



Cisco Unified Wireless Hybrid REAP

The Cisco Unified Wireless solution uses the Lightweight Access Point Protocol (LWAPP) between lightweight access points (APs) and a WLAN controller. In a typical centralized WLAN deployment, wireless user traffic and AP control and management traffic is tunneled between the AP and controller using LWAPP. The LWAPP tunnel can be established across Layer 2 or Layer 3 topologies. In a centralized architecture, the WLAN controller is responsible for the propagation of policies, QoS, and radio resource management information to each lightweight AP. The WLAN controller is also the sole point for ingress and egress of all wireless user traffic, and it ultimately enables mobility across a wireless enterprise through the use of LWAPP and Ethernet over IP (when roaming between controllers). However, when attempting to implement a centralized controller with lightweight APs that are deployed at remote branch locations, this architecture might not be a viable solution.

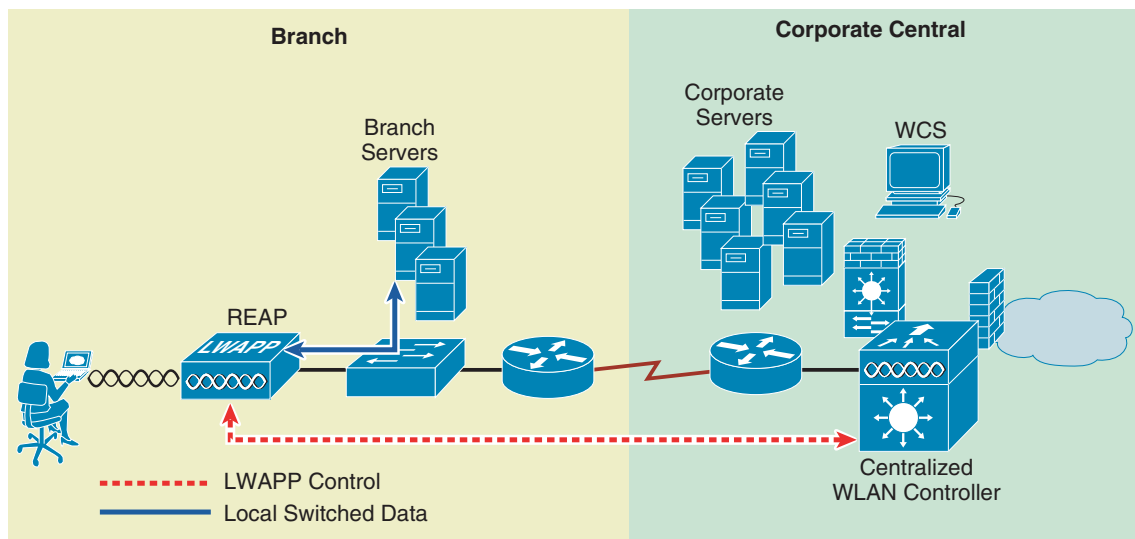
Remote Edge AP

Remote edge APs (REAPs) are special purpose LWAPP-based APs that are designed to be deployed in remote (branch) locations where:

- Fewer than three APs are needed to provide adequate wireless coverage for a given location. This is often more cost-effective than deploying and managing controllers at every location, especially if there are large numbers of small remote sites requiring wireless coverage.
- Wireless users at a branch or remote location require access to local network resources in addition to communicating back to a central site, or local wireless connectivity needs to be maintained during WAN link outages.
- Limited WAN bandwidth exists between the central site and a remote location where local connectivity is required. In this scenario, it would be impractical to tunnel all of the wireless user traffic to a centralized controller only to be routed back (in standard IP packets) across a bandwidth constrained WAN link to the remote site.

REAP APs are designed to address these remote branch needs by decoupling the LWAPP control plane from the wireless data plane. This allows WLANs to be terminated locally on a Layer 2 switch while LWAPP control and management data is tunneled back to a centralized WLAN controller. In this way, the benefits of a centralized architecture are preserved. [Figure 7-1](#) provides a high level REAP topology diagram.

Figure 7-1 High Level REAP Topology



The Cisco first generation REAP, the 1030, is capable of supporting up to 16 WLANs. Although all WLANs can be locally switched, the 1030 (when in REAP mode) has some limitations compared to a standard lightweight AP that is deployed in a conventional LWAPP/ controller topology. Specifically:

- It does not support 802.1Q trunking. All WLANs terminate on a single local VLAN/subnet.
- In the event of a WAN link outage all WLANs except WLAN 1 become disabled and are no longer beacons (if so enabled).

Cisco addressed these limitations with the introduction of a new version of REAP called Hybrid Remote Edge AP (H-REAP), which offers the ability to map WLANs to VLANs via 802.1Q trunking. Additionally, an H-REAP AP can support local switched and centrally switched WLANs concurrently. The remainder of this chapter focuses on application, features, limitations, and configuration of the H-REAP AP and, when applicable, highlights the differences between H-REAP and the older 1030 REAP platform.

Hybrid REAP

Supported Platforms

Controllers

H-REAP APs are supported by the following WLAN controller platforms with version 4.0 and later software images:

- Cisco 2000 Series
- Cisco 4400 Series
- Cisco 6500 Series (WISM)
- Cisco WLAN controller module for Integrated Service routers (ISR) Cisco C3750G-24WS

Access Points

The following IOS LWAPP APs support H-REAP functionality:

- Cisco 1130 Series
- Cisco 1240 Series

See [APs, page 2-10](#) for additional information on Cisco 1130 and 1240 series APs.

H-REAP functionality is not supported on Cisco 1000 Series LWAPP APs. However, basic REAP functionality is still supported.

H-REAP Terminology

This section provides a summary of H-REAP terminology and definitions.

Switching Modes

Unlike the 1030 Series REAP AP, which can map wireless user traffic only to a single VLAN, H-REAP APs are capable of supporting the following switching modes concurrently, on a per-WLAN basis:

- **Local Switched**—Local switched WLANs map wireless user traffic to discrete VLANs via 802.1Q trunking, either to a router or switch. One or more WLANs can be mapped to the same local 802.1Q VLAN.

A branch user who is associated to a local switched WLAN will have their traffic switched and forwarded by the on-site branch switch or router. Traffic destined off-site (to the central site) is forwarded as standard IP packets by the branch router.

All wireless control traffic is tunneled back to the centralized controller separately via LWAPP.

- **Central Switched**—Central switched WLANs tunnel both the wireless user traffic and all control traffic via LWAPP to the centralized controller where the user traffic is mapped to an interface or VLAN on the controller. This is normal LWAPP mode of operation.

The traffic of a branch user who is associated to a central switched WLAN will be tunneled directly to the centralized controller. If that user needs to communicate with computing resources within the branch (where that client is associated), their data must be forwarded as standard IP packets back across the WAN link to the branch location. Depending on the WAN link bandwidth, this might not be desirable behavior.

Operation Modes

Regardless of which switching mode is defined for a given WLAN, there is corresponding LWAPP control traffic that is sent to the controller. There are two modes of operation for an H-REAP AP:

- **Connected mode**—The controller is reachable. In this mode the H-REAP AP has LWAPP connectivity with its controller.
- **Standalone mode**—The controller is unreachable. The H-REAP has lost or failed to establish LWAPP connectivity with its controller. This would be the case when there is a WAN link outage between a branch and its central site.

Authentication Modes

The following are per-WLAN authentication modes:

- Authentication central—These are WLANs that require 802.1x, VPN, or web-based authentication services.
- Authentication local—Includes WLANs that use Open, Static, WEP or WPA PSK methods for authentication. H-REAP handles these locally, if the WAN link is down; otherwise, these are handled by the WLC.
- Authentication down—802.1x, VPN, or web authentication is unreachable because of the H-REAP AP being in standalone mode.

H-REAP States

An H-REAP WLAN, depending on its configuration and network connectivity, can be classified as being in one of the following states:

- Authentication-central / switch-central—WLAN uses centralized authentication services and user traffic is tunneled via LWAPP to the controller. Supported only when H-REAP is in Connected Mode (see [Figure 7-2](#)). 802.1X is used in this example, but other mechanisms are equally applicable.
- Authentication-central / switch-local—WLAN uses centralized authentication and user traffic is switched locally. Supported only when H-REAP is in Connected mode (see [Figure 7-3](#)). 802.1X is used in this example, but other mechanisms are equally applicable.
- Authentication-local / switch-local—WLAN uses local authentication: open, static wep or wpa psk and user traffic is switched locally at the branch. The H-REAP AP can be in connected mode or local mode (see [Figure 7-4](#)). If the AP is in connected mode, the authentication is processed by the WLC.
- Authentication-down / switch-local—An existing WLAN that requires central authentication will reject new users. Existing authenticated users continue to be switched locally. WLAN SSIDs continue to be beacons and respond to probes. The H-REAP AP is in standalone mode because the WLC is not accessible (see [Figure 7-5](#)).

Figure 7-2 Authentication-Central / Switch-Central WLAN

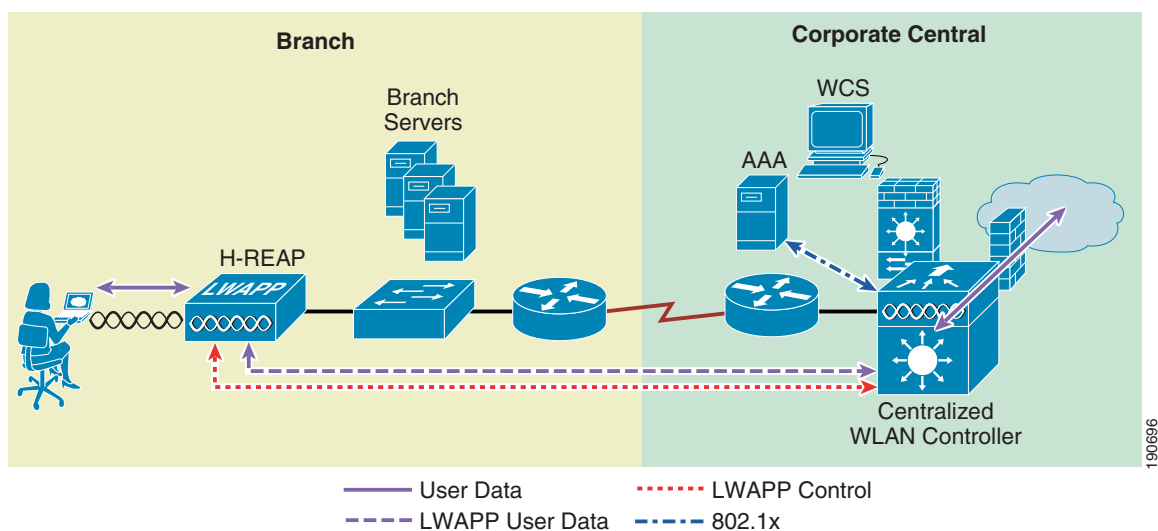


Figure 7-3 Authentication-Central / Switch-Local WLAN

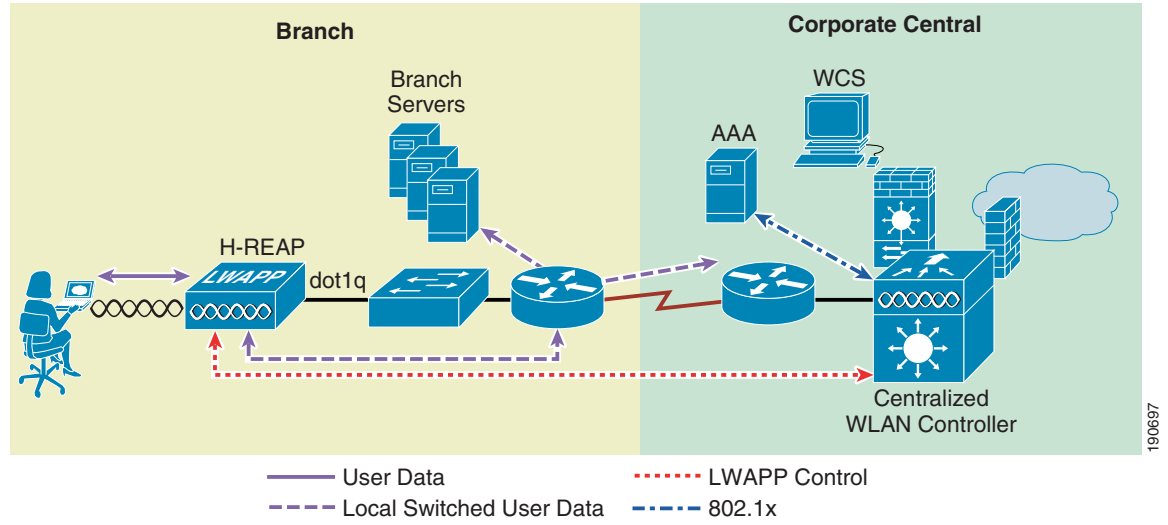


Figure 7-4 Authentication-Local / Switch-Local WLAN

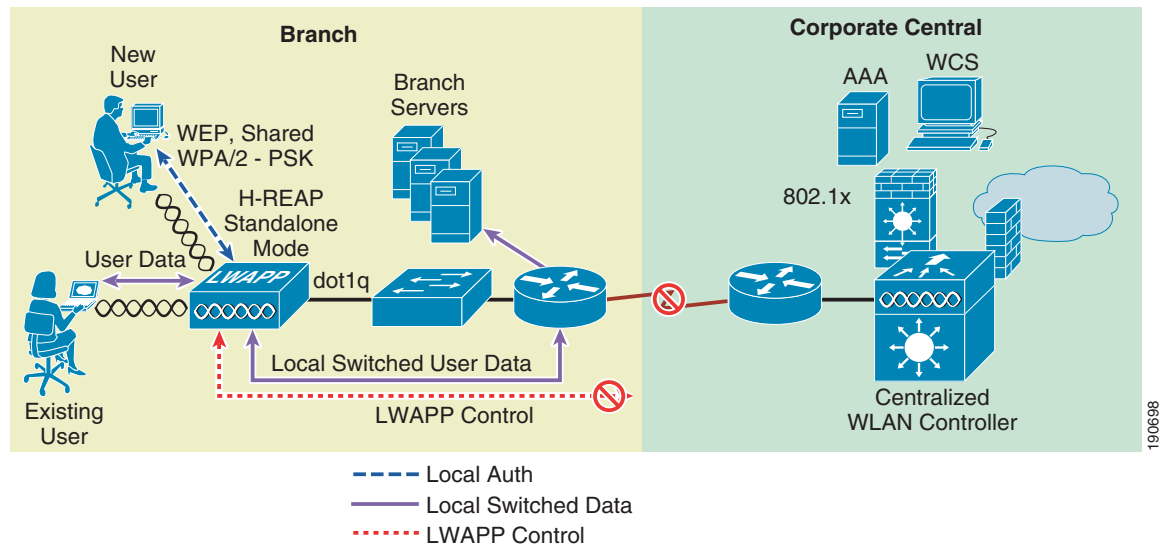
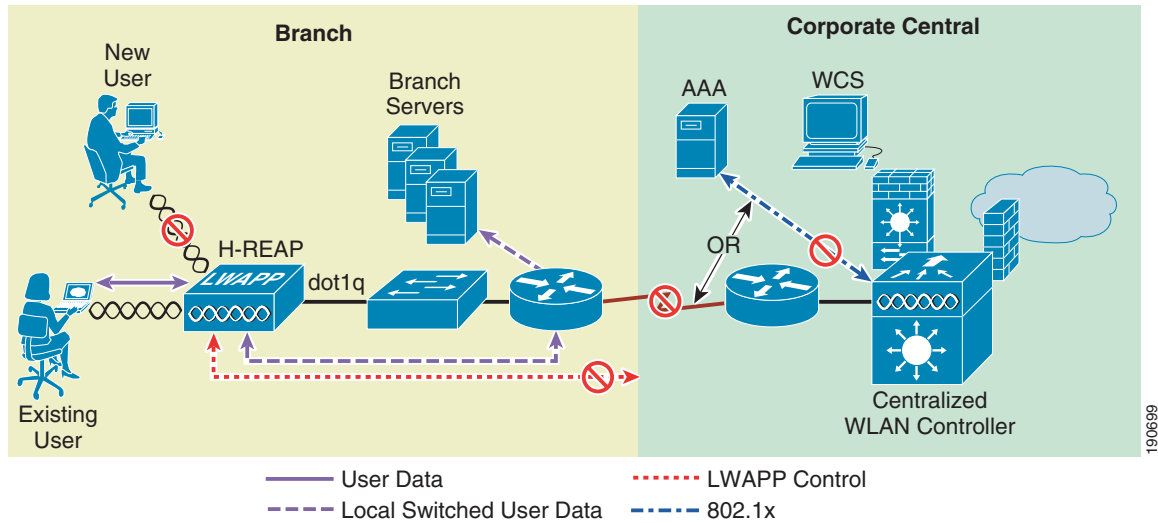


Figure 7-5 Standalone WLAN



Applications

With its expanded capabilities, the H-REAP AP offers great flexibility in how it can be deployed.

Branch Wireless Connectivity

The primary goal of REAP and H-REAP is to address the wireless connectivity needs in branch locations; permitting wireless user traffic to be terminated locally rather than be tunneled across the WAN to a central controller.

Because H-REAP can map individual WLANs to specific 802.1Q VLANs, branch locations can more effectively implement segmentation, access control, and QoS policies on a per-WLAN basis.

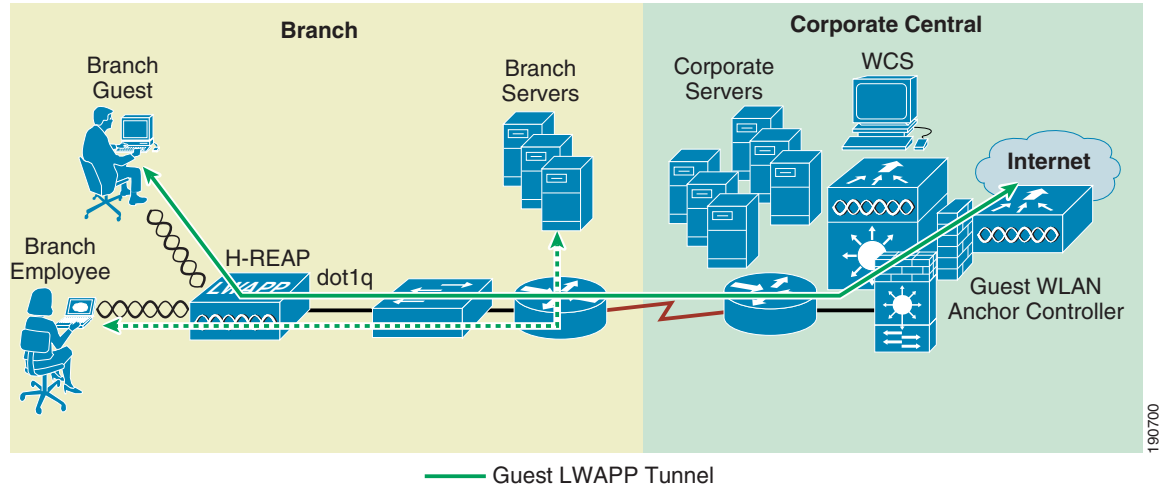
Branch Guest Access

One of the challenging aspects of using standard REAP APs in the branch is the implementation of guest access, which is difficult to implement for the following reasons:

- All WLANs map to the same local VLAN, thereby making it difficult to differentiate and segment guest users from branch users.
- All user traffic is switched locally, guest access traffic must somehow be segmented and routed back to the central site for access control and authentication, or if local Internet access is available at the branch, both segmentation and access control must be implemented locally.

The H-REAP AP helps overcome some of these challenges with the introduction of concurrent local and central switching. In an H-REAP topology, an SSID/WLAN designated for guest access can be tunneled via LWAPP to a central controller where its corresponding interface or VLAN can be switched directly to an interface of an access control platform, such as BBSM, SSG, or Clean Access. Or the centralized controller itself can perform web authentication for the guest access WLAN. In either case, the guest user's traffic is segmented (isolated) from other branch office traffic. Figure 7-6 provides an example of guest access topology using the H-REAP AP.

Figure 7-6 Branch Guest Access using H-REAP Central Switching



190700

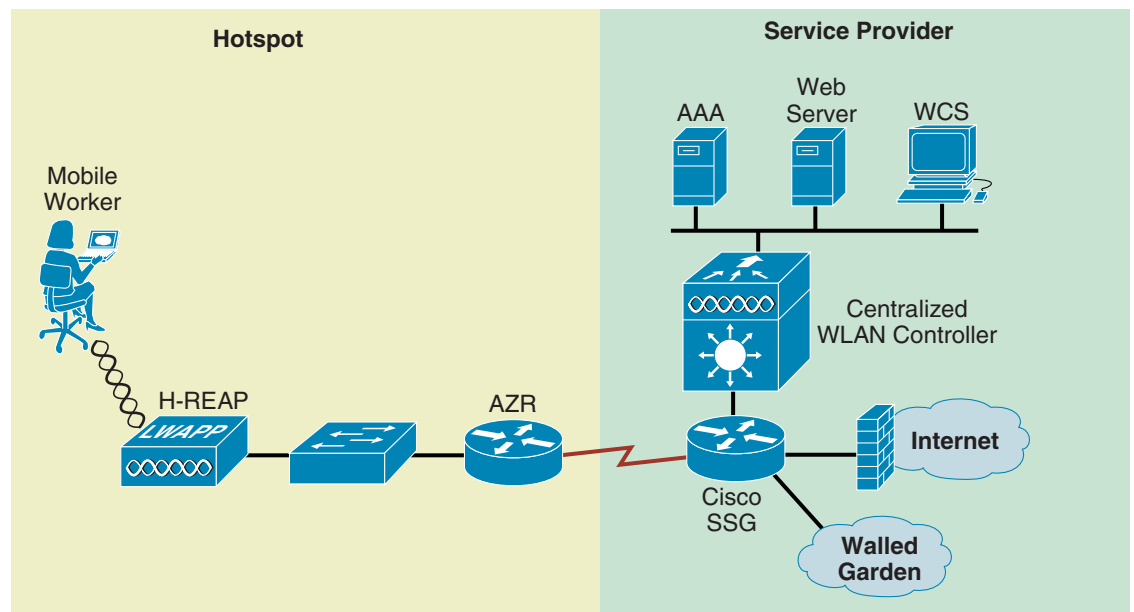
Public WLAN Hotspot

Many Public hotspot service providers are beginning to implement multiple SSID/WLANs. One reason for this is because an operator might want to offer an open authentication WLAN for web-based access and another WLAN that uses 802.1x/EAP for more secure public access.

The H-REAP AP, with its ability to map WLANs to separate VLANs, is now an alternative to an autonomous AP in small venue hotspot deployments where only one, or possibly two, APs are needed.

Figure 7-7 provides an example of hotspot topology using an H-REAP AP.

Figure 7-7 Hotspot Access using H-REAP Local Switching



190701

Deployment Considerations

The following section covers the various implementation and operational caveats that are associated with deploying H-REAP APs.

WAN Link

For the H-REAP AP to function predictably, there are a couple of things to keep in mind with respect to WAN link characteristics:

- **Latency**—A given WAN link should not impose latencies greater than 100 ms. The AP sends heartbeat messages to the controller once every thirty seconds. If a heartbeat response is missed, the AP will send five successive heartbeats (one per second) to determine if connectivity still exists. If connectivity is lost, then the H-REAP AP switches to standalone mode (see [Operation Modes, page 7-3](#) for operation mode definitions). The AP itself is fairly delay tolerant. It is on the client where timers associated with authentication are sensitive to link delay and thus a constraint of ≤ 100 ms is required. Otherwise, the client could timeout waiting to authenticate, which, in turn, could cause other unpredictable behaviors, such as looping.
- **Path MTU**—WLAN controller software images 4.0 and later, applying to both the 1030 REAP and H-REAP APs, required an MTU no smaller than 500 bytes.

Authentication Methods

See [Table 7-1](#) for a matrix of supported authentication methods based on the H-REAP mode of operation.

Table 7-1 Supported Authentication Modes

Authentication Method	Connected Mode	Standalone Mode	Notes
Open	Yes	Yes	
Shared	Yes	Yes	
EAP (TLS, PEAP, SIM and so on)	Yes	No	If the AP transitions to standalone mode, existing authenticated client sessions remain connected but no new authentications are possible.
WPA-802.1x	Yes	No	If the AP transitions to standalone mode, existing authenticated client sessions remain connected but no new authentications are possible.
WPA-PSK	Yes	Yes	
WPA2-802.1x	Yes	No	If the AP transitions to standalone mode, existing authenticated client sessions remain connected but no new authentications are possible.
WPA2-PSK	Yes	Yes	
Guest Access (Web Auth)	Yes	No	
VPN	Yes	No	
L2TP	Yes	No	
NAC	Yes	No	

Roaming

When an H-REAP AP is in Connected mode, all client probes (probe requests are handled at the AP, but are also forwarded to the WLC), association requests and response messages are passed between the H-REAP AP and the controller via the LWAPP control plane. This is also true for open, static wep, and wpa psk-based WLANs even though LWAPP connectivity is not required to support those authentication methods.

- **Dynamic WEP /WPA**—A client that roams between H-REAP APs using one of these key management methods must perform full authentication each time it roams, except in cases where the client supplicant supports Cisco CCKM. Otherwise, full 802.1x authentication is required (based on some EAP method) via the LWAPP control plane to an upstream AAA. After successful authentication, new keys are passed back to the AP and client. This behavior is the same as that in a traditional centralized WLAN deployment, except that in an H-REAP topology there can be link delay variations across the WAN, which can in turn impact total roam time.
- **WPA2**—To improve client roam times, WPA2 introduced key caching capabilities, based on IEEE's 802.11i specification. Cisco created an extension to this specification called Proactive Key Caching, or PKC. PKC today is supported only by Microsoft's Zero Config Wireless supplicant and Funk's (Juniper) Odyssey client. Cisco CCKM is also compatible with WPA2.

LWAPP APs support PKC—PKC capable clients that roam between LWAPP APs do not perform full 802.1x authentication. Instead, the client and AP recompute their PMKID using the PKC method and immediately begin key exchange. It should be noted that this exchange occurs between the AP and the controller via the LWAPP control plane so, while roam times can be improved, there is still a potential for link delay variations across the WAN, and it should also be noted that PKC is not supported for locally switched WLANs. Remote branch locations requiring predictable, fast roaming behavior should consider deploying a local WLAN controller, such as the Cisco WLC2006 or NM-WLC for Integrated Service routers.

- **Cisco Centralized Key Management (CCKM)**—H-REAP APs currently do not support CCKM fast roaming. As such, CCKM clients will undergo full 802.1x authentication every time they roam from one H-REAP to another.
- **Layer 2 Switch CAM Table Updates**—When a client roams from one AP to another on a locally switched WLAN, the H-REAP AP currently does not announce to a Layer 2 switch that the client has changed ports. The switch does not discover that the client has roamed until the client performs an ARP for its gateway router. This behavior, while subtle, can have an impact on roaming performance.

**Note**

H-REAP clients roaming on local switched WLANs where the APs reside on different subnets must renew their IP addresses when roaming to ensure they have an appropriate address for the network to which they have roamed.

WAN Link Disruptions

As described in sections [Operation Modes, page 7-3](#) through [H-REAP States, page 7-4](#), certain H-REAP modes and functionality require LWAPP control plane connectivity to the controller. Following is a summary of the features and functions that are impacted when the H-REAP is in Standalone mode.

EAP 802.1x and Web Auth WLANs

If existing local switched clients remain connected until the client roams or session re-authentication. No new client authentications are permitted.

If existing central switched clients are disconnected, no new client authentications are permitted.

As mentioned in [H-REAP States, page 7-4](#), open, static WEP, and WPA/2-PSK configured WLANs can function in either Connected or Standalone modes and therefore are not impacted in the same way as WLANs requiring RADIUS services, such 802.1x or web authentication. If there is a requirement for a remote branch location to maintain wireless connectivity during WAN link disruptions, we suggest that a backup WLAN be implemented based on one of the three Layer 2 security polices above. Of these, WPA/2-PSK offers the strongest security and therefore is strongly recommended.

Other Features

The following features are unavailable when an H-REAP is in standalone mode:

- Radio resource management DFS support is maintained
- Wireless intrusion detection
- Location-based services
- NAC
- Rogue detection
- AAA override

Radio Configuration

The following radio configuration information is maintained when an H-REAP is in standalone mode:

- DTIM
- Beacon period
- Short preamble
- Power level
- Country code
- Channel number
- Blacklist

H-REAP Limitations and Caveats

Local Switching Restrictions

If one of the following VPN security methods is configured on the controller for a specific WLAN, then that WLAN cannot be configured for local switching for use by an H-REAP AP:

- IPSEC
- L2TP
- PPTP
- CRANITE
- FORTRESS¹

**Note**

VPN pass-through to external aggregation platforms is permitted. However, controller-imposed VPN passthrough restriction is not permitted.

Max Supported WLANs

H-REAP APs support eight WLANs. Therefore, any WLAN that is expected to be supported by an H-REAP AP must fall within WLAN IDs 1–8. WLAN IDs 9–16 are not propagated.

Network Address Translation (NAT/PAT)

Controller

A controller cannot reside behind a NAT boundary when communicating with APs because LWAPP APs communicate with the controller in two phases using two different IP addresses:

- **Controller discovery**—An LWAPP AP initially queries a list of controllers using a controller's management IP address. The management IPs are learned via DHCP Option 43, DNS, or they can be configured manually (see [Initial Configuration, page 7-13](#)). The discovery phase is used to determine which controller, within the list of eligible controllers, the AP will join. This is conveyed by sending an LWAPP control message containing the eligible controller's AP management IP address.
- **Controller join**—The AP joins the eligible controller using the learned AP management IP address. The AP management IP address cannot be supported by NAT because the AP learns this address during the discovery phase. Even if 1:1 NAT relationships are established, the controller is not capable of passing the AP manager's outside NAT address as the IP address the AP should use to join the controller.

AP

See [Figure 7-8](#). A REAP or H-REAP AP can reside behind a NAT boundary in either of the following scenarios:

- If only one H-REAP AP resides behind a boundary, then PAT (NAT overload) can be used so long as port forwarding is enabled to map UDP ports 12222 and 12223 to the inside IP representing the H-REAP AP. We strongly recommend that the H-REAP be configured with a static IP address, or be given a static DHCP reservation to ensure that the NAT port mapping function works reliably. 1:1 NAT is also an option.
- If more than one H-REAP AP resides behind a boundary, only static 1:1 (inside to outside) NAT mapping can be used. Otherwise, PAT also operates correctly because of the unique UDP source port used by each AP. Multicast LWAPP messages do not correctly traverse NAT or PAT.

Figure 7-8 H-REAP with NAT/PAT

RADIUS Assigned VLANs

RADIUS-based VLAN assignment is supported for those H-REAP WLANs that are central-switched. This feature is not available when the H-REAP is in Standalone mode.

Web Authentication (Guest Access)

Controller-based web authentication may be used with local switched WLANs so long as the H-REAP is in Connected mode. Otherwise, those WLANs using web authentication are unavailable when the H-REAP is in Standalone mode.

Restricting Inter-Client Communication

Two or more clients, associated to a WLAN that is locally switched (by an H-REAP), are not prevented from communicating with one another even if Peer-to-Peer Blocking mode is enabled on the controller. This is because locally switched wireless traffic does not go through the controller. If it becomes necessary to block inter-client communication for a local-switched WLAN, then some kind of uRPF, such as ACL, can be applied at the ingress interface of the first Layer 3 hop.

Those H-REAP WLANs that are central switched have inter-client communication restricted based on the Peer-to-Peer Blocking mode setting on the controller.

H-REAP Scaling

- Per-Site—Sites requiring more than three APs should consider deploying a controller locally at the branch location. There are a few reasons for this:
 - Roaming performance—As described in [Roaming, page 7-9](#), roaming performance can be impacted by the availability and link characteristics of the WAN backhaul. This is true even when key caching methods, such as 802.11i or Cisco CCKM, are employed.

- Reliability—Branch WLAN topologies that depend on authentication, radio resource management and other upstream services are only as good as the availability of the WAN backhaul.
- WAN backhaul bandwidth consumption—As the number of H-REAP APs increases, bandwidth use also increases as a result of LWAPP control plane traffic. All client probes, association requests, and authentication-related messages result in LWAPP control and data traffic being sent across the WAN to the controller, even when WLANs are local switched.
- Per-controller—There are no restrictions with regard to the number of APs that can operate in H-REAP mode. The total number of H-REAP APs per controller is bound only by the maximum number of Lightweight APs that are supported for a given controller model.

Inline Power

The Cisco 1130 and 1240 Series APs support both the Cisco inline power specification and conform to the 802.3af standard, whereas the former Cisco 1030 Series REAP APs support 802.3af only.

Management

H-REAP APs can be managed and monitored either through the controller's GUI or Cisco Wireless Control System (WCS) in the same way that regular LWAPP APs are managed. The only exception is when the H-REAP APs become un-reachable due to WAN outages. For more information on management and WCS please see chapter X, section Y of this document.

H-REAP Configuration

Initial Configuration

An eligible Cisco 1130 or 1240 series AP requires the following minimum information to join a controller so that it can be configured for H-REAP operation:

- An IP address
- A default gateway address
- Management interface IP address of one or more controllers

The above information can be obtained in one of four ways:

- Static configuration via serial console port
- DHCP with statically configured controller addresses
- DHCP with DNS resolution for controller addresses, as discussed in [Chapter 2, “Cisco Unified Wireless Technology and Architecture”](#)
- DHCP with Option 43, as discussed in [Chapter 2, “Cisco Unified Wireless Technology and Architecture”](#)

Serial Console Port

Unlike the earlier 1030 series REAPs, The 1130 and 1240 series APs offer a serial console port that can be used to establish basic parameters for connectivity. Use the following steps to establish initial configuration using the console port method. The serial console port method can be used only when the AP is not actively joined with a controller when being configured and is running LWAPP image 12.3(11)JX or later.



Note

Complete [Step 4 a.](#) and [b.](#) only if DHCP will not be used at the branch to assign an IP address to the H-REAP AP. Care must be taken to ensure that the addresses used conform to the addressing scheme being used at the branch location.

-
- Step 1** Using a standard Cisco DB9/RJ45 console cable connect the AP to a laptop running Hyper Terminal or other compatible terminal communications software. As with all Cisco devices, the serial parameters need to be set at 9600bps, 8 data bits, 1 stop bit and No flow control.
- Step 2** Power on the AP. To configure the AP through the console port, it should not be connected to the network. Otherwise, if the AP discovers a controller and joins it, you will not be able to establish an exec session. Therefore, Cisco recommends that the AP remain disconnected from the network (Standalone mode) until the initial configuration has been completed.
- Step 3** After the AP has completed loading its local image, establish an exec session by typing **enable** and then entering **cisco** for the enable password.
- Step 4** At the <ap-mac-address># prompt, use the following commands to configure the IP, mask, gateway, hostname, and the primary controller:
- lwapp ap ip address** *ip-addr subnet-mask*
 - lwapp ap ip default-gateway** *ip-addr*
 - lwapp ap hostname** *ap-hostname* (optional)
 - lwapp ap controller ip address** *ip-addr*



Note

If DHCP services are used within the branch (see [DHCP with Statically Configured Controller IPs, page 7-15](#)) and you do not want to use DHCP Option 43 or DNS methods to issue controller management IP addresses, enter only the **lwapp ap controller ip address** *ip-addr* command from [Step 4](#).

The preceding commands are saved directly to NVRAM.

- Step 5** To review the static configuration, type the following command:

show lwapp ip config

Output similar to the following is displayed:

```
AP0014.1ced.494e# sho lwapp ip config
LWAPP Static IP Configuration
IP Address      10.20.104.50
IP netmask      255.255.255.0
Default Gateway 10.20.104.1
Primary Controller 10.20.30.41

AP0014.1ced.494e#
```

If an error has been made, repeat the commands listed in [Step 4](#) to correct.

Step 6 To clear one or more static entries, use the following commands:

- a. `clear lwapp ap ip address`
- b. `clear lwapp ap ip default-gateway`
- c. `clear lwapp ap controller ip address`
- d. `clear lwapp ap hostname`

When you are connected to the branch network, the AP boots and sends discovery requests to each controller defined in [Step 4 d](#). The AP then joins the least used controller.

DHCP with Statically Configured Controller IPs

This method uses DHCP to dynamically configure the AP with an IP address and default gateway. The DHCP service can be implemented locally or remotely using an external server or locally using DHCP services resident within IOS. The WLC management interface IP addresses can be manually configured using the APs console interface; this can either be done before shipping to the branch office or on site. See [Serial Console Port, page 7-14](#). When connected to the branch network, the AP boots and sends discovery requests to each controller defined. The AP then joins the least used controller.

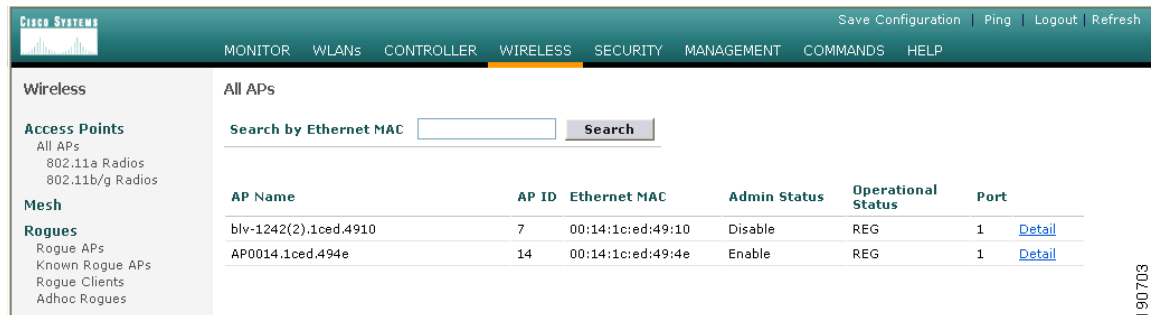
Configuring AP for H-REAP Operation

The following configuration tasks are accomplished using the wireless LAN controller GUI interface.

When an AP joins the controller for the first time it defaults to local AP mode. The AP must be set for H-REAP mode before local switching parameters can be established.

Step 1 From the controller **Wireless** configuration tab, locate the newly joined AP and click **Detail** (see [Figure 7-9](#)):

Figure 7-9 Wireless Configuration Tab



The screenshot shows the Cisco Wireless Configuration Tab interface. The 'Wireless' tab is selected, and the 'All APs' section is active. A search bar is present with the text 'Search by Ethernet MAC' and a 'Search' button. Below the search bar is a table listing APs with columns for AP Name, AP ID, Ethernet MAC, Admin Status, Operational Status, and Port. Two APs are listed: 'blv-1242(2).1ced.4910' and 'AP0014.1ced.494e'. The 'AP0014.1ced.494e' entry has a 'Detail' link next to its port number.

AP Name	AP ID	Ethernet MAC	Admin Status	Operational Status	Port
blv-1242(2).1ced.4910	7	00:14:1c:ed:49:10	Disable	REG	1 Detail
AP0014.1ced.494e	14	00:14:1c:ed:49:4e	Enable	REG	1 Detail

Step 2 Select **AP Mode, Name, Location, and Controller Priority**.

From the AP mode drop-down list, choose **H-REAP**. (See [Figure 7-10](#).)

Figure 7-10 Wireless Configuration—AP Mode

Optionally, configure an AP name or optionally configure a location name.

- Step 3** Identify the primary controller the AP should join and, optionally, a secondary and tertiary controller in the event the primary (or secondary) controller becomes unreachable.

These names are case-sensitive and correspond to the system name. If none of the named controllers are available, the AP will join one of the other controllers that belong to the mobility group based on automatic load balancing.

- Step 4** Click **Apply**.

The AP reboots and re-joins the controller in H-REAP mode.



Note

When the H-REAP AP reboots, its interface is not configured for 802.1q trunking mode. Ensure that the DHCP scope used for assigning addresses to H-REAP APs is configured on the native VLAN because the AP originates DHCP requests with no VLAN tag.

Enabling VLAN Support

After the H-REAP AP has joined the controller in H-REAP mode:

- Step 1** Find the AP under the controller Wireless settings and click **Details**.

Note that there are new H-REAP configuration settings presented in the AP details window. (See [Figure 7-11](#).)

- Step 2** Place a check mark in the **VLAN Support** check box.
Note that a Native VLAN ID definition window and a VLAN Mappings button are added.
- Step 3** Enter the VLAN number defined as the native VLAN.
- Step 4** Click **Apply**.

Figure 7-11 Wireless Settings

The screenshot shows the Cisco Wireless Settings page for an H-REAP AP. The page is divided into several sections:

- General:** AP Name (HREAP(1).1ced.494e), Ethernet MAC Address (00:14:1c:ed:49:4e), Base Radio MAC (00:14:1b:59:42:40), Regulatory Domain (80211bg: -A 80211a: -A), AP IP Address (10.20.104.57), AP Static IP (unchecked), AP ID (15), Admin Status (Enable), AP Mode (H-REAP), Mirror Mode (Disable), Operational Status (REG), Port Number (1), MFP Frame Validation (checked, Global MFP Disabled), AP Group Name (--), Location (Branch), Primary Controller Name (Controller1), Secondary Controller Name (Controller2), Tertiary Controller Name (Controller3), Statistics Timer (180).
- Versions:** S/W Version (4.0.126.0), Boot Version (12.3.7.1), IOS Version (12.3(20060502:110346)), Mini IOS Version (3.0.51.0).
- Inventory Information:** AP PID (AIR-LAP1242AG-A-K9), AP VID (0), AP Serial Number (FTX0942B055), AP Entity Name (Cisco AP), AP Entity Description (Cisco Wireless Access Point), AP Certificate Type (Manufacture Installed), H-REAP Mode supported (Yes).
- H-REAP Configuration:** VLAN Support (checked), Native VLAN ID (1). A **VLAN Mappings** button is located below this section.
- Power Over Ethernet Settings:** (Section header visible at the bottom).

Advanced Configuration

The following steps outline how to configure an H-REAP AP to perform local and or central switching in addition to highlighting any caveats associated with the configuration process.

Choosing WLANs for Local Switching

Before a WLAN can be mapped to a local VLAN on the H-REAP AP, the WLAN must first be made eligible for H-REAP local switching.

- Step 1** Click the **WLANs** tab.
- Step 2** Find the WLANs that need to be locally switched and click **Edit**. (See [Figure 7-12](#).)

Figure 7-12 WLANs Tab

The screenshot shows the Cisco Systems WLANs configuration page. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', and 'HELP'. The main content area displays a table of WLANs with columns for WLAN ID, WLAN SSID, Admin Status, and Security Policies. A 'New...' button is located in the top right corner. A red asterisk note at the bottom states: '* WLAN IDs 9-16 will not be pushed to 1130,1200 and 1240 AP models.'

WLAN ID	WLAN SSID	Admin Status	Security Policies			
1	SRND	Enabled	802.1X	Edit	Remove	Mobility Anchors
2	WEP	Enabled	WEP	Edit	Remove	Mobility Anchors
3	CCKM	Enabled	[WPA1][Auth(802.1x)]	Edit	Remove	Mobility Anchors
4	PKC	Enabled	[WPA1][Auth(802.1x)]	Edit	Remove	Mobility Anchors
5	WPA	Enabled	[WPA1][Auth(PSK)]	Edit	Remove	Mobility Anchors
6	guest	Enabled	Web-Auth	Edit	Remove	Mobility Anchors

Configuring H-REAP Support on a WLAN

Step 3 Place a check mark in the **H-REAP Local Switching** check box. (See Figure 7-13.)

Figure 7-13 WLANs—Edit

The screenshot shows the Cisco Systems WLANs Edit configuration page for WLAN ID 4 with SSID PKC. The page is divided into 'General Policies' and 'Security Policies' sections. The 'H-REAP Local Switching' checkbox is checked. The 'Security Policies' section includes options for IPv6 Enable, Layer 2 Security (WPA1+WPA2), Layer 3 Security (None), and Web Policy. A red asterisk note at the bottom states: '* Web Policy cannot be used in combination with IPsec and L2TP.' Another note states: '** When client exclusion is enabled, a timeout value of zero means infinity (will require administrative override to reset excluded clients)'. A third note states: '*** CKIP is not supported by 10xx APs'.

General Policies

- Radio Policy: All
- Admin Status: Enabled
- Session Timeout (secs): 1800
- Quality of Service (QoS): Silver (best effort)
- WMM Policy: Disabled
- 7920 Phone Support: Client CAC Limit AP CAC Limit
- Broadcast SSID: Enabled
- Aironet IE: Enabled
- Allow AAA Override: Enabled
- Client Exclusion: Enabled ** 60 Timeout Value (secs)
- DHCP Server: Override
- DHCP Addr. Assignment: Required
- Interface Name: wlan-int
- MFP Version Required: 1
- MFP Signature Generation: (Global MFP Disabled)
- H-REAP Local Switching:

Security Policies

- IPv6 Enable:
- Layer 2 Security: WPA1+WPA2 MAC Filtering
- Layer 3 Security: None Web Policy *

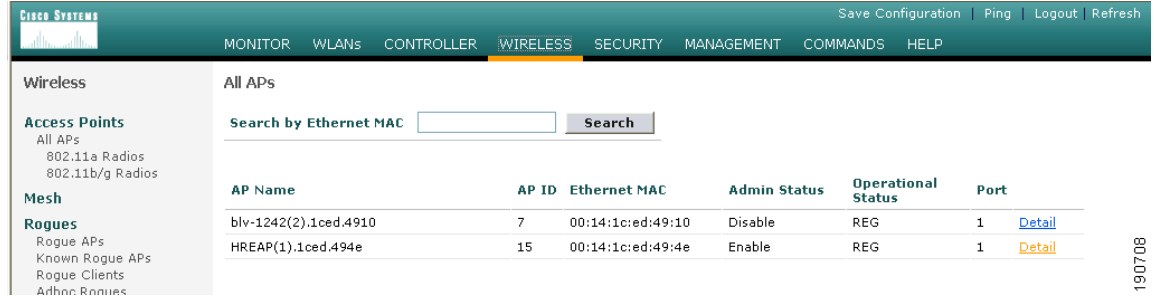
Step 4 Click **Apply**.

H-REAP Local Switching (VLAN) Configuration

After all eligible WLANs have been configured to support H-REAP, do the following:

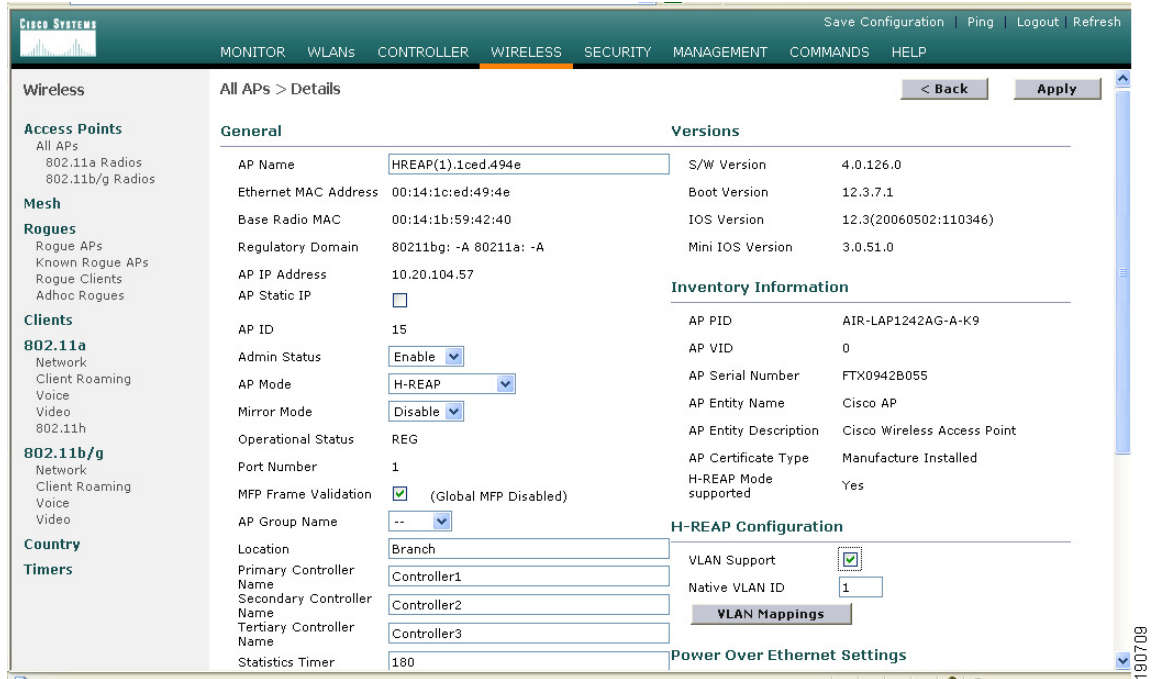
- Step 1** Click the **Wireless** tab.
- Step 2** From the list of APs, find the H-REAP and click **Detail**. (See [Figure 7-14](#).)

Figure 7-14 Wireless Tab—APs



- Step 3** From the AP Details configuration page, click **VLAN Mappings**. (See [Figure 7-15](#).)

Figure 7-15 All APs—Details



Establishing a WLAN to VLAN Mapping

The VLAN Mappings page displays all WLANs that have been configured for H-REAP switching, along with a configurable VLAN ID field. (See [Figure 7-16](#).)

Figure 7-16 VLAN Mappings

The screenshot shows the 'VLAN Mappings' configuration page for AP HREAP(1).1ced.494e. The page is divided into several sections:

- Wireless:** Shows the AP Name (HREAP(1).1ced.494e) and Base Radio MAC (00:14:1b:59:42:40).
- WLAN Mappings Table:**

WLAN Id	SSID	VLAN ID
3	CCKM	30
4	PKC	30
5	WPA	31
- Centrally Switched WLANs Table:**

WLAN Id	SSID	VLAN ID
1	SRND	N/A
2	WEP	N/A
6	guest	N/A



Note

The WLAN IDs that are displayed initially are inherited from the central controller WLAN interface settings.

Step 1

For each WLAN/SSID, configure a locally relevant VLAN number.

More than one WLAN can be mapped to local VLAN number.

Step 2

Click **Apply**.



Note

All WLANs shown in the grey box are centrally switched and might not be active, depending on whether the WLAN is enabled globally. All user traffic associated with a centrally switched WLAN are tunneled back to the controller.

Centrally switched WLANs can be excluded from the H-REAP by using the WLAN override feature to uncheck the WLANs that are not required.



Note

For each locally switched WLAN, there must be a DHCP helper address or local DHCP pool configured for the mapped VLAN.

H-REAP Verification

Verifying the H-REAP AP Addressing

- If using DHCP to assign an address, verify DHCP server configuration settings, correct subnet, mask, and default gateway.
- Ensure AP DHCP scope is defined on the native VLAN.
- If AP was configured with a static addresses, ensure AP address, subnet, mask and gateway are consistent with addressing scheme used within the branch location using the **show lwapp ip config** command. See [Serial Console Port, page 7-14](#) for more information.

Verifying the Controller Resolution Configuration

- If using DHCP Option 43/60 for controller resolution, verify that the VCI and VSA string format on the DHCP server is correct.
- Verify that the correct controller management IP address is configured in the DHCP server.
- If using DNS resolution, verify that a DNS query of CISCO-LWAPP-CONTROLLER@localdomain can be made from the branch location and resolves to one or more valid controller management IP address.
- Verify valid DNS server addresses are being assigned via DHCP
- If the controller IP was configured manually, verify the configuration via the serial console port with the AP disconnected from the network using the **show lwapp ip config** command. See [Serial Console Port, page 7-14](#) for more information.

Troubleshooting

This section provides troubleshooting guidelines for some common problems.

H-REAP Does Not Join the Controller

If an H-REAP AP is not joining the expected controller:

- Verify routing from the branch location to the centralized controller. Check that you can ping the Controller management IP address from the AP subnet.
- Verify that the LWAPP protocol (UDP ports 12222 and 12223) is not being blocked by an ACL or firewall
- Verify that the H-REAP hasn't joined another controller in the mobility group

Check to see whether a controller within the mobility group has been designated as “master controller”, which could cause an H-REAP to join a controller other than the one expected.

Client Associated to Local Switched WLAN Cannot Obtain an IP Address

- Verify that 802.1q trunking is enabled (and matches the AP configuration) on the switch and/or router ports to which the AP is connected.
- Verify that an IP helper address or local DHCP pool has been configured for the VLAN (sub-interface) at the first Layer 3 hop for the WLAN in question.

Client Cannot Authenticate or Associate to Locally Switched WLAN

If local switched WLAN uses central authentication:

- Verify H-REAP is not in Standalone mode (WAN backhaul down).
- Verify a valid RADIUS authentication server has been configured for the WLAN.
- Verify reachability to the RADIUS authentication server from the controller.
- Verify that the RADIUS server is operational.
- Verify that the authentication service and user credentials are configured on the RADIUS server.

If the local switched WLAN uses a pre-shared key:

- Verify that the WPA or WEP configuration on the client matches that of the WLAN.
- Verify if wireless client requires WLAN SSID to be broadcast (if disabled) to authenticate/associate.

Client Cannot Authenticate or Associate to the Central Switched WLAN

If the central switch WLAN uses central authentication:

- Verify H-REAP is not in Standalone mode (WAN backhaul down)
- Verify a valid RADIUS authentication server has been configured for WLAN
- Verify reachability to RADIUS authentication server from the Controller
- Verify that the RADIUS server is operational.
- For AAA authenticated clients, verify that authentication service and user credentials are configured on the RADIUS server.

If local switched WLAN uses a pre-shared key:

- Verify that the WPA or WEP configuration on the client matches that of the WLAN.
- Verify if wireless client requires WLAN SSID to be broadcast (if disabled) to authenticate / associate.

H-REAP Debug Commands

This section contains debug commands that can be used for advanced troubleshooting.

Controller Debug Commands

The following commands are entered through, and their output can be viewed using, the controller's serial console interface:

```
debug lwapp events enable
```

```
debug lwapp packets enable
```

H-REAP AP Debug Commands

The following commands are entered through, and their output can viewed using, the H-REAP serial console interface:

debug lwapp client packet

debug lwapp client mgmt

debug lwapp client config

debug lwapp client event

debug lwapp reap load

debug lwapp reap mgmt

