the different RF channels that listen for RRM neighbor packets. It is possible that the LAP receives or does not receive an RRM neighbor packet on the first boot. This depends on:

1. How many LAPs are in the area (the greater the number of LAPs in the area, the greater the chance of the LAP receiving an RRM neighbor packet)
2. How many channels are being used by Auto−RF (the more channels, the less likely the LAP is to receive an RRM neighbor packet)
3. How long the LAP scans the RF channels during the OTAP process (typical scan times before the AP moves into the discovery phase are 18 to 35 seconds for all channels)

When the LAP moves into the Discovery phase, it sends discovery requests through its primary interface to each of the controllers in the lists based on how it learned about them. For the controllers that are learned through OTAP, the LAP sends the controller a Discovery Request packet with the OTAP bit set. This indicates to the controller that the AP learned its management IP address through OTAP. Other discovery methods, such as DNS or DHCP option 43, are not differentiated in the Discovery Request packet because they are learned through wired connections.

This controller can reject discovery requests for these reasons:

1. The OTAP bit is set in the Discovery Request packet and OTAP is disabled on the controller.
2. The Discovery Request packet is too large.
3. The Discovery Request packet is not received on the management interface.

LAPs support OTAP only when they have a full LWAPP Cisco IOS image. OTAP is not supported by the LWAPP Recovery Cisco IOS image. The LWAPP Recovery Image is shipped from the factory and loaded by the upgrade tool. The recovery images (cXXXX−rcvk9w8−mx), shipped with new out of−the−box LAPs, do not contain any radio firmware and do not bring up any radio interfaces during the boot process. Hence OTAP does not work with out−of−the−box LAPs. The exceptions are out−of−the−box 1510s and 1520 APs, which have a full image installed in flash.

Note: OTAP enabled on the controller indicates to the controller whether or not to respond to discovery requests with the OTAP bit set. It does not prevent the LAPs already joined to the controller from the transmission of the management IP address of the controller in the clear in RRM neighbor packets. Thus, if you disable OTAP on the controller, this does not disable it on the access point. OTAP cannot be disabled on the access point.

Radio Resource Management (RRM) Neighbor Packets

OTAP utilizes RRM neighbor packets. This section provides a brief background on RRM neighbor packets. LAPs already joined to a controller transmit RRM neighbor packets to the RRM multicast address 01:0b:85:00:00:00. Each LAP must transmit a Neighbor Discovery packet once every 60 seconds on each of the configured Auto−RF channels for 802.11b/g and 802.11a. The RRM neighbor packets are transmitted without any encryption similar to other RF management packets, such as probe requests and probe responses. The RRM neighbor packets contain neighbor control messages. See the RRM Neighbor Packet for 802.11a section for more information. Each neighbor control message consists of:

- Radio ID
- Group ID
- Management IP Address (of the Controller)
- Channel Count
- Antenna Pattern (Omni, Left, Diversity, Right)
- Measurement Interval
- Key
- Channels
- Power

The LAPs encapsulate and forward to the controller any RRM neighbor packets they receive. This allows the controller to form RF groups for the adjustment of the power and channels among LAPs that can see each other. LAPs that are booting can use these RRM neighbor packets in order to discover the controller to which neighbor LAPs are already joined.

RRM Neighbor Packet for 802.11a

Here is a sample RRM neighbor packet for 802.11a:

```
No.  Time                 Source               Destination
8313 23:39:20.169855117 00:14:1b:5a:40:10     01:0b:85:00:00:00


Protocol Info
LLC     U, func=UI; SNAP, OUI 0x000B85 (Unknown), PID 0xCCCD

Frame 8313 (80 bytes on wire, 80 bytes captured)
    [Protocols in frame: wlan:llc:data]
IEEE 802.11
    Data Rate: 6.0 Mb/s
    Channel: 60
    Signal Strength: 0%
    Type/Subtype: Data (32)
    Frame Control: 0x0308 (Normal)
        Version: 0
        Type: Data frame (2)
        Subtype: 0
        Flags: 0x3
            DS status: Frame part of WDS from one AP to another AP
                       (To DS: 1 From DS: 1) (0x03)
            .... .0.. = More Fragments: This is the last fragment
            .... 0... = Retry: Frame is not being retransmitted
            ...0 .... = PWR MGT: STA will stay up
            ..0. .... = More Data: No data buffered
            .0.. .... = Protected flag: Data is not protected
            0... .... = Order flag: Not strictly ordered
    Duration: 0
    Receiver address: 01:0b:85:00:00:00 (01:0b:85:00:00:00)
    Transmitter address: 00:14:1b:5a:40:1f (00:14:1b:5a:40:1f)
    Destination address: 01:0b:85:00:00:00 (01:0b:85:00:00:00)
    Fragment number: 0
    Sequence number: 487
    Source address: 00:14:1b:5a:40:10 (00:14:1b:5a:40:10)
    Frame check sequence: 0x84bab9b3 [correct]
Logical-Link Control
    DSAP: SNAP (0xaa)
    SSAP: SNAP (0xaa)
    Control field: U, func=UI (0x03)
        000. 00.. = Command: Unnumbered Information (0x00)
        .... ..11 = Frame type: Unnumbered frame (0x03)
    Organization Code: Airespace (0x000b85)
    Protocol ID: 0xcccd
Data (38 bytes)
```

```
0000   08 03 00 00 01 0b 85 00 00 00 00 00 14 1b 5a 40 1f   .............Z@.
0010   01 0b 85 00 00 00 70 1e 00 14 1b 5a 40 10 aa aa   ......p....Z@...
0020   03 00 0b 85 cc cd 01 1b 00 1a 6c 91 80 80 00 04   ..........l.....
0030   0a 01 00
0f 3c 01 01 3c 04 ff ff 00 4e 40 fd ec   ....<..<....N@..
0040   a7 4a f4 c4 d3 7b 19 be 10 92 50 91 84 ba b9 b3   .J...{....P.....
```

The RRM neighbor multicast address and the management IP address of the controller are highlighted.

Related Information

- **Lightweight AP (LAP) Registration to a Wireless LAN Controller (WLC)**
- **Cisco Wireless LAN Controller Configuration Guide, Release 7.0**
- **Deploying Cisco 440X Series Wireless LAN Controllers**
- **Technical Support & Documentation – Cisco Systems**