Lightweight AP (LAP) Registration to a Wireless LAN Controller (WLC)

Document ID: 70333

Introduction

In a Cisco Unified Wireless Network architecture, access points (APs) are lightweight. This means they cannot act independently of a wireless LAN controller (WLC). The lightweight access points (LAPs) have to first discover the WLCs and register with them before the LAPs service wireless clients. This document explains the different methods that LAPs use in order to discover WLCs. The document also explains the registration process that happens between the LAP and the WLC after the discovery phase.

Prerequisites

Requirements

Ensure that you meet these requirements before you attempt this configuration:

- Knowledge of Lightweight Access Point Protocol (LWAPP).
- Knowledge of how to configure basic parameters on the WLC.

  If you are a new user and have not configured the WLC for basic operation, refer to the Using the CLI Configuration Wizard section of *Cisco Wireless LAN Controller Configuration Guide, Release 6.0*.
- Knowledge of how to configure Microsoft Windows 2000 DHCP Server and Domain Name System (DNS) Server.

Components Used

The information in this document is based on these software and hardware versions:

- Cisco 4400 Series WLC that runs firmware 4.0.217.0
- Cisco 1000 Series LAPs
- Windows 2000 DHCP Server
- Windows 2000 DNS Server

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

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

Background Information

The WLCs and Cisco LAPs are part of the Cisco Unified Wireless Network architecture. The Cisco Unified Wireless Network architecture centralizes WLAN configuration and control on the WLC. The LAPs cannot act independently of the WLC. The WLC manages the LAP configurations and firmware. The LAPs are "zero touch" deployed, and no individual configuration of LAPs is required.

In order for the WLC to be able to manage the LAP, the LAP should discover the controller and register with the WLC. After the LAP has registered to the WLC, LWAPP messages are exchanged and the AP initiates a firmware download from the WLC (if there is a version mismatch between the AP and WLC). If the AP's onboard firmware is not the same as the WLC's, the AP will download firmware to stay in sync with the WLC. The firmware download mechanism utilizes LWAPP. Then, the WLC provisions the LAP with the configurations that are specific to the WLANs so that the LAP can accept client associations. These WLAN−specific configurations include:

- Service set identifier (SSID)
- Security parameters
- IEEE 802.11 parameters, such as:
    - Data rate
    - Radio channels
    - Power levels

There are different methods that an LAP uses in order to discover the WLC. This document discusses the different methods that the LAP can use in order to register the WLC. But first, the document explains the sequence of events that occur when an LAP registers with the WLC.

Note: The Management interface is the default interface for in−band management of the WLC and connectivity to enterprise services such as AAA servers.The management interface is also used for layer two communications between the WLC and access points. The Management interface is the only consistently "pingable" in−band interface IP address on the WLC.

Note: A WLC has one or more AP Manager Interfaces that are used for all Layer 3 communications between the WLC and the lightweight access points after the access point discovers the controller. The AP Manager IP address is used as the tunnel source for LWAPP packets from the WLC to the access point, and as the destination for LWAPP packets from the access point to the WLC. The AP Manager must have a unique IP address. Usually this is configured on the same subnet as the Management interface, but this is not necessarily a requirement. An AP Manager IP address is not pingable from outside the WLC. Refer to the Configuring Ports and Interfaces section of Wireless LAN Controller Configuration Guide for more information.

Register the LAP with the WLC

This sequence of events must occur in order for an LAP to register to a WLC:

1. The LAPs issue a DHCP discovery request to get an IP address, unless it has previously had a static IP address configured.
2. The LAP sends LWAPP discovery request messages to the WLCs.
3. Any WLC that receives the LWAPP discovery request responds with an LWAPP discovery response message.
4. From the LWAPP discovery responses that the LAP receives, the LAP selects a WLC to join.
5. The LAP then sends an LWAPP join request to the WLC and expects an LWAPP join response.
6. The WLC validates the LAP and then sends an LWAPP join response to the LAP.
7. The LAP validates the WLC, which completes the discovery and join process. The LWAPP join process includes mutual authentication and encryption key derivation, which is used to secure the join process and future LWAPP control messages.
8. The LAP registers with the controller.

The first problem that the LAP faces is how to determine where to send the LWAPP discovery requests (step 2). The LAP uses a hunting procedure and a discovery algorithm in order to determine the list of WLCs to which the LAP can send the discovery request messages.

This procedure describes the hunting process:

1. The LAP issues a DHCP request to a DHCP server in order to get an IP address, unless an assignment was made previously with a static IP address.
2. If Layer 2 LWAPP mode is supported on the LAP, the LAP broadcasts an LWAPP discovery message in a Layer 2 LWAPP frame. Any WLC that is connected to the network and that is configured for Layer 2 LWAPP mode responds with a Layer 2 discovery response. If the LAP does not support Layer 2 mode, or if the WLC or the LAP fails to receive an LWAPP discovery response to the Layer 2 LWAPP discovery message broadcast, the LAP proceeds to step 3.
3. If step 1 fails, or if the LAP or the WLC does not support Layer 2 LWAPP mode, the LAP attempts a Layer 3 LWAPP WLC discovery.

   See the Layer 3 LWAPP WLC Discovery Algorithm section of this document.
4. If step 3 fails, the LAP resets and returns to step 1.

Note: If you want to specify an IP address for an access point instead of having one assigned automatically by a DHCP server, you can use the controller GUI or CLI to configure a static IP address for the access point. Refer to the Configuring a Static IP Address on a Lightweight Access Point section of the WLC Configuration guide for more information. If the LAP is assigned a static IP address and can not reach the WLC, it falls back to DHCP.

Layer 2 LWAPP WLC Discovery Algorithm

LWAPP communication between the AP and the WLC can be in native, Layer 2 Ethernet frames. This is known as Layer 2 LWAPP mode. Although defined in the RFC draft, Layer 2 LWAPP mode is considered deprecated in Cisco's implementation. Only Cisco 1000 Series LAPs support Layer 2 LWAPP mode. Also, Layer 2 LWAPP mode is not supported on Cisco 2000 Series WLCs. These WLCs support only Layer 3 LWAPP mode.

This is the first method that a LAP uses to discover a WLC. The LAPs that support Layer 2 LWAPP mode broadcast a LWAPP discovery request message in a Layer 2 LWAPP frame. If there is a WLC in the network configured for Layer 2 LWAPP mode, the controller responds with a discovery response. The LAP then moves to the join phase (see step 5 of the Register the LAP with the WLC section).

This **debug lwapp events enable** command output shows the sequence of events that occur when a LAP using Layer 2 LWAPP mode registers with the WLC:

Note: The lines of this output have been moved to second lines due to space constraints.

```
Thu Sep 27 00:24:25 2007: 00:0b:85:51:5a:e0 Received LWAPP DISCOVERY REQUEST
from AP 00:0b:85:51:5a:e0 to ff:ff:ff:ff:ff:ff on port '2'
Thu Sep 27 00:24:25 2007: 00:0b:85:51:5a:e0 Successful transmission of
LWAPP Discovery−Response to AP 00:0b:85:51:5a:e0 on Port 2
Thu Sep 27 00:24:40 2007: 00:0b:85:51:5a:e0 Received LWAPP JOIN REQUEST
from AP 00:0b:85:51:5a:e0 to 00:0b:85:48:53:c0 on port '2'
Thu Sep 27 00:24:40 2007: 00:0b:85:51:5a:e0 AP ap:51:5a:e0:
txNonce  00:0B:85:48:53:C0 rxNonce  00:0B:85:51:5A:E0
Thu Sep 27 00:24:40 2007: 00:0b:85:51:5a:e0 LWAPP Join−Request MTU path from
AP 00:0b:85:51:5a:e0 is 1500, remote debug mode is 0
Thu Sep 27 00:24:40 2007: 00:0b:85:51:5a:e0 Successfully added NPU Entry for
AP 00:0b:85:51:5a:e0 (index 48)Switch IP: 0.0.0.0, Switch Port: 0, intIfNum 2,
vlanId 0AP IP: 0.0.0.0, AP Port: 0, next hop MAC: 00:0b:85:51:5a:e0
Thu Sep 27 00:24:40 2007: 00:0b:85:51:5a:e0 Successfully transmission of
LWAPP Join−Reply to AP 00:0b:85:51:5a:e0
Thu Sep 27 00:24:40 2007: 00:0b:85:51:5a:e0 Register LWAPP event for
AP 00:0b:85:51:5a:e0 slot 0
Thu Sep 27 00:24:40 2007: 00:0b:85:51:5a:e0 Register LWAPP event for
AP 00:0b:85:51:5a:e0 slot 1
```

Layer 3 LWAPP WLC Discovery Algorithm

The LAPs use the Layer 3 discovery algorithm if the Layer 2 discovery method is not supported or if the Layer 2 discovery method fails. The Layer 3 discovery algorithm uses different options in order to attempt to discover WLCs. The Layer 3 LWAPP WLC discovery algorithm is used to build a controller list. After a controller list is built, the AP selects a WLC and attempts to join the WLC.

The LWAPP Layer 3 WLC discovery algorithm repeats until at least one WLC is found and joined.

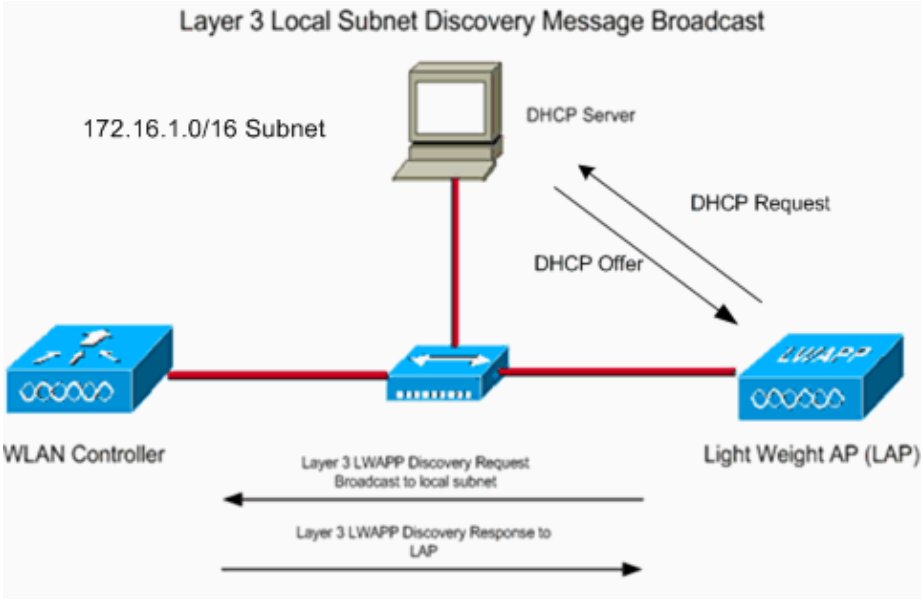
Note: During the LWAPP Layer 3 WLC discovery, the AP always completes all steps 1 through 5 in this section in order to build a list of candidate WLCs. After the AP has completed the LWAPP WLC discovery steps, the AP selects a WLC from the candidate WLC list on the basis of certain criteria, and then sends that WLC an LWAPP join request.

Each example scenario that this section explains is independent of the others and is provided only to give an understanding of how each step in the discovery process works. The LAP uses all the discovery steps in order to find a list of candidate WLCs before it selects a WLC to join.

This procedure describes the steps that the Layer 3 discovery algorithm goes through in the attempt to discover WLCs:

1. After the LAP gets an IP address from the DHCP server, the LAP begins this discovery process:

    a. The LAP broadcasts a Layer 3 LWAPP discovery message on the local IP subnet. Any WLC that is configured for Layer 3 LWAPP mode and that is connected to the same local subnet receives the Layer 3 LWAPP discovery message.
    b. Each of the WLCs that receives the LWAPP discovery message replies with a unicast LWAPP discovery response message to the LAP.



Here is an example. Assume that you have a WLC and an LAP in the same subnet (172.16.1.0/16). You also have a DHCP server subnet. When the LAP powers up, it sends out a DHCP request, with the hope that a DHCP server will provide an IP address. After the LAP gets an IP address from the DHCP server, the LAP broadcasts a Layer 3 LWAPP discovery message on to its local subnet. Because the WLC is also on the same subnet, the WLC receives the LWAPP discovery request from the LAP and responds with a Layer 3 LWAPP discovery response. This example output of the **debug lwapp events enable** command shows this discovery process:

```
(Cisco Controller) >debug lwapp events enable
Mon May 22 12:00:21 2006: Received LWAPP DISCOVERY REQUEST from AP
00:0b:85:5b:fb:d0 to ff:ff:ff:ff:ff:ff on port '1'
Mon May 22 12:00:21 2006: Successful transmission of LWAPP Discovery-Response
to AP 00:0b:85:5b:fb:d0 on Port 1
```

The **debug lwapp packet enable** command output for the local subnet broadcast discovery looks like this example:

```
(Cisco Controller) >debug lwapp packet enable
Tue May 23 12:37:50 2006: Start of Packet
Tue May 23 12:37:50 2006: Ethernet Source MAC (LRAD):      00:0B:85:51:5A:E0
Tue May 23 12:37:50 2006: Msg Type       :
Tue May 23 12:37:50 2006:    DISCOVERY_REQUEST
Tue May 23 12:37:50 2006: Msg Length     :   31
Tue May 23 12:37:50 2006: Msg SeqNum     :   0
Tue May 23 12:37:50 2006:
        IE             :   UNKNOWN IE 58
Tue May 23 12:37:50 2006:       IE Length     :   1
Tue May 23 12:37:50 2006:       Decode routine not available, Printing Hex Dump
Tue May 23 12:37:50 2006: 00000000: 00
```

Notice the lines that are marked in boldface. The value of the **IE 58** parameter indicates the discovery type:

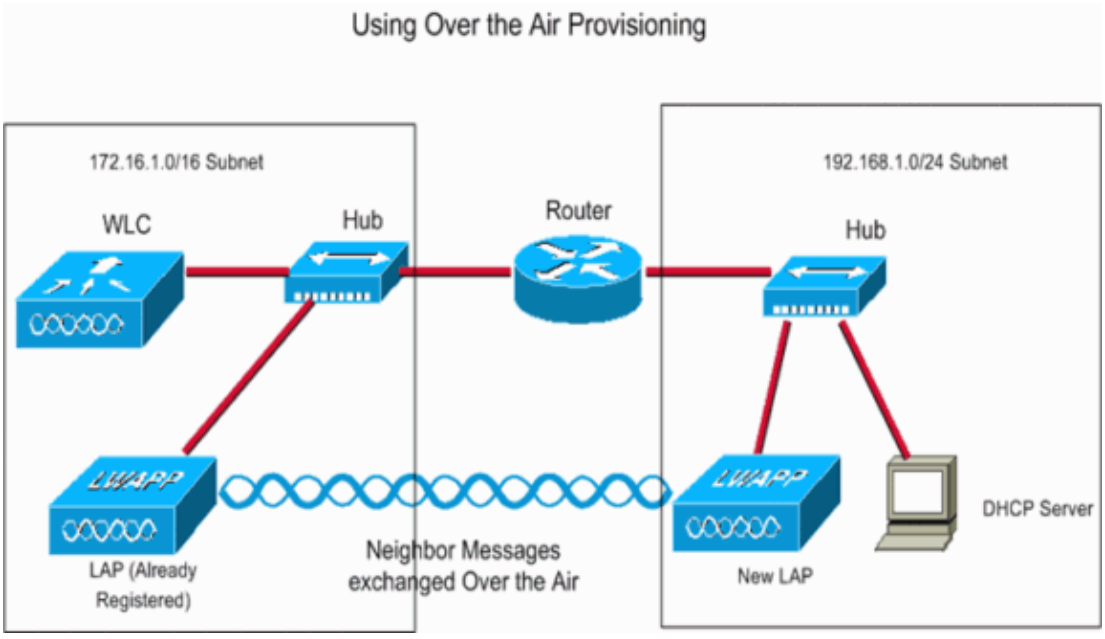
0 – broadcast
1 – configured
2 – OTAP
3 – dhcp server
4 – dns

Because this is a local subnet broadcast, the **IE 58** parameter value is **0** in this **debug lwapp packet enable** command output.

2. LAPs also use the Over−the−Air Provisioning (OTAP) feature in order to discover the WLC. The OTAP feature is *disabled by default* in 4.2.39.13, 5.0.68.0 and later WLC versions. OTAP is *enabled by default* in the WLC versions earlier than 4.2.39.13.. This is the discovery process when OTAP is enabled:

    a. The LAPs that are already registered to the WLC can advertise the WLC IP address to the LAPs (in an attempt to find the WLC) with the use of neighbor messages that are sent over the air.
    b. New LAPs that attempt to discover WLCs hear these messages and then unicast LWAPP discovery request messages to the WLCs.
    c. WLCs that receive the LWAPP discovery message reply with a unicast LWAPP discovery response message to the LAP.

You should have OTAP enabled only during AP provisioning intervals. After APs are deployed, disable OTAP as a deployment best practice. Also, Cisco Aironet LAPs (1130 AG, 1200, and 1240 AG series) ship from the factory with a stripped−down version of lightweight Cisco IOS® Software that is called the LWAPP Recovery Cisco IOS image. OTAP is not supported on those APs out−of−the−box that run LWAPP Cisco IOS Software. When you upgrade Cisco Aironet APs from autonomous Cisco IOS Software to lightweight mode, the LWAPP Recovery Cisco IOS image is the software that is loaded. The LWAPP Recovery Cisco IOS image does not support OTAP. In order to support OTAP, Aironet LAPs must first join a WLC in order to download a full LWAPP Cisco IOS image.



Here is an example. Assume that, in the subnet 172.16.1.0/16, you have an LAP that is already registered with the WLC, and OTAP is enabled on the WLC. When the new LAP in the 192.168.1.0/24 subnet comes up, the LAP looks for a DHCP server and gets an IP address (if no assignment was made previously with a static IP address). The LAP then sends out a discovery request to the local subnet. Because in this scenario there is no WLC in the local subnet, the LAP tries to use OTAP in order to discover WLCs. The LAP listens to neighbor messages that are sent over the air by the LAPs (in the 172.16.1.0/16 subnet) that are already registered and looks for WLC IP addresses. From the list of WLC IP addresses that the new LAPs learn from the neighbor messages, the new LAPs send out a Layer 3 LWAPP discovery request to the WLCs. The WLCs that receive this discovery request respond with a Layer 3 LWAPP discovery response. This **debug lwapp event enable** command output illustrates the sequence of messages that the WLCs send:

```
Tue May 23 14:37:10 2006: Received LWAPP DISCOVERY REQUEST from AP
00:0b:85:5b:fb:d0 to 00:0b:85:33:84:a0 on port '1'
Tue May 23 14:37:10 2006: Successful transmission of LWAPP Discovery-Response to
AP 00:0b:85:5b:fb:d0 on Port 1
```

Note: Because the LAP knows the WLC IP address through neighbor messages, the LAP sends a unicast discovery request to the WLC. In this way, this step is unlike the method in step 1 of this procedure, in which the LAP sends out a local subnet broadcast.

Note: The value of the **IE 58** parameter in the **debug lwapp packet enable** command output shows you that the LAP used OTAP as the discovery method.

```
Tue May 23 14:21:55 2006: Start of Packet
Tue May 23 14:21:55 2006: Ethernet Source MAC (LRAD):      00:D0:58:AD:AE:CB
Tue May 23 14:21:55 2006: Msg Type       :
Tue May 23 14:21:55 2006:    DISCOVERY_REQUEST
Tue May 23 14:21:55 2006: Msg Length     :   31
Tue May 23 14:21:55 2006: Msg SeqNum     :   0
Tue May 23 14:21:55 2006:
        IE             :   UNKNOWN IE 58
Tue May 23 14:21:55 2006:       IE Length     :   1
Tue May 23 14:21:55 2006:       Decode routine not available, Printing Hex Dump
Tue May 23 14:21:55 2006: 00000000: 02
Tue May 23 14:21:55 2006:
```

3. If the LAP was registered to a WLC in a previous deployment, the LAP maintains the list of WLC IP addresses locally in NVRAM. The stored WLC IP addresses include all of the WLCs that are in previously joined WLC "mobility groups". This is the discovery process:

    a. LAPs send a unicast Layer 3 LWAPP discovery request to each of the WLC IP addresses that the LAP has in its NVRAM.
    b. WLCs that receive the LWAPP discovery message reply with a unicast LWAPP discovery response message to the LAP.

    Here is example output of the **debug lwapp events enable** command and the **debug lwapp packet enable** command for this method of WLC discovery:

    Note: If you use the **clear ap-config** *ap_name* command in order to reset the LAP to the factory defaults, all the LAP configurations are reset. The configurations that are reset include the WLC IP addresses that are stored in NVRAM. In this case, the LAP must use some other method in order to discover the WLC.

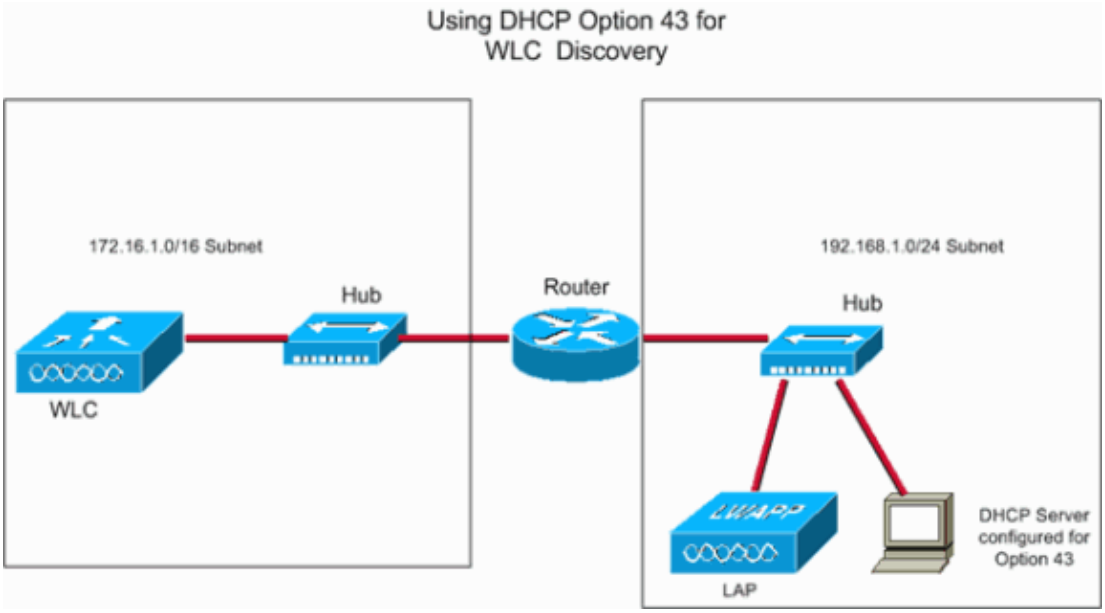
    ```
    (Cisco Controller) >debug lwapp events enable
    Tue May 23 14:37:10 2006: Received LWAPP DISCOVERY REQUEST from AP
    00:0b:85:5b:fb:d0 to 00:0b:85:33:84:a0 on port '1'
    Tue May 23 14:37:10 2006: Successful transmission of LWAPP Discovery-Response to
    AP 00:0b:85:5b:fb:d0 on Port 1

    (Cisco Controller) >debug lwapp packet enable
    Tue May 23 14:45:36 2006: Start of Packet
    Tue May 23 14:45:36 2006: Ethernet Source MAC (LRAD):      00:D0:58:AD:AE:CB
    Tue May 23 14:45:36 2006: Msg Type       :
    Tue May 23 14:45:36 2006:    DISCOVERY_REQUEST
    Tue May 23 14:45:36 2006: Msg Length     :   31
    Tue May 23 14:45:36 2006: Msg SeqNum     :   0
    Tue May 23 14:45:36 2006:
            IE             :   UNKNOWN IE 58
    Tue May 23 14:45:36 2006:       IE Length     :   1
    Tue May 23 14:45:36 2006:       Decode routine not available, Printing Hex Dump
    Tue May 23 14:45:36 2006: 00000000: 01
    Tue May 23 14:45:36 2006:
    ```

4. You can also program DHCP servers to return WLC IP addresses in the vendor-specific "option 43"

in the DHCP offer to LAPs. This is the discovery process:

a. When an LAP gets an IP address from the DHCP server, the LAP looks for WLC IP addresses in the option 43 field of the DHCP offer.
b. The LAP sends a Layer 3 LWAPP discovery request to each of the WLCs that are listed in the DHCP option 43.
c. WLCs that receive the LWAPP discovery message reply with a unicast LWAPP discovery response message to the LAP.

Note: You can use DHCP option 43 when the LAPs and the WLCs are in different subnets.



Here is an example scenario. Assume that you have a WLC in one subnet (as an example, 172.16.1.0/16) and the LAPs and the DHCP server in a different subnet (for example, 192.168.1.0/24). Routing is enabled between the two subnets. You can configure the DHCP server to return the WLC IP addresses to the LAP in the DHCP offer message. You can use any DHCP server that supports option 43.

Note: Refer to DHCP OPTION 43 for Lightweight Cisco Aironet Access Points Configuration Example for information on how to configure the Windows 2000 DHCP Server for option 43.

So, when the LAP powers up, it looks for a DHCP server in order to get an IP address. The DHCP server allots an IP address to the LAP and also provides the list of WLC IP addresses with the use of DHCP option 43. The LAP sends out a unicast discovery request to each of the WLCs. The WLCs that hear these messages reply with a discovery response, which initiates the registration process. This **debug lwapp events enable** command output shows the sequence of LWAPP messages:

```
Tue May 23 14:43:42 2006: Received LWAPP DISCOVERY REQUEST from AP
00:0b:85:5b:fb:d0 to 00:0b:85:33:84:a0 on port '1'
Tue May 23 14:43:42 2006: Successful transmission of LWAPP Discovery-Response to
AP 00:0b:85:5b:fb:d0 on Port 1
```

Here is **debug lwapp packet enable** command output that indicates that DHCP option 43 was used as the discovery method in order to discover WLC IP addresses:

```
Tue May 23 16:14:32 2006: Start of Packet
Tue May 23 16:14:32 2006: Ethernet Source MAC (LRAD):      00:D0:58:AD:AE:CB
Tue May 23 16:14:32 2006: Msg Type       :
Tue May 23 16:14:32 2006:    DISCOVERY_REQUEST
Tue May 23 16:14:32 2006: Msg Length     :   31
```

```
Tue May 23 16:14:32 2006: Msg SeqNum     :   0
Tue May 23 16:14:32 2006:
IE            :   UNKNOWN IE 58
Tue May 23 16:14:32 2006:       IE Length     :   1
Tue May 23 16:14:32 2006:       Decode routine not available, Printing Hex Dump
Tue May 23 16:14:32 2006: 00000000: 03
Tue May 23 16:14:32 2006:
```

5. Finally, you can also use the DNS server in order to return WLC IP addresses to the LAP. This is the discovery process:

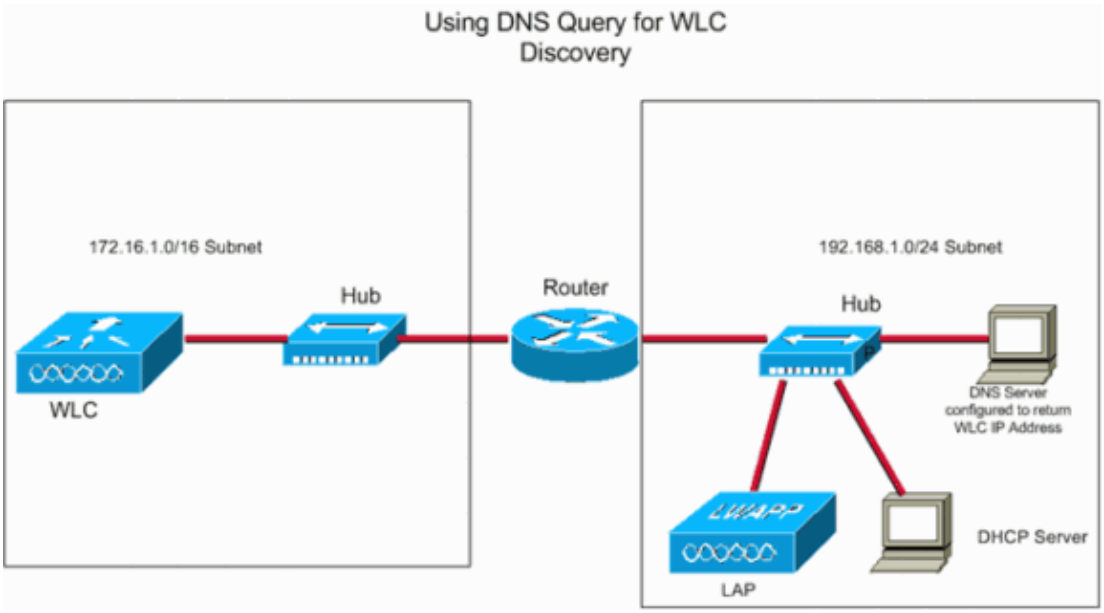
    a. The LAP attempts to resolve the DNS name "CISCO−LWAPP−CONTROLLER.localdomain."

    Note: In this DNS name syntax, localdomain refers to the domain name that needs to be resolved. For example, if the domain is cisco.com, then this DNS name is CISCO−LWAPP−CONTROLLER.cisco.com. The AP needs to be informed about the domain name that needs to be resolved so that the AP can send the request to the DNS server that made the request to resolve this particular domain name. The AP is informed of this domain name through DHCP option 15. DHCP option 15 specifies the domain name that the AP should use for DNS resolution. Therefore, it is necessary that DHCP option 15 be configured with the domain name information. This allows the DHCP server that sends the IP address of the DNS server to also send this DHCP option 15 information (the domain name to be resolved) to the AP.

    b. When the LAP is able to resolve this name to one or more WLC IP addresses, the LAP sends a unicast Layer 3 LWAPP discovery request to each of the WLCs.

    c. The WLCs that receive the LWAPP discovery message reply with a unicast LWAPP discovery response message to the AP.

This example uses the same setup that was used for DHCP option 43 (step 3). However, in this example, the DHCP server does not use option 43. Instead, the DHCP server provides the LAP with an IP address and also gives the IP address of the DNS server in the DHCP offer. After the LAP gets the DNS server IP address, the LAP sends out a DNS query for the DNS name CISCO−LWAPP−CONTROLLER.localdomain. The DNS server should be configured such that it returns the WLC IP address for this query. When the LAP gets the WLC IP address, the LAP starts the registration process with the WLC.



This **debug lwapp packet enable** command output shows the discovery type as DNS:

```
Tue May 23 16:14:32 2006: Start of Packet
Tue May 23 16:14:32 2006: Ethernet Source MAC (LRAD):      00:D0:58:AD:AE:CB
Tue May 23 16:14:32 2006: Msg Type       :
Tue May 23 16:14:32 2006:    DISCOVERY_REQUEST
Tue May 23 16:14:32 2006: Msg Length     :   31
Tue May 23 16:14:32 2006: Msg SeqNum     :   0
Tue May 23 16:14:32 2006:
IE            :   UNKNOWN IE 58
Tue May 23 16:14:32 2006:       IE Length     :   1
Tue May 23 16:14:32 2006:       Decode routine not available, Printing Hex Dump
Tue May 23 16:14:32 2006: 00000000: 04
Tue May 23 16:14:32 2006:
```

Note: If, after the completion of steps 1 through 5, the LAP does not receive an LWAPP discovery response, the LAP resets and restarts the hunting algorithm.

6. **Use IP helper address on the Router**

   Although this is not a part of the Layer 3 discovery algorithm, this is a simpler method that can be used when WLC and LAPs are in different subnets. After the LAP gets an IP address from the DHCP server, the LAP broadcasts a Layer 3 LWAPP discovery message on to its local subnet. The IP address of the WLC is configured as the *ip−helper* address on the router. The router forwards these broadcasts to the IP addresses configured with the *ip−helper* command on the *interface* on which the broadcast is heard. When you use the *ip helper−address* command, DIRECTED BROADCASTS, as well as unicasts, eight different UDP ports are forwarded automatically. Those ports are Trivial File Transfer (TFTP) (Port 69), Domain Name System (Port 53), Time Service (Port 37), NetBIOS Name Server (Port 137), NetBIOS Datagram Server (Port 138), Boot Protocol (BOOTP) Client and Server (Port 67 and Port 68), TACACS service (Port 49). Since LWAPP broadcast uses UDP port *12223* it must be explicitly forwarded on the router. Here is an example scenario. Assume that you have a WLC in one subnet, such as 172.16.0.0/16, and the LAPs and the DHCP server in a different subnet, such as 192.168.1.0/24. Routing is enabled between the two subnets. This example shows the configuration on the router:

```
Router(config)#interface Fastethernet 0/1
Router(config−if)#ip helper−address 172.16.0.1

!−−− IP address of the WLC

Router(config−if)#exit
Router(config)ip forward−protocol udp 12223
```

WLC Selection Process

After the LAP completes steps 1 to 5 of the Layer 3 LWAPP WLC Discovery Algorithm, the LAP selects a WLC from the candidate WLC list and sends that WLC an LWAPP join request.

WLCs embed this important information in the LWAPP discovery response:

- The controller sysName
- The controller type
- The controller AP capacity and its current AP load
- The Master Controller flag
- An AP−manager IP address

The LAP uses this information to make a controller selection, with use of these precedence rules:

1. If the LAP has previously been configured with a primary, secondary, and/or tertiary controller, the LAP examines the controller sysName field (from the LWAPP discovery responses) in an attempt to

find the WLC that is configured as primary . If the LAP finds a matching sysName for the primary controller, the LAP sends an LWAPP join request to that WLC. If the LAP cannot find its primary controller or if the LWAPP join fails, the LAP tries to match the secondary controller sysName to the LWAPP discovery responses. If the LAP finds a match, it then sends an LWAPP join to the secondary controller. If the secondary WLC cannot be found or the LWAPP join fails, the LAP repeats the process for its tertiary controller.

2. The LAP looks at the Master Controller flag field in the LWAPP discovery responses from the candidate WLCs if one of these items is true:

    - No primary, secondary, and/or tertiary controllers have been configured for an AP.
    - These controllers cannot be found in the candidate list.
    - The LWAPP joins to those controllers have failed.

    If a WLC is configured as a Master Controller, the LAP selects that WLC and send it an LWAPP join request.
3. If the LAP cannot successfully join a WLC on the basis of the criteria in step 1 and step 2, the LAP attempts to join the WLC that has the greatest excess capacity.

After the LAP selects a WLC, the LAP sends an LWAPP join request to the WLC. In the LWAPP join request, the LAP embeds a digitally signed X.509 certificate. When the certificate is validated, the WLC sends an LWAPP join response in order to indicate to the LAP that it is successfully joined to the controller. The WLC embeds its own digitally signed X.509 certificate in the LWAPP join response that the LAP must validate. After the LAP validates the WLC certificate, the LWAPP join process is complete.

The LAP and Wireless LAN Controller handle fragmentation and reassembly for the LWAPP tunnel. They operate under the 1500 byte MTU assumption. It is not a configurable parameter. At the AP or WLC, if the MTU is bigger than 1500 bytes, it fragments the packet and sends the packet across. The system handles up to four fragments as of Version 3.2. Earlier versions support up to only two fragments.

Troubleshoot

The controller has firmware version 3.2.78.0. When you run the **debug lwapp events** command, this output appears:

```
Sun Sep 3 21:49:51 2006 [ERROR] spam_lrad.c 2544:
         Security processing of Image Data failed from AP 00:17:59:67:76:80
```

This error message means that the image 3.2.78.0 does not support the LAP. Essentially, the controller cannot find the image for the LAP in its list of images. Therefore, the LAP is not able to download the image from the WLC. In order to resolve this issue, upgrade the controller to 3.2.116.0 or later. This resolves the problem and the LAP joins the controller and downloads the image from the controller.

Sometimes, you can encounter this error message at your controller:

```
Received a Discovery Request with subnet broadcast with wrong AP IP address (source addres
```

This error message means that the controller received a discovery request through a broadcast IP address that has a source IP address (given), which is not in any configured subnets on the controller. It also means that the controller dropped the packet. This typically happens when the customer trunks all allowed VLANs instead of restricted them to wireless VLANs.

You can also encounter this error message:

```
Received a Discovery−Request from <source MAC address>
 for someone else (IP address).
```

It means that the controller received a discovery request where the destination IP address (given) is not its management IP address. It also means that the controller dropped the packet.

There are many reasons a Lightweight Access Point (LAP) can fail to join the WLC. Refer to Troubleshoot a Lightweight Access Point Not Joining a Wireless LAN Controller for information about some of the reasons a LAP fails to join a WLC and how to troubleshoot the issues.

AP Fail−over Between Different Mobility Groups

Consider this scenario. Mobility group **MG1** contains two controllers, C1 and C2. These controllers are deployed in one building, with LAPs load−balanced between the two. The branch office of the company deploys a third controller C3, and configures it for mobility group **MG2**.LAPs from that controller (C3) do not fail over to one of the other two controllers, but one day, when the Controller C3 reboots, the LAPs that were originally registered with C3 now register to C1 in mobility group **MG1**.

Now, even though the primary of the LAPs is C3, and there is no secondary or tertiary, the LAPs have joined C1; a reboot of the LAP does not bring it back to C3. What is the problem?

The reason behind this is that within the initial deployment, the company created one of two scenarios:

- A DNS entry for **CISCO−LWAPP−CONTROLLER.localdomain** to point to C1 or C2
- The addition of a DHCP option 43 to point to C1 or C2 to ease the initial installation. Once the installation of the first building was done, these entries were never removed.

Note: The AP can also learn of C1 or C2 controllers by any other method of discovery, such as L3 broadcast and OTAP, so make sure that the proper precautions are taken that the AP can only learn about controllers from one mobility group through any of the methods.

When controller C3 goes down, the LAPs that were connected to it reboot. They undergo their discovery process as outlined. They not only send discovery requests to those controllers in the NVRAM configuration, but also to the IP addresses learned through DNS and DHCP, which, as a result, include C1 or C2.

Since C3 is down at the time of discovery, the LAPs do not get a DISCOVERY RESPONSE, so they cannot proceed to join its configured primary controller and must join the controller they learned through DHCP or DNS.

Once these LAPs join C1 or C2, they download the new mobility group list, which includes IP addresses for only C1 and C2, so, if they are rebooted, they have no way to learn the IP address of C3 to which to send discovery requests; they cannot join that controller. The only way to bring the LAPs back to C3 is to add C3 to the mobility group list of C1 and C2 or to change option 43 or the DNS entry.

There are several ways to prevent such problems:

- It is suggested that DNS and DHCP options are used only within initial deployment and are removed once the network is configured. This way, APs on the network have no way to learn about other mobility groups.
- Separate the DHCP scopes or DNS domains. Have one scope for building 1 and another scope for building 2 in the corporate DHCP server; the administrator can configure different Option 43 IP addresses for each scope. The same applies for DNS domains; with a building1.companyname.com hostname for one building, and building2.companyname.com for another, you can have different options for CISCO−LWAPP−CONTROLLER for each subdomain.
- You can also use functions in the WLC to control some behaviors:

- In the case of APs with Self−Signed Certificates (SSC), only add the SSCs to the controllers you wish the APs to join.
- In the case of APs with Manufacturer−Installed Certificates (MIC), use the **Authorize APs against AAA function** on the WLC (with the **config auth−list ap−policy authorize−ap enable** command) to tell the controller to check whether it should accept the AP.

  In order to allow APs to join, use one of these options:

  - Add them to the authorization list of the WLC: use the **config auth−list add mic <MAC−Address>** command.
  - Add them as clients to the RADIUS server. The Called−Station−ID is the MAC address of the controller. If you separate the APs into groups, you can create policies to define which APs can authenticate against which Called−Station−IDs.

In order to get an LAP to join a controller that is not part of the mobility group of the currently joined controller, you need to make sure that the primary controller name is that of the controller to which you wish to send the LAP.

Once that is done, all you need to do is give the LAP a way to discover that controller. This can be done through any of the methods described in the WLC discovery algorithm as explained in this document.

Related Information

- **Controlling Lightweight Access Points**
- **Wireless LAN Controller and Lightweight Access Point Basic Configuration Example**
- **LWAPP Traffic Study**
- **Cisco Wireless LAN Controller Configuration Guide, Release 6.0**
- **Technical Support & Documentation − Cisco Systems**

Updated: Sep 12, 2008 Document ID: 70333