

# Hybrid Remote Edge Access Point (H-REAP) Basic Troubleshooting

Document ID: 83417

---

## Introduction

### Prerequisites

- Requirements
- Components Used
- Conventions

### Background Information

#### H-REAP Troubleshooting

- H-REAP Does Not Join the WLC
- Verification of the H-REAP Mode of Operation
- Console Commands of H-REAP are Not Operational and Return an Error
- Clients Cannot Connect to H-REAP
- Wireless Control System (WCS) Reports Incorrect Client Counts to AP in H-REAP

Mode

### Related Information

---

## Introduction

Hybrid Remote Edge Access Point (H-REAP) is a solution for branch office and remote office deployments. It enables customers to configure and control two or three access points (APs) in a branch or remote office from the corporate office through a wide area network (WAN) link without the need to deploy a controller in each office. This document discusses some of the common issues that can occur in a H-REAP environment. This document also provides information on how to troubleshoot these issues. Refer to H-REAP Design and Deployment Guide for H-REAP design considerations when you deploy H-REAP and Configuring Hybrid REAP on Cisco Wireless LAN Controllers for the configuration steps.

## Prerequisites

### Requirements

- Functional knowledge of H-REAP and its operating modes
- Knowledge of Lightweight Access Point (LAP) registration process to a controller

### Components Used

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

- Cisco 4400 and 2100 Series Wireless LAN Controllers (WLCs) that run Version 5.1
- Cisco 1130AG APs, 1240 AG APs, and 1250 APs
- Cisco 2800 and 3800 Series Routers that run Version 12.4

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

These are the restrictions to remember while you use H-REAP.

- H-REAP is supported only on the 1130AG, 1240AG, 1250, and AP801 access points and on the 2100 and 4400 series controllers, the Catalyst 3750G Integrated Wireless LAN Controller Switch, the Cisco Wireless Services Module (WiSM), and the Controller Network Module for Integrated Services Routers.
- Any security type that requires control over the data path, such as VPN, does not work with traffic on locally switched WLANs because the controller cannot exercise control over data that is not tunneled back to it. Any other security type works on either centrally or locally switched WLANs, provided that the path between the H-REAP and the controller is up. When this conduit is down, only a subset of these security options allows new clients to connect to locally switched WLANs.
- When a H-REAP access point enters standalone mode, WLANs that are configured for open, shared, WPA-PSK, or WPA2-PSK authentication enter the "local authentication, local switching" state and continue new client authentications.

In controller software release 4.2 or later, this is also true for WLANs that are configured for 802.1X, WPA-802.1X, WPA2-802.1X, or Cisco Centralized Key Management (CCKM). However, these authentication types require that an external RADIUS server be configured. Other WLANs enter either the "authentication down, switching down" state (if the WLAN was configured for central switching) or the "authentication down, local switching" state (if the WLAN was configured for local switching).

- With H-REAP in Connected mode, the controller is free to impose client exclusion/blacklisting to prevent some clients from associating with its APs. This function can occur either in automated or manual fashion. In regard to global and per-WLAN configurations, clients can be excluded for a host of reasons, which range from repeated failed authentication attempts to IP theft, as well as for any given amount of time. Clients can also be entered into this exclusion list manually. The use of this feature is only possible while the AP is in Connected mode. Clients that have been placed on this exclusion list remain unable to connect to the AP, even while it is in Standalone mode
- WLANs that use MAC Authentication (local or upstream) no longer allow additional client authentications when the AP is in Standalone mode, which is identical to the way a similarly configured WLAN with 802.1X or WebAuth operates in the same mode.
- WLC Versions 4.2.61.0 and later support fast secure roaming using CCKM. H-REAP mode supports Layer 2 fast secure roaming using CCKM. This feature prevents the need for full RADIUS EAP authentication as the client roams from one AP to another. In order to use CCKM fast roaming with H-REAP access points, you need to configure H-REAP groups.

## H-REAP Troubleshooting

There are a few common scenarios and situations that arise and prevent smooth H-REAP configuration and client connectivity. These are just a few such situations with their suggested troubleshooting steps.

### H-REAP Does Not Join the WLC

These are the basic reasons for a H-REAP not to join the WLC:

- H-REAP is unable to obtain an IP address to itself, or it has been assigned with an incorrect IP

address.

- There is not any layer-3 connectivity between H-REAP and the WLC.
- There is not a Lightweight Access Point Protocol (LWAPP) connectivity between the H-REAP and WLC.
- Other reasons are the H-REAP joining to a different controller, certificate mismatch, problem with WLC or H-REAP itself, etc.

Perform these steps to troubleshoot these problems:

1. Verify that H-REAP AP is assigned an IP address.

If DHCP is used through the console of the AP, verify that the AP gets an address with this command:

```
AP_CLI#show dhcp lease.
```

If the output of this command is none, it implies that DHCP addressing is not used for this AP.

Now, ensure that the static IP address is assigned to the AP in a proper way. This can be verified with this command:

```
AP_CLI#show lwapp ip config.
```

```
LWAPP Static IP Configuration
IP Address          10.77.244.222
IP netmask          255.255.0.0
Default Gateway     10.77.244.220
```

The output displays a static IP address of 10.77.244.222 assigned to the AP. If this is not the intended IP address to be assigned, correct the address to the intended value.

2. Verify the IP connectivity between the AP and the management interface of the controller.

Once the IP address has been verified, ping the management IP address of the controller to make sure that the AP can communicate with the controller. Use the ping command through the console of the AP with this syntax:

```
AP_CLI#ping 10.77.244.210
```

*!--- 10.77.244.210/27 is the example management interface IP address of the controller.*

If the ping is not successful, it indicates that there is a problem in the IP connectivity between AP and the controller. Ensure that the upstream network is properly configured and that WAN access back to the corporate network is up. Verify that the controller is operational and is **not** behind any **NAT/PAT** boundaries. Ping from the controller to the AP with the same syntax. Make sure the **MTU** for the path between the controller and the H-REAP is at a minimum of **1500**. This can be checked with the **ping -l 1500 <WLC Management IP >** command from a computer on the H-REAP side of the WAN.

Here is a sample output of the successful **ping** command:

```
ping -l 1500 10.77.244.210

Pinging 10.77.244.204 with 1500 bytes of data:

Reply from 10.77.244.210: bytes=1500 time=6ms TTL=252
Reply from 10.77.244.210: bytes=1500 time=6ms TTL=252
Reply from 10.77.244.210: bytes=1500 time=6ms TTL=252
Reply from 10.77.244.210: bytes=1500 time=6ms TTL=252
```

```
Ping statistics for 10.77.244.204:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
  Minimum = 6ms, Maximum = 6ms, Average = 6ms
```

3. Verify the LWAPP connectivity between the AP and the controller.

Once IP connectivity between the H-REAP and the controller has been verified, perform LWAPP debugs on the controller to confirm that LWAPP messages are communicated across the WAN and to identify related problems. On the controller, first create a MAC filter to limit the scope of the debug output. Use this command to limit the output of the subsequent command to a single AP:

```
AP_CLI#debug mac addr <AP s wired MAC address> .
```

Once this is set to limit debug output, turn on the LWAPP debugging with this command:

```
Controller_CLI#debug lwapp events enable.
```

You see debug messages similar to these:

```
-----
-----
Thu Mar 15 15:07:56 2007: 00:12:44:b2:ae:d0
Received LWAPP DISCOVERY REQUEST from AP 00:12:44:b2:ae:d0
to ff:ff:ff:ff:ff:ff on port '1'
Thu Mar 15 15:08:06 2007: 00:12:44:b2:ae:d0
Received LWAPP JOIN REQUEST from AP 00:12:44:b2:ae:d0
to 00:0b:85:33:84:a0 on port '1'
Thu Mar 15 15:08:06 2007: 00:12:44:b2:ae:d0
AP AP0012.d92b.3a5e: txNonce 00:0B:85:33:84:A0 rxNonce 00:12:44:B2:AE:D0
Thu Mar 15 15:08:06 2007: 00:12:44:b2:ae:d0
LWAPP Join-Request MTU path from AP 00:12:44:b2:ae:d0
is 1500, remote debug mode is 0
Thu Mar 15 15:08:06 2007: 00:12:44:b2:ae:d0 Successfully added NPU Entry
for AP 00:12:44:b2:ae:d0 (index 50)Switch IP: 10.77.244.211,
Switch Port: 12223, intIfNum 1, vlanId 0AP IP: 172.16.1.10, AP Port: 45989,
next hop MAC: 0 0:12:d9:2b:3a:5e
Thu Mar 15 15:08:06 2007: 00:12:44:b2:ae:d0
Successfully transmission of LWAPP Join-Reply to AP 00:12:44:b2:ae:d0
Thu Mar 15 15:08:06 2007: 00:12:44:b2:ae:d0
Register LWAPP event for AP 00:12:44:b2:ae:d0 slot 0
Thu Mar 15 15:08:06 2007: 00:12:44:b2:ae:d0
Register LWAPP event for AP 00:12:44:b2:ae:d0 slot 1
Thu Mar 15 15:08:08 2007: 00:12:44:b2:ae:d0
Received LWAPP CONFIGURE REQUEST from AP 00:12:44:b2:ae:d0 to 00:0b:85:33:84:a0
-----
-----
-----
```

This debug output indicates a successful transmission of LWAPP messages between the controller and the AP, followed by a successful Join request from the AP and the parallel Join reply from the controller. Later the AP gets registered with the controller.

If no such LWAPP debug messages are seen, ensure that the H-REAP has at least one method by which a controller can be discovered. If such methods are in place (like Local subnet broadcast, DHCP option 43, or DNS), verify that they are properly configured. If no other discovery method is in place, ensure that the IP address of the controller is manually entered into the AP through the console CLI.

```
AP_CLI#lwapp ap controller ip address <management interface Ip address of controller>
```

4. If you have manually configured the H-REAP, make sure you clear previously associated controller information when you move your AP to a different location in your network. This allows your AP to

associate with the controller in the new location. In order to clear the previous configuration, issue the **AP CLI#clear lwapp private-config** command. Then, verify whether or not the AP joins the correct controller.

In order to verify with which controllers the AP communicates, issue the **debug ip udp** command to the AP CLI. From the output of this command, view the source and destination addresses of each packet that traverses the IP stack of the AP.

This is an example:

**AP\_CLI#debug ip udp**

```
*Mar 15 16:41:47.999: UDP: sent src=10.77.244.222(45989), dst=10.77.244.211(12223)
, length=60
*Mar 15 16:41:47.999: UDP: sent src=10.77.244.222(45989), dst=10.77.244.210(12223)
, length=75
*Mar 15 16:41:48.000: UDP: rcvd src=10.77.244.211(12223), dst=10.77.244.222(45989)
, length=22
*Mar 15 16:41:48.000: UDP: rcvd src=10.77.244.210(12223), dst=10.77.244.222(45989)
, length=49
*Mar 15 16:41:57.778: UDP: sent src=10.77.244.222(45989), dst=10.77.244.211(12223)
, length=76
*Mar 15 16:41:57.779: UDP: rcvd src=10.77.244.211(12223), dst=10.77.244.222(45989)
, length=22
```

From this output, you can see that the UDP packets are sourced from the AP and that they reach the management interface (10.77.244.210) and AP manager interface (10.77.244.211) of the controller.

5. Troubleshoot certificate issues if the AP attempts to join the controller but fails.

If LWAPP messages are seen on the controller, but the AP fails to join, this is likely a certificate issue. For more LWAPP troubleshooting tips, which include troubleshooting certificate issues, refer to LWAPP Upgrade Tool Troubleshoot Tips.

6. One other reason that H-REAP APs do not join WLCs is if the Proxy ARP is disabled on the gateway for the H-REAP APs. From the AP console, this message is logged:

```
*Jul 29 14:04:10.897: LWAPP_CLIENT_ERROR_DEBUG:
Retransmission count for packet exceeded more than max(CHANGE_STATE_EVENT , 1)
```

This can be caused by Cisco bug ID CSCse92856. This problem applies only to AP1130 and AP1240. This problem does not apply to AP1000s, AP1100, or AP1200.

This problem occurs when these conditions are met:

- a. HREAP mode is used in the WLAN. Local mode is not affected by this issue. Native VLAN mapping is required.
- b. The APs have to be on a different IP subnet than the AP Manager of the WLCs.
- c. Proxy ARP is disabled on the default gateway for the AP.
- d. The H-REAP AP gets the default gateway from a DHCP server.

In order to resolve this issue, enable Proxy ARP on the default gateway router of the AP.

## Verification of the H-REAP Mode of Operation

Once the H-REAP has joined the correct controller, you can verify whether or not the H-REAP AP is connected to the controller at any time. In other words, you can verify in which mode the H-REAP AP functions. This can be verified with the **show lwapp reap status** command from the AP CLI.

## AP\_CLI#show lwapp reap status

```
AP Mode:          REAP, Connected
                  Radar detected on:
```

This output says that the H-REAP AP is in H-REAP mode and Connected mode. In other words, the WAN link between the AP and the controller is UP (connected), and the Operating mode is H-REAP.

## AP\_CLI#show lwapp reap status

```
AP Mode:          REAP, Standalone
                  Radar detected on:
```

This output says that the AP is in Standalone mode, which means that the WAN link between AP and controller is down. The AP Operating mode is REAP. This means that WLANs that are configured for local switching with local authentication are functional and allow new clients to this WLAN. Refer to H-REAP Modes of Operation Configuration Example in order to understand the different operating modes of H-REAP.

## Console Commands of H-REAP are Not Operational and Return an Error

Any configuration commands (either setting or clearing of the configuration) performed through the H-REAP CLI return the **ERROR!!! Command is disabled** message. This can occur for one of two reasons:

- H-REAP APs that are in the Connected mode (registered to the controller) do not allow any configurations to be set or cleared through the console. When the AP is in this state, configurations must be done through the controller interface. If access to configuration commands at the AP is required, ensure that the AP is in Standalone mode before you attempt to enter any configuration commands.
- Once an AP has connected or registered to a controller at any point, ensure that the default enable password of H-REAP, **Cisco**, is changed. If this default password is not changed, you cannot access the Console CLI of the H-REAP is moved to Standalone Mode. Enable password can only be set through the CLI of the controller to which the AP is connected. This command syntax can be used at the controller to set either the console password of an individual AP or the password to all the APs of the controller: (WLC\_CLI)>**config ap username** <user-id> **password** <passwd> {**all** | <AP name>}

Here is an example:

```
WLC-1>config ap username hreap
                  hreap appassword
```

**Note:** For an AP that has not had its console passwords set, be aware that this configuration is only sent to the AP when the command is entered at the controller. Any APs that subsequently join the WLC require the command to be entered again.

**Note:** These commands work on **Out-of-Box** H-REAPs even when the default password is not changed:

- ◆ **lwapp ap hostname** <name>
- ◆ **lwapp ap ip address** <AP's IP address> <subnet mask>
- ◆ **lwapp ap ip default-gateway** <Gateway's IP address>
- ◆ **lwapp ap controller ip address** <WLC IP address>
- ◆ **clear lwapp private-config**
- **Note:** In order to completely return the AP to factory defaults, upon AP boot, press the **Mode** button until the Ethernet light turns amber. On the 1131, this light is near the Mode button and is clearly

marked with Ethernet. On the 1242, this is under the white plastic facade and notated with an E. Release the Mode button and let the AP boot. The AP is returned to the interface, which is available through the IOS Recovery Image of the AP. Be aware that if the new configuration commands are desired, the AP needs to run Cisco IOS® Software Release 12.3(11)JX1 or later. This can be verified through the console of the AP by entering the **show version** command.

**Note:** All **show** and **debug** commands continue to work without a default password being set and while the AP is in Connected mode.

Only at this point can any LWAPP configurations be made.

## Clients Cannot Connect to H-REAP

If the wireless clients cannot connect to H-REAP, perform these steps:

1. Ensure that the WAN link between the Controller and H-REAP is up.
2. Verify that the AP has properly joined the controller and that the controller has at least one properly configured (and enabled) WLAN. Ensure that the **H-REAP** is in the Enabled state for locally switched WLANs
3. At the controller, configure the WLAN to broadcast its SSID to help troubleshoot this process. On the client end, verify if the client is able to find the AP with the SSID. Mirror the SSID name and security configuration of the WLAN on the client. Client-side security configurations are where the vast majority of connectivity problems reside.
4. Ensure that the clients on locally switched WLANs are properly IP addressed. If DHCP is used, make sure an upstream DHCP server is properly configured and that it provides addresses to the clients. If static addressing is used, ensure that the clients are properly configured for the correct subnet.
5. Ensure that UDP ports **12222** and **12223** are open on any intermediary firewalls.
6. In order to further troubleshoot client connectivity issues at the console port of the H-REAP, issue this command:

```
AP_CLI#show lwapp reap association
```

7. In order to debug the 802.11 connectivity issues of a client, issue this command:

```
AP_CLI#debug dot11 state enable
```

8. In order to debug the 802.1X authentication process and failures of a client, issue this command:

```
AP_CLI#debug dot1x events enable
```

## Wireless Control System (WCS) Reports Incorrect Client Counts to AP in H-REAP Mode

If your wireless environment is managed by Wireless Control System (WCS), sometimes this WCS can report incorrect clients to the H-REAP AP, as opposed to the correct client counts specified by the controller.

This problem is due to Cisco bug ID CSCsg48059 (registered customers only). WCS reports client counts that are too high when H-REAP is enabled on the controller. This is the workaround.

1. In order to find out how many clients are associated to the APs or the given controller, use the **WCS Monitor > Clients** feature.
2. Search by the AP or controller, which is limited by the radio type, to avoid duplicates.
3. Use the total number of items found as your true population number.

You can also use the WLC to find the correct client count.

## Related Information

- [Troubleshoot a Lightweight Access Point Not Joining a Wireless LAN Controller](#)
  - [Resetting the LWAPP Configuration on a Lightweight AP \(LAP\)](#)
  - [H-REAP Design and Deployment Guide](#)
  - [Configuring Hybrid REAP on Cisco Wireless LAN Controllers](#)
  - [H-REAP Modes of Operation Configuration Example](#)
  - [Configuring Hybrid REAP on WCS](#)
  - [Lightweight Access Point FAQ](#)
  - [Cisco Aironet Access Point FAQ](#)
  - [Cisco Wireless hardware Frequently Asked Questions](#)
  - [Wireless LAN Controller \(WLC\) Troubleshoot FAQ](#)
  - [Wireless Control System \(WCS\) Troubleshoot FAQ](#)
  - [Technical Support & Documentation – Cisco Systems](#)
- 

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2008 – 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

---

Updated: Oct 30, 2008

Document ID: 83417

---