H−REAP Modes of Operation Configuration Example

Document ID: 81680

Introduction

This document introduces the concept of Hybrid Remote Edge Access Point (H−REAP) and explains its different modes of operation with an example configuration.

Prerequisites

Requirements

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

- Knowledge of Wireless LAN Controllers (WLCs) and how to configure the WLC basic parameters
- Knowledge of REAP
- Knowledge of Wi−Fi Protected Access (WPA) concepts
- Knowledge of the configuration of an external DHCP server and/or Domain Name System (DNS) server
- Knowledge of how to configure users and groups in an Access Control Server (ACS)
- Knowledge of how to configure a basic WAN link on Cisco Routers
- Knowledge of basic routing protocols

Components Used

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

- Cisco 2000 Series WLC that runs firmware release 4.0
- Cisco 1131AG Lightweight Access Point (LAP)
- Cisco 2800 Series Routers that run version 12.4(11)T.
- Cisco Aironet 802.11a/b/g Client Adapter that runs firmware release 2.5
- Cisco Aironet Desktop Utility version 2.5
- Cisco Secure ACS that runs version 3.2

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

H−REAP is a wireless solution for branch office and remote office deployments. H−REAP enables customers to configure and control access points (APs) in a branch or remote office from the corporate office through a WAN link without deploying a controller in each office.

H−REAPs can switch client data traffic locally and perform client authentication locally when the connection to the controller is lost. When connected to the controller, H−REAPs can also tunnel traffic back to the controller.

H−REAP is a new feature supported by these:

- Both the 1131, 1242 and 1250 Aironet APs and in Cisco Unified Wireless Network controller release versions 4.0 and later
- The 2000 and 4400 Series Controllers, and the 2106 Controller
- Catalyst 3750G Integrated Controller Switch
- Catalyst 6500 Series Wireless Services Module (WiSM)
- Wireless LAN Controller Module (WLCM) for Integrated Services Routers (ISRs)

Client traffic on H−REAPs can either be switched locally at the AP or tunneled back to a controller. This depends on per−WLAN configuration. Also, locally switched client traffic on the H−REAP can be 802.1Q tagged to provide for wired−side separation. During WAN outage, service on all locally switched, locally authenticated WLANs persists.

Note: If the APs are in H−REAP mode and locally switched at the remote site, the dynamic assignment of users to a specific VLAN based on the RADIUS server configuration is not supported. However, you should be able to assign users to specific VLANs based on the static VLAN to service set identifier (SSID) mapping done locally at the AP. Therefore, a user that belongs to a particular SSID can be assigned to a specific VLAN to which the SSID is mapped locally at the AP.

Note: If voice over WLAN is important, then the APs should be run in local mode so that they get CCKM and Connection Admission Control (CAC) support, which are not supported in H−REAP mode.

H−REAP over REAP

Refer to Remote−Edge AP (REAP) with Lightweight APs and Wireless LAN Controllers (WLCs) Configuration Example for more information to help understand REAP.

H−REAP was introduced as a result of these shortcomings of REAP:

- REAP does not have wired−side separation. This is due to lack of 802.1Q support. Data from the WLANs land on the same wired subnet.
- During a WAN failure, a REAP AP ceases service offered on all WLANs, except the first one specified in the controller.

This is how H−REAP overcomes these two shortcomings:

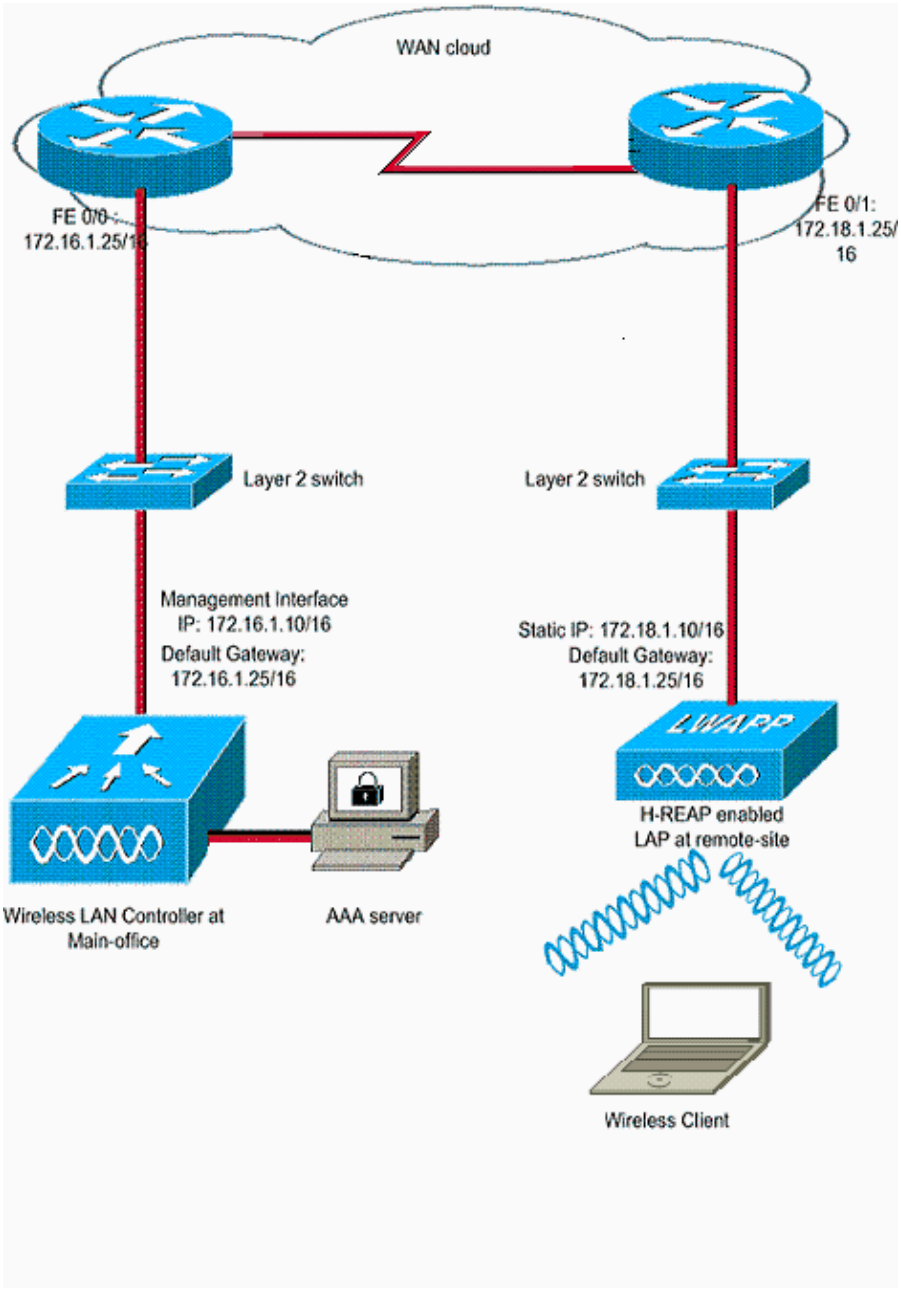
- Provides dot1Q support and VLAN to SSID mapping. This VLAN to SSID mapping needs to be done at H−REAP. While you perform this, ensure that configured VLANs are properly allowed through the ports in intermediate switches and routers.
- Provides continuous service to all WLANs configured for local switching.

Configure

In this section, you are presented with the information to configure the features described in this document.

Network Diagram

This document uses this network setup:



Configuration

This example assumes that the controller is already configured with basic configurations. The controller uses these basic configurations:

- Management interface IP address¡72.16.1.10/16
- AP−Manager interface IP address¡72.16.1.11/16
- Default Gateway router IP address¡72.16.1.25/16
- Virtual Gateway IP address¡.1.1.1

Note: This document does not show WAN configurations and configuration of routers and switches available between the H−REAP and the controller. This assumes that you are aware of the WAN encapsulation and the routing protocols that are used. Also, this assumes that you understand how to configure them in order to maintain connectivity between the H−REAP and controller through the WAN link. In this example, HDLC encapsulation is used on the WAN link.

Priming the AP with a Controller and Configure H−REAP

If you want the AP to discover a controller from a remote network where LWAPP discovery mechanisms are not available, you can use priming. This method enables you to specify the controller to which the AP should connect.

In order to prime an H−REAP−capable AP, connect the AP to the wired network at the main office. During its boot up, the H−REAP−capable AP first looks for an IP address for itself. Once it acquires an IP address through a DHCP server, it boots up and looks for a controller to perform the registration process.

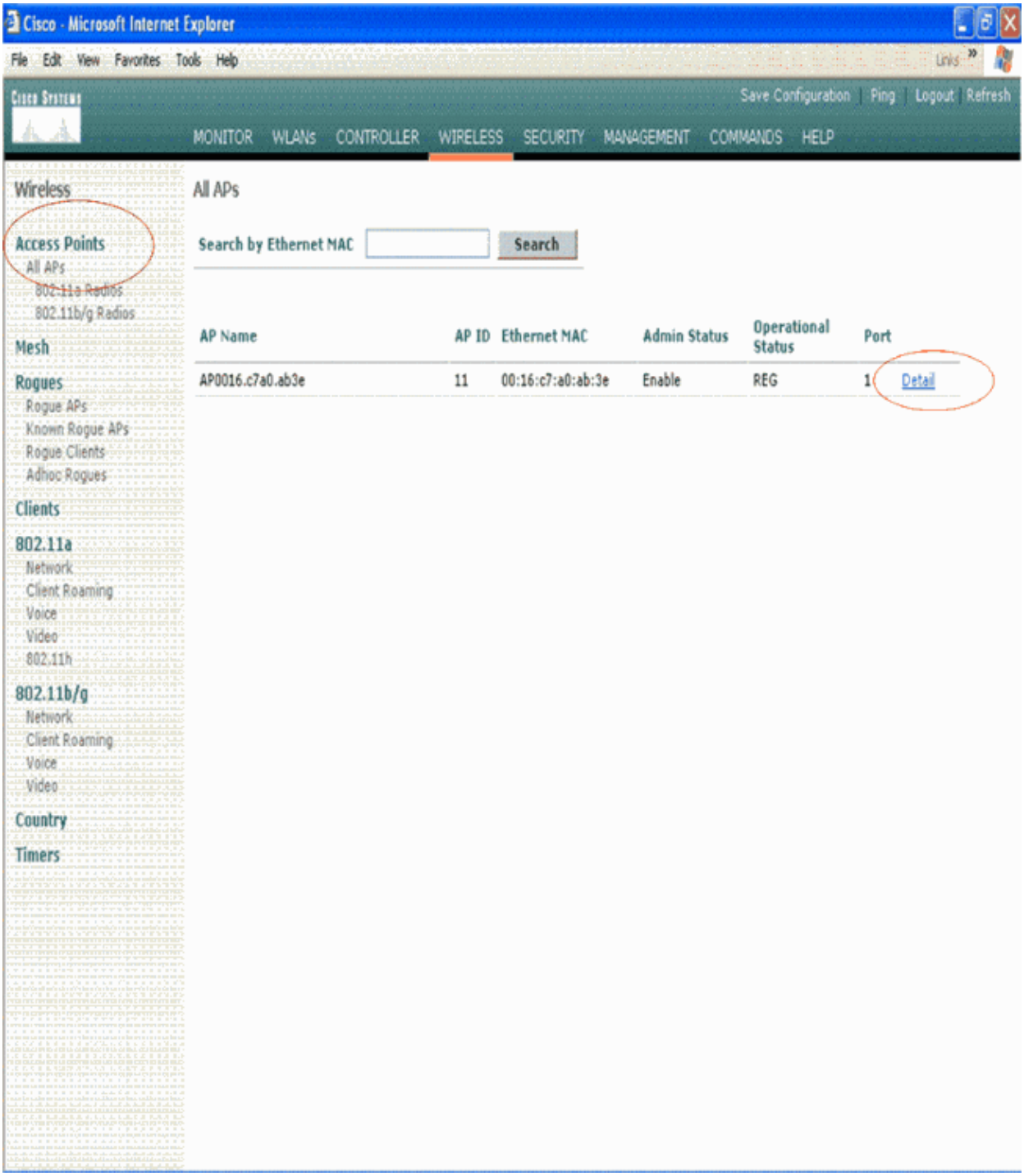
An H−REAP AP can learn the controller IP address in any of the ways explained in Lightweight AP (LAP) Registration to a Wireless LAN Controller (WLC).

The example in this document uses the DHCP option 43 procedure for the H−REAP to learn the controller IP address. Then it joins the controller, downloads the latest software image and configuration from the controller, and initializes the radio link. It saves the downloaded configuration in non−volatile memory for use in standalone mode.

Once the LAP is registered with the controller, complete these steps:

1. In the Controller GUI, choose **Wireless>Access Points**.

   This displays the LAP registered with this controller.
2. Click **Details** that corresponds to the intended LAP.



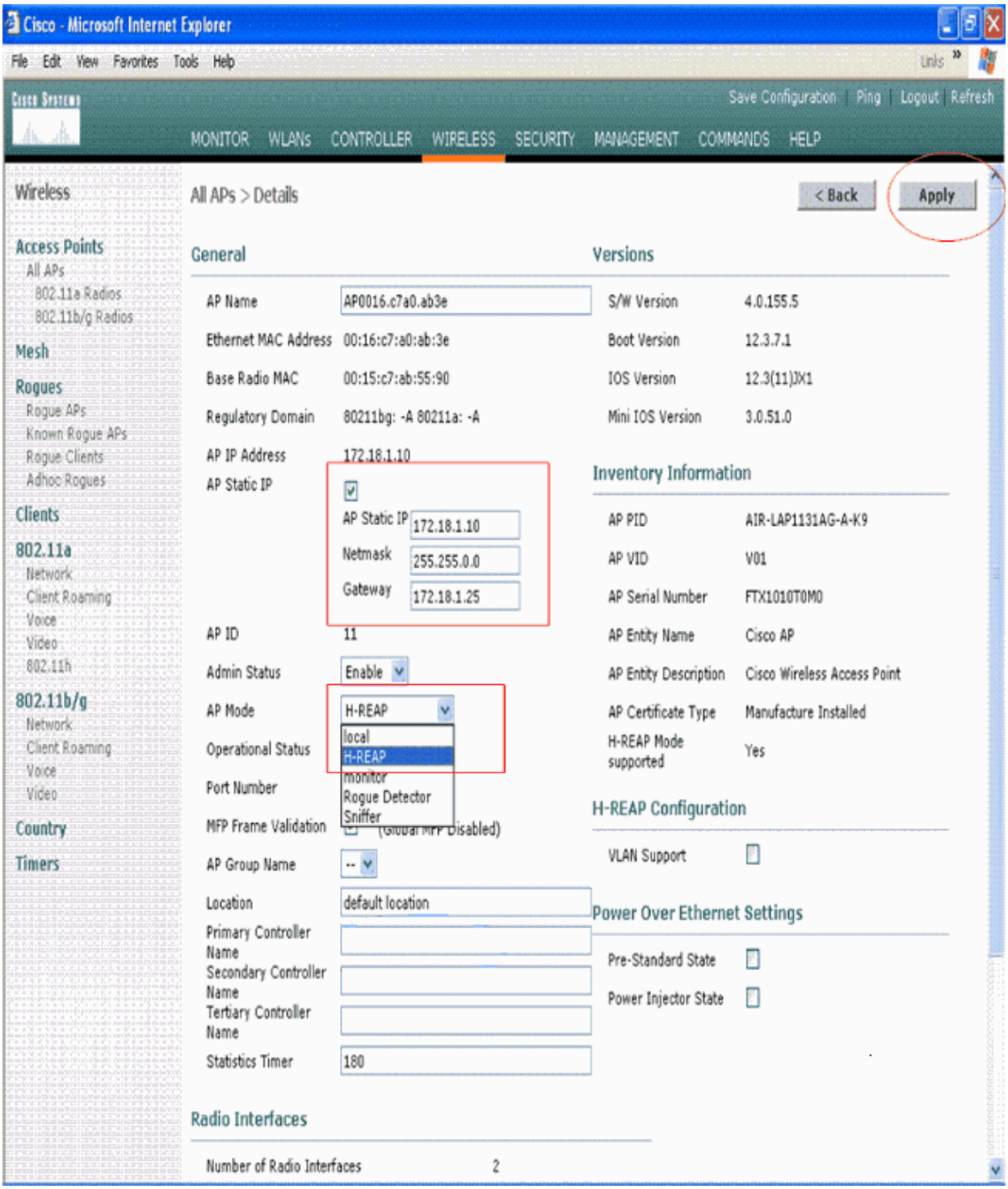
3. In the APs>Details window, define the controller names that the APs will use to register, then click **Apply**.

   You can define up to three controller names (primary, secondary, and tertiary). The APs search for the controller in the same order that you provide in this window. Because this example uses only one controller, the example defines the controller as the primary controller.

   Note: In this example window, you can see that the IP address of the AP is changed to static mode and the static IP address 172.18.1.10 has been assigned. This assignment occurs because this is the subnet to be used at the remote office. Therefore, you use the IP address from the DHCP server, and only during the first time registration stage. After the AP is registered to the controller, you change the address to a static IP address.
4. Configure LAP for H−REAP.

In order to configure the LAP to operate in H−REAP mode, in the same APs>Details window , choose **AP mode** as H−REAP from the corresponding drop down menu.

This configures the LAP to operate in H−REAP mode.



Note: You can also configure the LAP to discover the controller through CLI commands at the AP. Refer to H−REAP Controller Discovery using CLI commands for more information.

Now that your LAP is primed with the controller and configured for H−REAP mode, the next step is to configure H−REAP at the controller side and discuss the H−REAP switching states.

H−REAP Theory of Operations

The H−REAP−capable LAP operates in these two different modes:

- **Connected** mode:

  An H−REAP is said to be in connected mode when its LWAPP control plane link to the WLC is up and operational. This means that the WAN link between the LAP and WLC is not down.
- **Standalone** mode:

  An H−REAP is said to be in the standalone mode when its WAN link to the WLC is down. For example, when this H−REAP no longer has connectivity to the WLC connected across the WAN link.

The authentication mechanism used to authenticate a client can be defined as **Central** or **Local**.

- **Central Authentication** Refers to the authentication type that involves the process of the WLC from the remote site.
- **Local Authentication** Refers to the authentication types that do not involve any processing from the WLC for authentication.

Note: All 802.11 authentication and association processing occurs at the H−REAP, no matter which mode the LAP is in. While in connected mode, H−REAP then proxies these associations and authentications to the WLC. In standalone mode, the LAP cannot inform the WLC of such events.

When a client connects to an H−REAP AP, the AP forwards all authentication messages to the controller. After successful authentication, its data packets are then either switched locally or tunneled back to the controller. This is in accordance to the configuration of the WLAN to which it is connected.

With H−REAP, the WLANs configured on a controller can be operated in two different modes:

- **Central Switching:**

  A WLAN on H−REAP is said to operate in central switching mode if the data traffic of that WLAN is configured to be tunneled to the WLC.
- **Local Switching:**

  A WLAN on H−REAP is said to operate in local switching mode if the data traffic of that WLAN terminates locally at the wired interface of the LAP itself, without getting tunneled to the WLC.

  Note: Only WLANs 1 through 8 can be configured for H−REAP Local Switching because only these WLANs can be applied to the 1130, 1240 and 1250 Series APs that support H−REAP functionality.

H−REAP Switching States

Combined with the authentication and switching modes mentioned in the previous section, an H−REAP can operate in any of these states:

- Central Authentication, Central Switching
- Authentication Down, Switching Down
- Central Authentication, Local Switching
- Authentication Down, Local Switching
- Local Authentication, Local Switching

Central Authentication, Central Switching

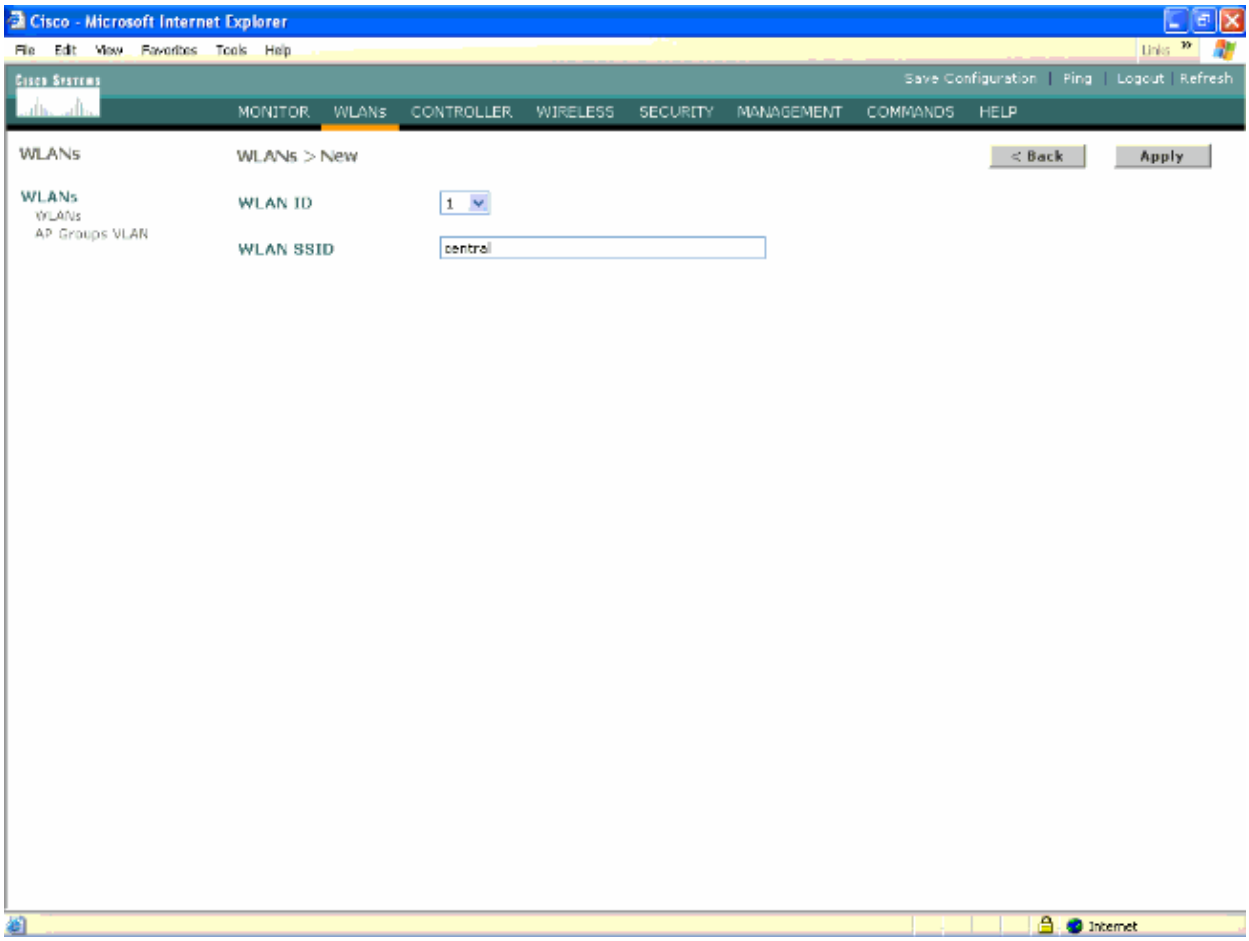
In this state, for the given WLAN, the AP forwards all client authentication requests to the controller and tunnels all client data to the WLC. This state is valid only when the H−REAP is in the connected mode. Any WLAN that is configured to operate in this mode is lost during WAN outage, no matter what the authentication method is.

This example uses these configuration settings:

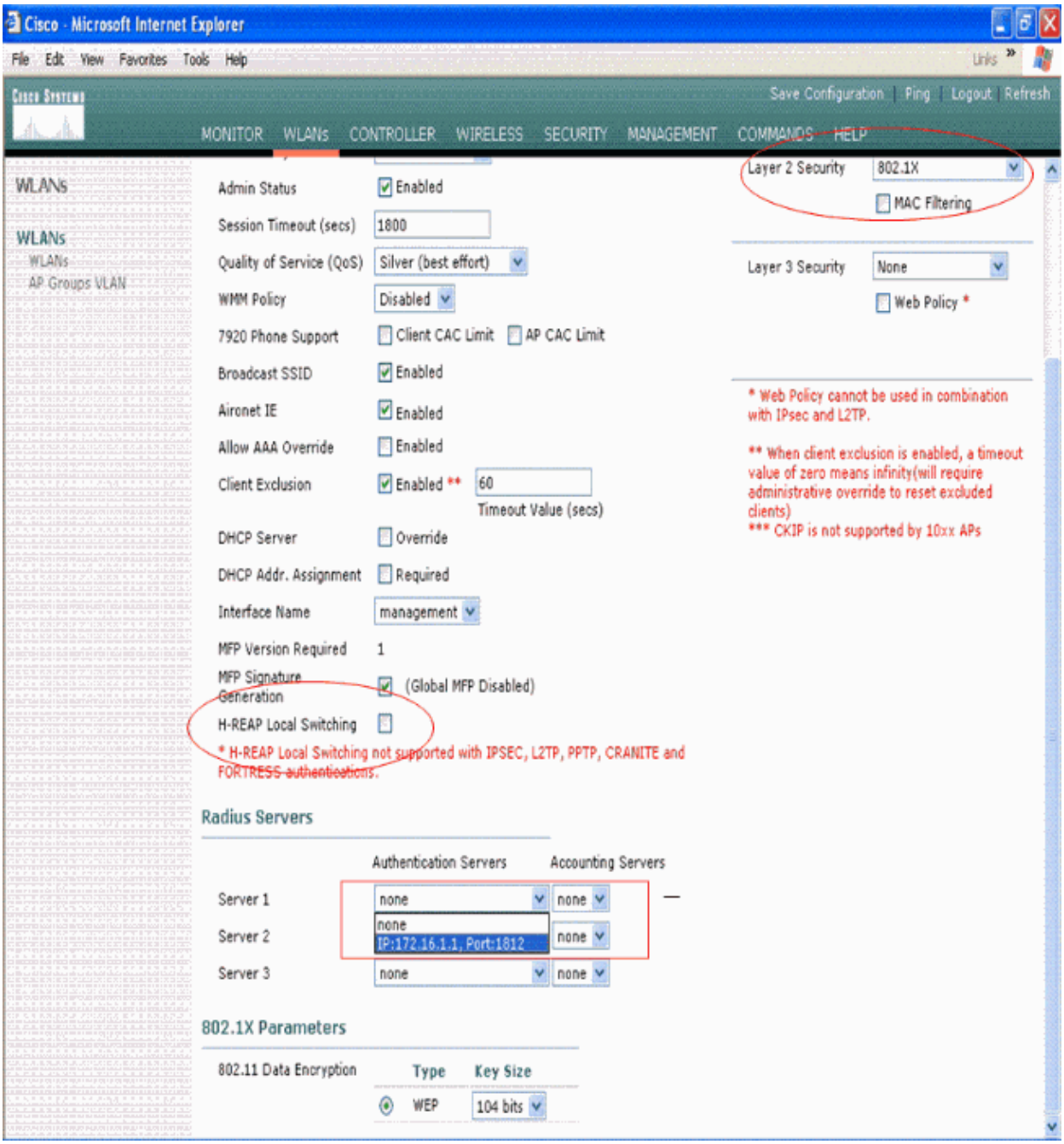
- WLAN/SSID name: **central**
- Layer 2 Security: **802.1x/LEAP**
- H−REAP Local Switching: **disabled**

Complete these steps in order to configure the WLC for central authentication, central switching using GUI:

1. Click **WLANs** in order to create a new WLAN named **central**, then click **Apply**.

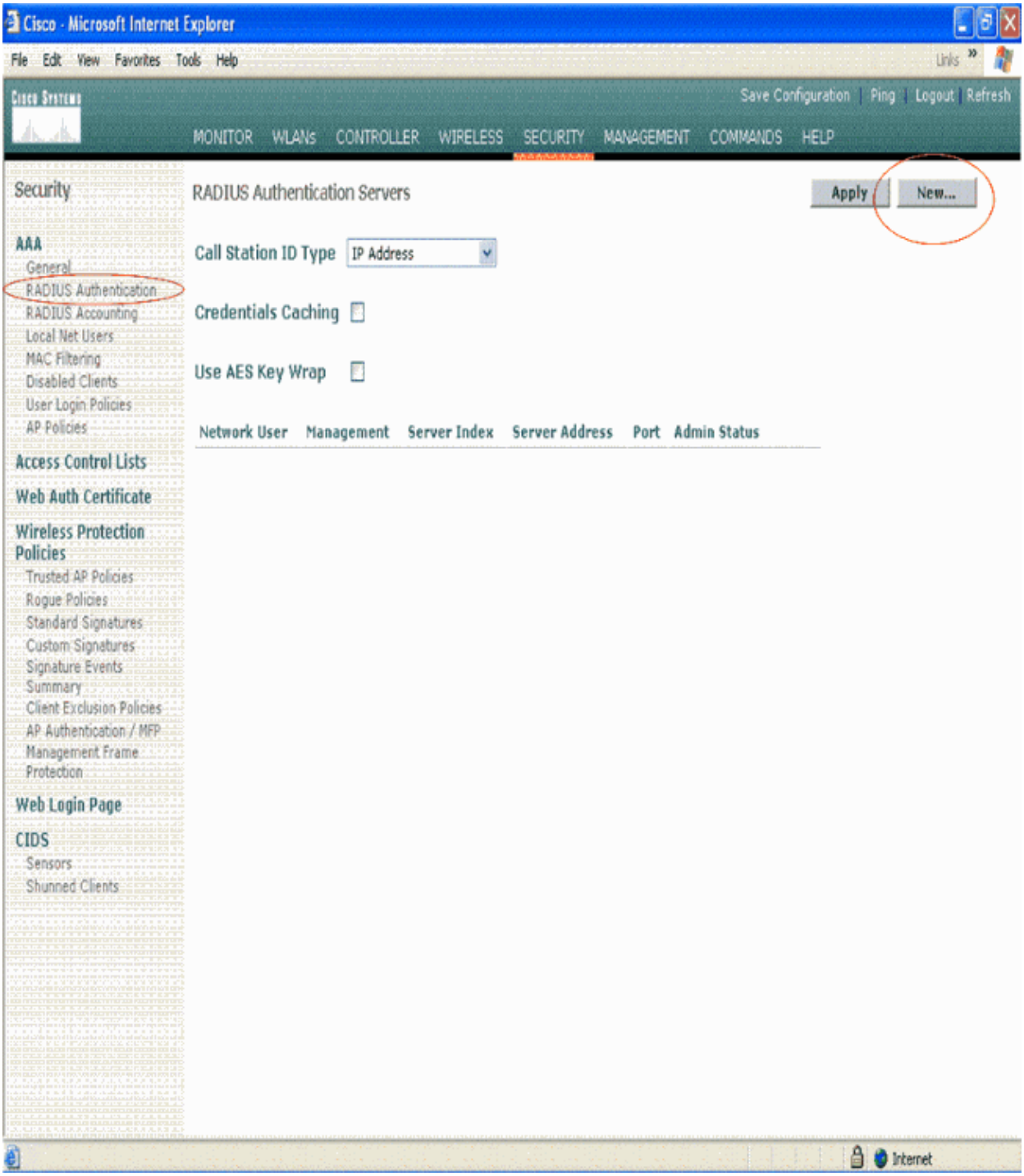


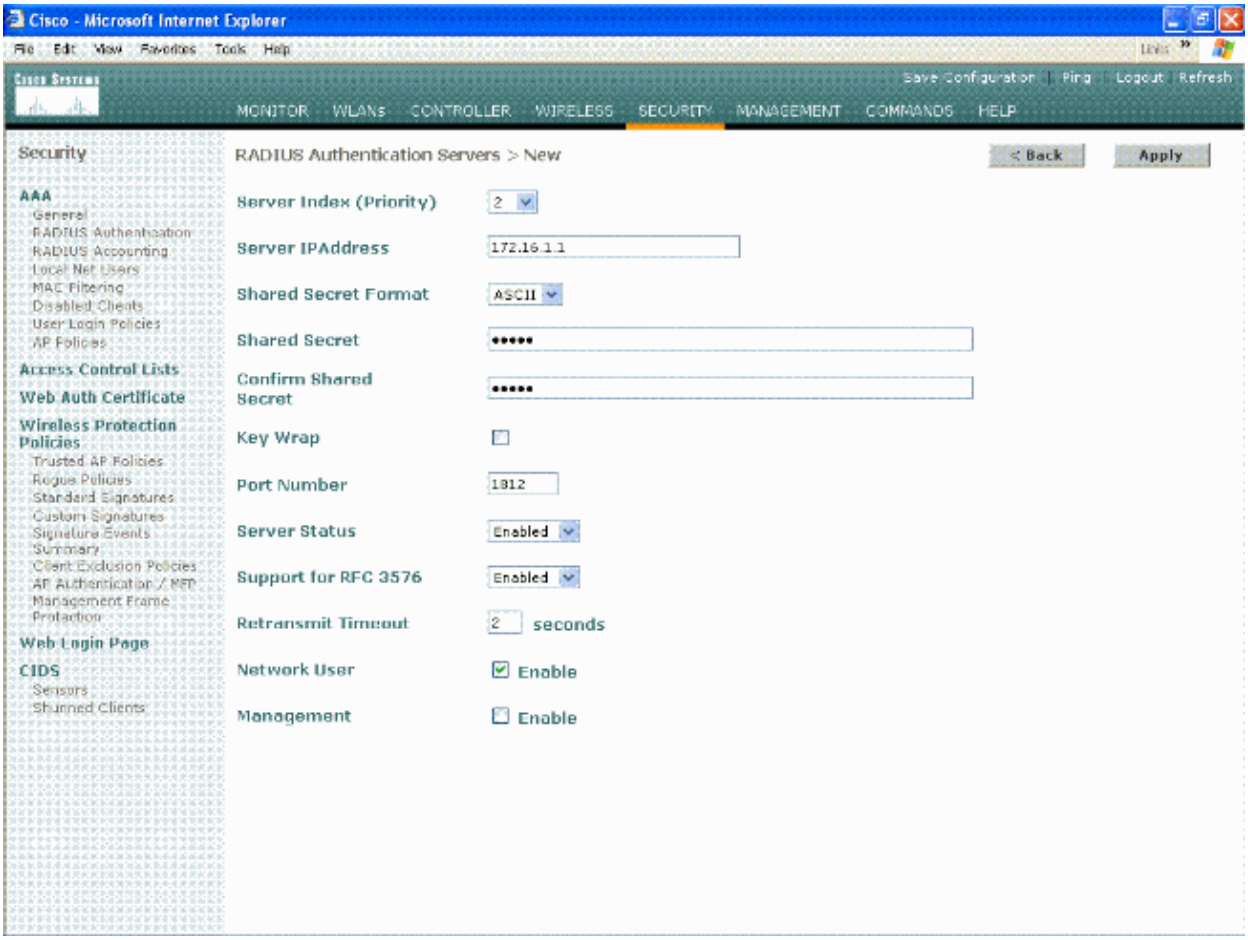
2. Because this WLAN uses central authentication, choose **802.1x** authentication in the Layer 2 Security field.
3. Under the Radius Servers section, choose the appropriate server configured for authentication.
4. Because this WLAN uses central switching, you need to ensure that the H−REAP Local Switching check box is disabled (i.e. Local Switching check box is not selected). Then, click **Apply**.



5. Choose **Security > Radius Authentication** in order to configure the RADIUS server information in the WLC.

   These figures explain the procedure to configure the RADIUS server information in the WLC:


Cisco - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Links
Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
Security
AAA
General
RADIUS Authentication
RADIUS Accounting
Local Net Users
MAC Filtering
Disabled Clients
User Login Policies
AP Policies
Access Control Lists
Web Auth Certificate
Wireless Protection Policies
Trusted AP Policies
Rogue Policies
Standard Signatures
Custom Signatures
Signature Events Summary
Client Exclusion Policies
AP Authentication / MFP
Management Frame Protection
Web Login Page
CIDS
Sensors
Shunned Clients
RADIUS Authentication Servers
Apply
New...
Call Station ID Type
IP Address
Credentials Caching
Use AES Key Wrap
Network User
Management
Server Index
Server Address
Port
Admin Status
Internet



Note: The shared secret used here should be the same than in the ACS server. If not, the WLC is not added as an AAA client of the ACS server. This document does not explain how to configure the RADIUS servers and EAP authentication. Refer to EAP Authentication with WLAN Controllers (WLC) Configuration Example for information on how to configure EAP authentication with WLCs.

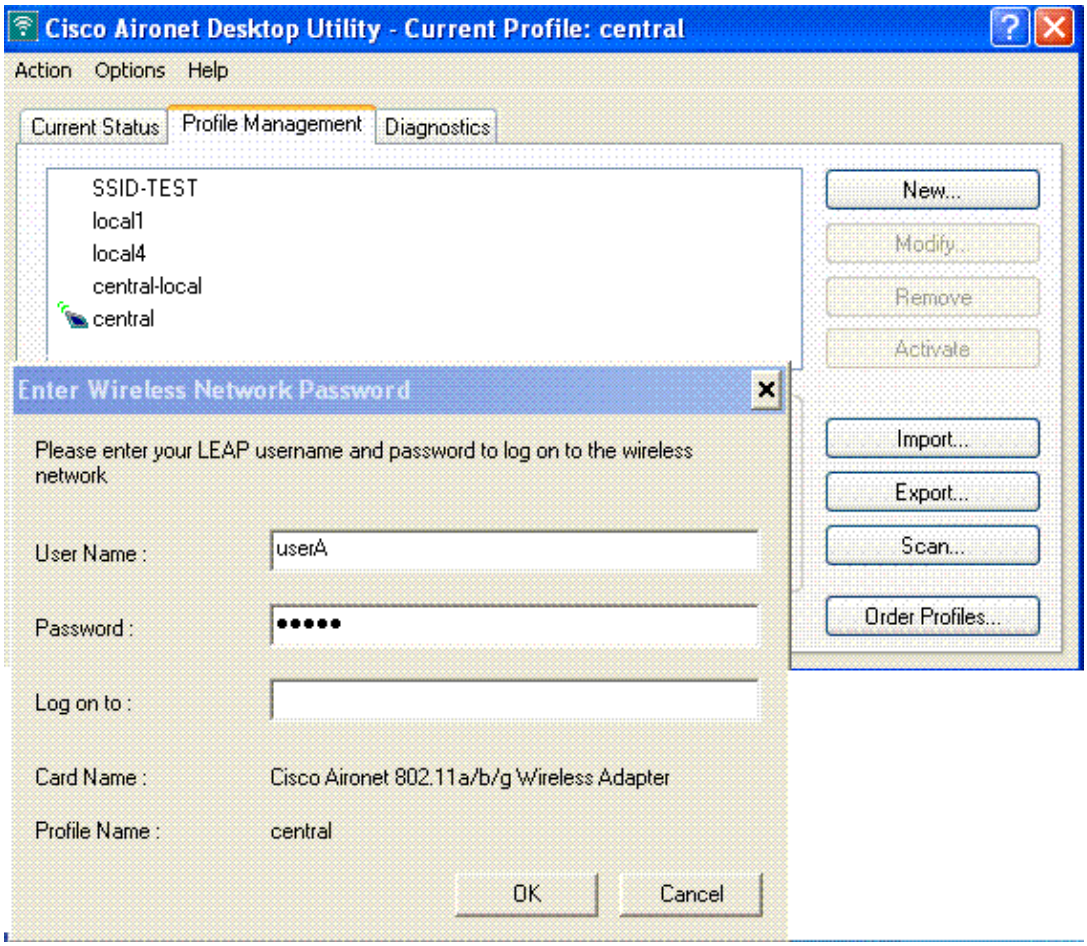
Verify Central Authentication, Central Switching

Complete these steps:

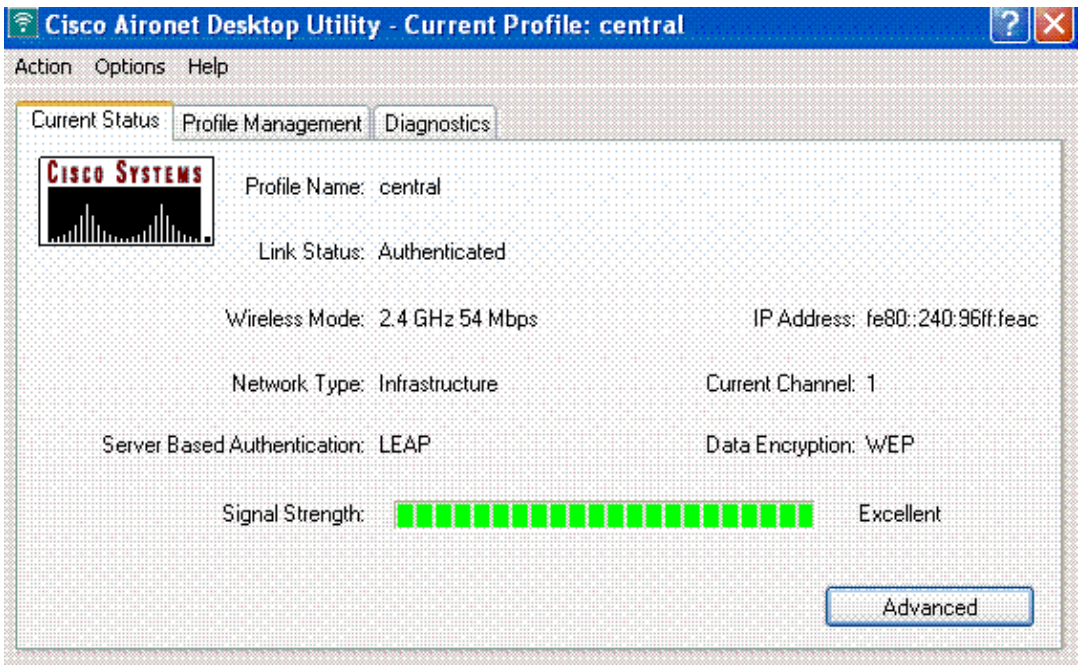
1. Configure the wireless client with the same SSID and security configurations.

   In this example, the SSID is *central* and the security method is *802.1x/LEAP*. This document uses ADU version 2.5 as its client utility.
2. Enter the username and password as configured in the RADIUS server>User Setup in order to activate the central SSID in the client.

   This example uses *userA* as the username and password.



The client is centrally authenticated by the RADIUS server and is associated with the H−REAP AP. The H−REAP is now in **central authentication, central switching**.



Note: This document uses a static IP address of 172.18.1.5 for the wireless client. You can also assign an IP address to the client through a DHCP server.

Authentication Down, Switching Down

With the same configuration explained in the Central Authentication, Central Switching section, disable the WAN link that connects the controller. Now, the controller waits for a heartbeat reply from the AP. A heartbeat reply is similar to keepalive messages. The controller tries five consecutive heartbeats, each every one second.

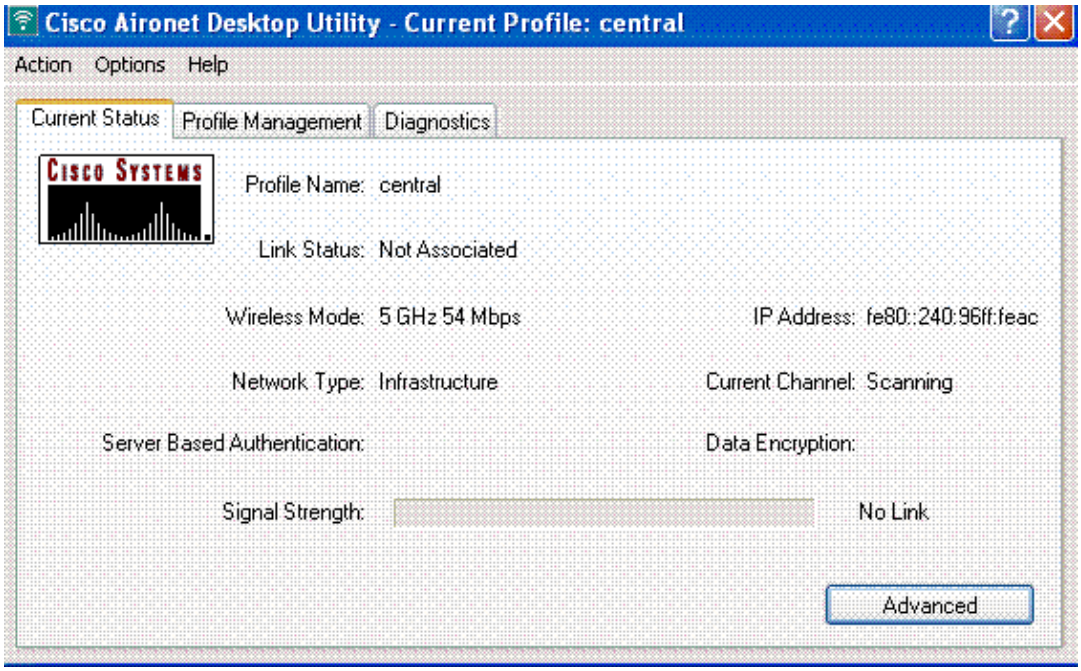
Because it is not received with a heartbeat reply from the H−REAP, the WLC deregisters the LAP.

Issue the **debug lwapp events enable** command from the WLC's CLI in order to verify the deregistration process. This is the example output of this **debug** command:

```
Thu Jan 18 03:19:32 2007: 00:15:c7:ab:55:90 Did not receive heartbeat reply from
AP 00:15:c7:ab:55:90
Thu Jan 18 03:19:32 2007: 00:15:c7:ab:55:90 apfSpamProcessStateChangeInSpamConte
xt: Down LWAPP event for AP 00:15:c7:ab:55:90 slot 0
Thu Jan 18 03:19:32 2007: 00:15:c7:ab:55:90 apfSpamProcessStateChangeInSpamConte
xt: Deregister LWAPP event for AP 00:15:c7:ab:55:90 slot 0
Thu Jan 18 03:19:32 2007: 00:15:c7:ab:55:90 apfSpamProcessStateChangeInSpamConte
xt: Down LWAPP event for AP 00:15:c7:ab:55:90 slot 1
Thu Jan 18 03:19:32 2007: 00:15:c7:ab:55:90 apfSpamProcessStateChangeInSpamConte
xt: Deregister LWAPP event for AP 00:15:c7:ab:55:90 slot 1
Thu Jan 18 03:19:32 2007: 00:15:c7:ab:55:90 Received LWAPP Down event for AP 00:
15:c7:ab:55:90 slot 0!
Thu Jan 18 03:19:32 2007: 00:15:c7:ab:55:90 Deregister LWAPP event for AP 00:15:
c7:ab:55:90 slot 0
Thu Jan 18 03:19:32 2007: 00:15:c7:ab:55:90 Received LWAPP Down event for AP 00:
15:c7:ab:55:90 slot 1!
Thu Jan 18 03:19:32 2007: 00:15:c7:ab:55:90 Deregister LWAPP event for AP 00:15:
c7:ab:55:90 slot 1
```

The H−REAP goes into standalone mode. Issue the **debug lwapp reap** command from the CLI of the LAP in order to verify the transition of LAP from H−REAP mode to standalone mode.

Because this WLAN was previously centrally authenticated and centrally switched, both control and data traffic were tunneled back to the controller. Therefore, without the controller, the client is unable to maintain association with the H−REAP and it is disconnected. This state of H−REAP with both client association and authentication being down is referred to as Authentication Down, Switching Down.



Central Authentication, Local Switching

In this state, for the given WLAN, the WLC handles all client authentication, and the H−REAP LAP switches data packets locally. After the client authenticates successfully, the controller sends LWAPP control commands to the H−REAP and instructs the LAP to switch that given client s data packets locally. This message is sent per client upon successful authentication. This state is applicable only in connected mode.

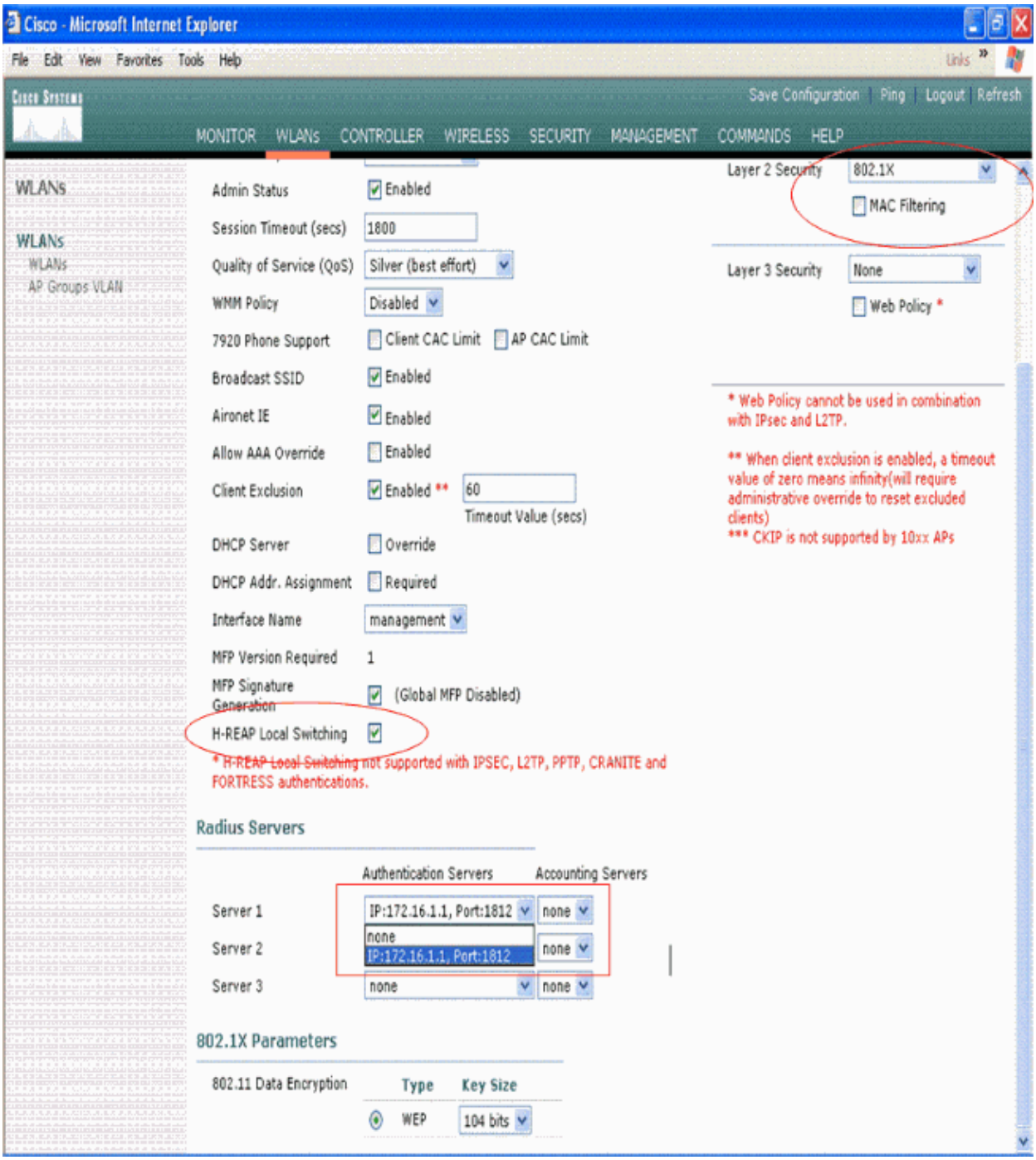
This example uses these configuration settings:

- WLAN/SSID name: **central−local**
- Layer 2 Security: **802.1x/LEAP**.
- H−REAP Local Switching: **Enabled**

From the Controller GUI, complete these steps:

1. Click **WLANs** in order to create a new WLAN named central−local, then click **Apply**.
2. Because this WLAN uses central authentication, choose **802.1x** authentication in the Layer 2 Security field.
3. Under the Radius Servers section, choose the appropriate server configured for authentication.

   In order to configure radius server information in the controller, see step 4 in the Central Authentication, Central Switching section of this document.
4. Check the **H−REAP Local Switching** check box in order to switch client traffic that belongs to this WLAN locally at the H−REAP.



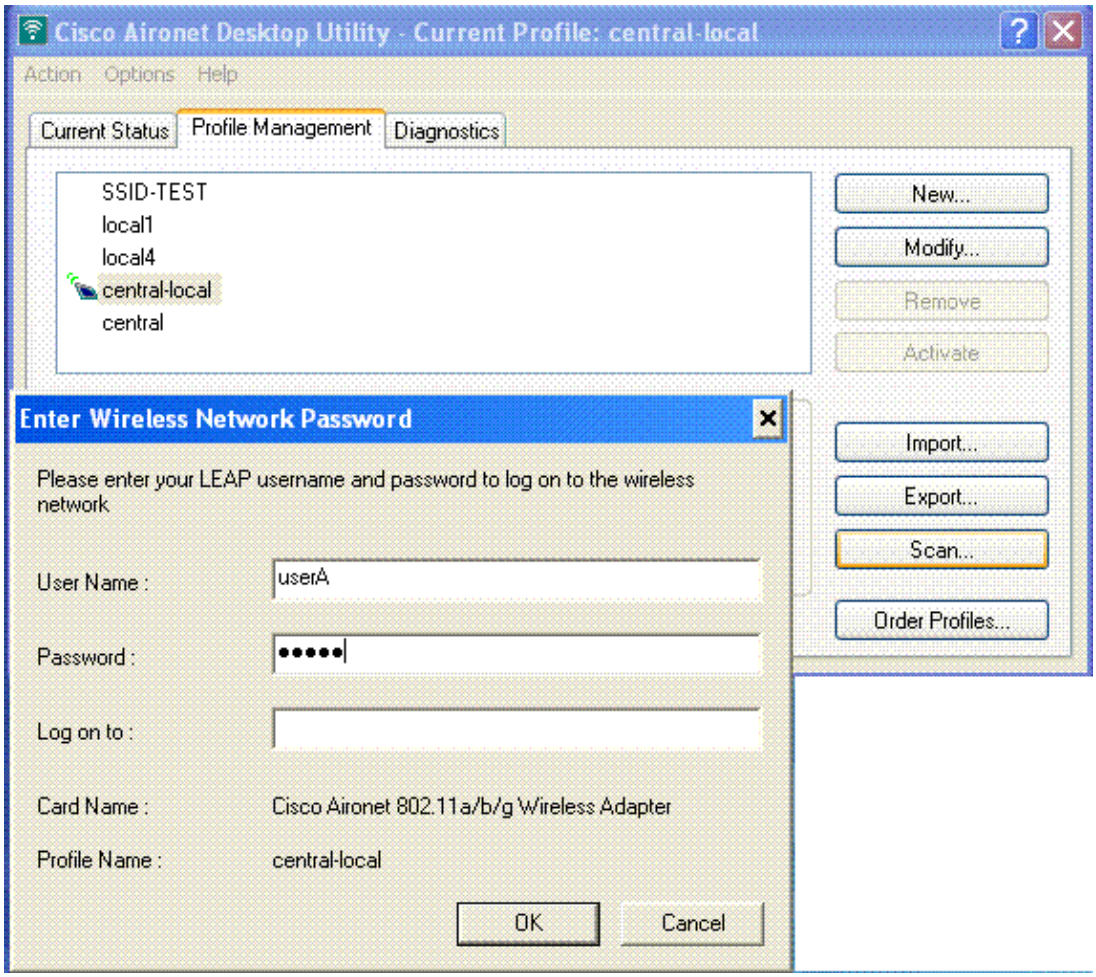
Verify Central Authentication, Local Switching

Complete these steps:

1. Configure the wireless client with the same SSID and security configurations.

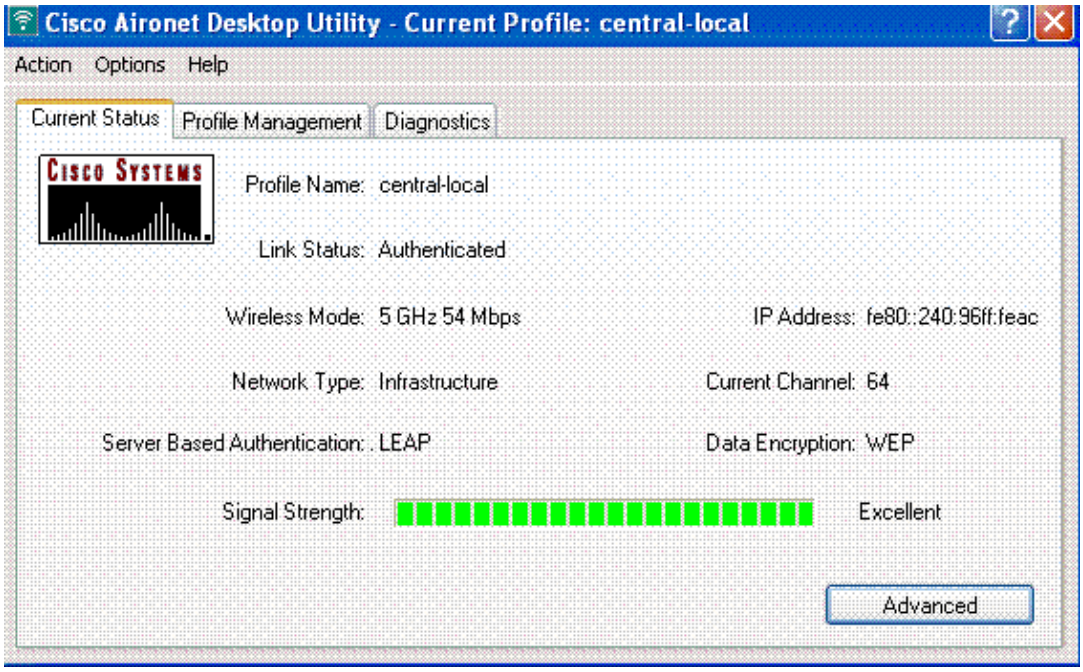
   In this example, the SSID is *central−local* and the security method is *802.1x/LEAP*.
2. Enter the username and password as configured in the RADIUS server>User Setup in order to activate the central−local SSID in the client.

   This example uses *userA* as the username and password.



3. Click **OK**.

The client is centrally authenticated by the RADIUS server and gets associated with the H−REAP AP. The H−REAP is now in **central authentication, local switching**.



Authentication Down, Local Switching

If a locally switched WLAN is configured for any authentication type that is required to be processed on the WLC (such as EAP authentication [dynamic WEP/WPA/WPA2/802.11i], WebAuth, or NAC), upon WAN failure, it enters the **authentication down, local switching** state. In this state, for the given WLAN, the H−REAP rejects any new clients that try to authenticate. However, it continues to send beacons and probe responses to keep existing clients properly connected. This state is valid only in standalone mode.

In order to verify this state, use the same configuration explained in the Central Authentication, Local Switching section.

If the WAN link that connects the WLC is down, the WLC goes through the process of deregistering the H−REAP.

Once deregistered, H−REAP goes into standalone mode. This transition from H−REAP mode to standalone mode can be verified at the H−REAP CLI with the **debug lwapp REAP** command. This is the example output of this debug command:

```
 REAP: REAP AP Switching to Standalone mode,
Connected to Controller 1
LWAPP_CLIENT_ERROR_DEBUG:  GOING BACK TO DISCOVER MODE
WIDS−6−DISABLED: IDS Signature is removed and disabled.
LWAPP−5−CHANGED: LWAPP changed state to DISCOVERY
```

The client associated through this WLAN still maintains its connectivity. However, because the controller, the authenticator is not available, H−REAP does not allow any new connections from this WLAN.

This can be verified by the activation of another wireless client in the same WLAN. You can find that the authentication for this client fails and that client is not allowed to associate.

Note: When a WLAN client count equals zero, the H−REAP ceases all associated 802.11 functions and no longer beacons for the given SSID. This moves the WLAN to the next H−REAP state, **authentication down, switching down**.

Local Authentication, Local Switching

In this state, the H−REAP LAP handles client authentications and switches client data packets locally. This state is valid only in standalone mode and only for authentication types that can be handled locally at the AP and do not involve the processing of controller

The H−REAP that was previously in the **central authentication, local switching** state, moves into this state, provided the configured authentication type can be handled locally at the AP. If the configured authentication cannot be handled locally, such as 802.1x authentication, then in standalone mode, the H−REAP goes to **authentication down, local switching** mode.

These are some of the popular authentication mechanisms that can be handled locally at the AP in standalone mode:

- Open
- Shared
- WPA−PSK
- WPA2−PSK

Note: All authentication processes are handled by the WLC when the AP is in the connected mode. While the

H−REAP is in standalone mode, open, shared, and WPA/WPA2−PSK authentications are transferred to the LAPs where all client authentication occurs.

This example uses these configuration settings:

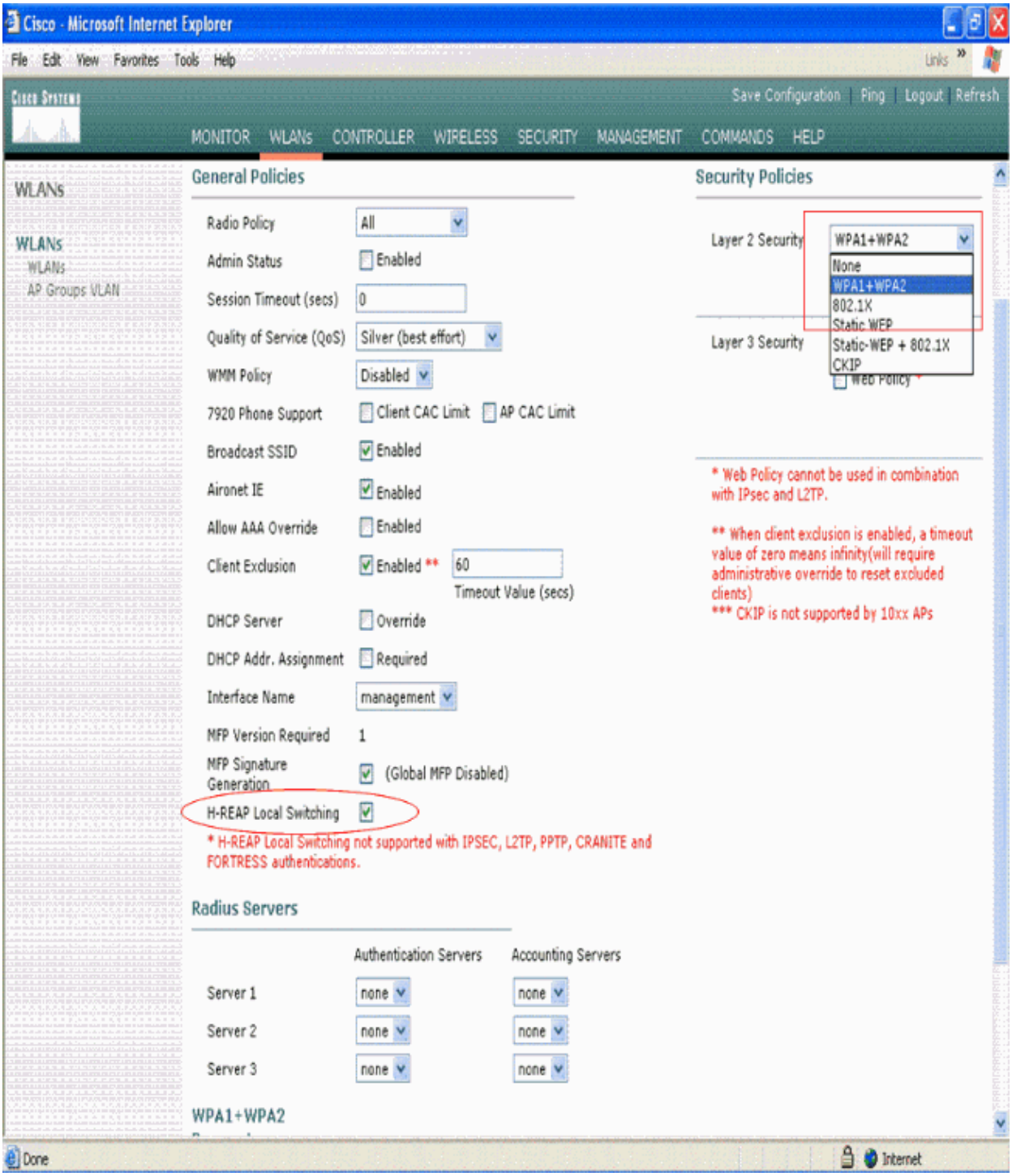
- WLAN/SSID name: **local1**
- Layer 2 Security: **WPA−PSK**
- H−REAP Local Switching: **enabled**

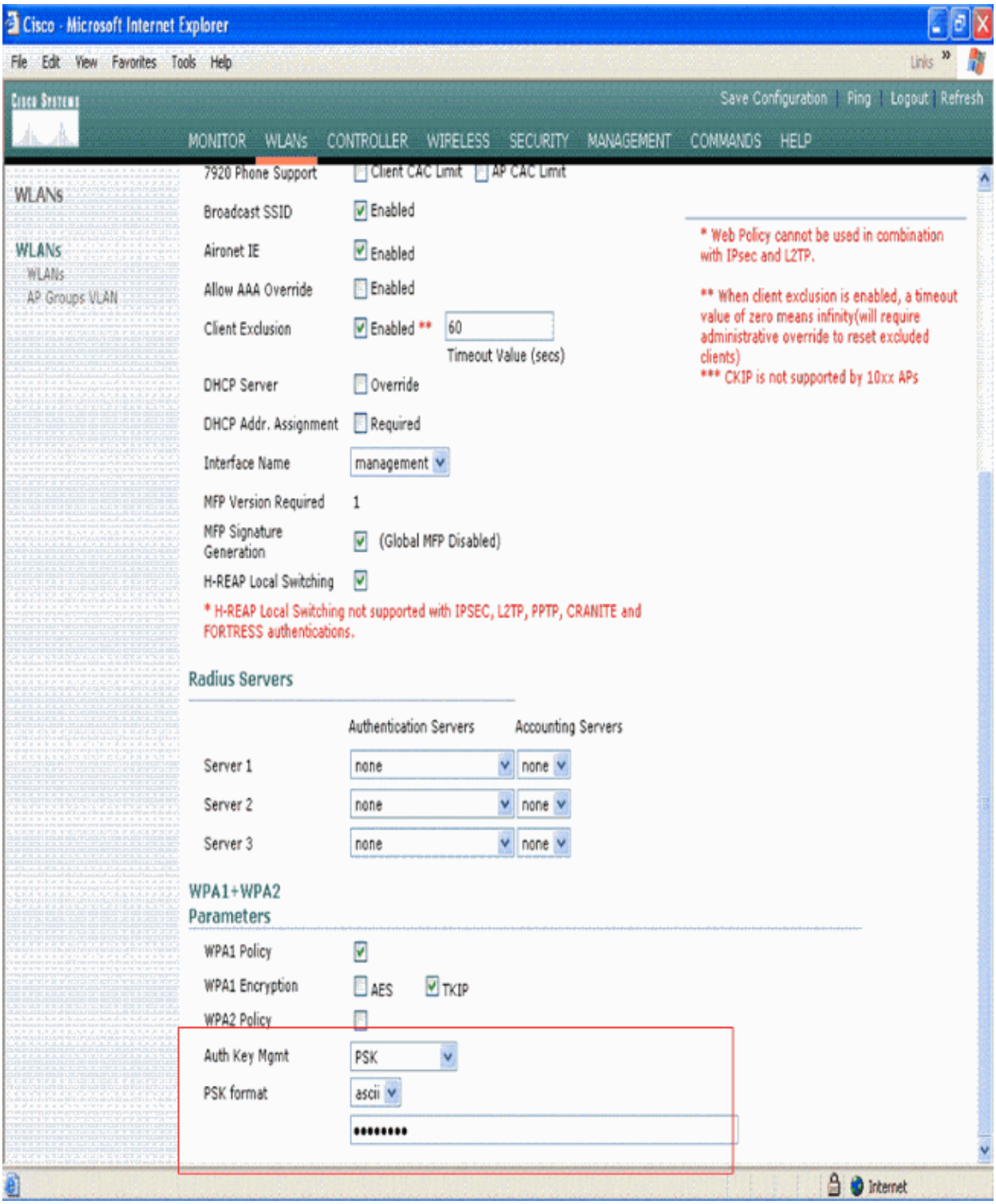
From the Controller GUI, complete these steps:

1. Click **WLANs** in order to create a new WLAN named local1, then click **Apply**.
2. Because this WLAN uses local authentication, choose **WPA−PSK** or any of the mentioned security mechanisms that can be handled locally in the Layer 2 Security field.

   This example uses **WPA−PSK**.
3. Once chosen, you need to configure the Pre−shared Key/Pass Phrase to be used.

   This must be the same at the client side for authentication to be successful.
4. Check the **H−REAP Local Switching** check box in order to switch client traffic that belongs to this WLAN locally at the H−REAP.


Cisco - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Links
Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
WLANs
WLANs
WLANs
AP Groups VLAN
General Policies
Radio Policy All
Admin Status Enabled
Session Timeout (secs) 0
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 management
MFP Version Required 1
MFP Signature Generation (Global MFP Disabled)
H-REAP Local Switching
* H-REAP Local Switching not supported with IPSEC, L2TP, PPTP, CRANITE and FORTRESS authentications.
Radius Servers
Authentication Servers
Accounting Servers
Server 1 none none
Server 2 none none
Server 3 none none
WPA1+WPA2
Security Policies
Layer 2 Security WPA1+WPA2
None
WPA1+WPA2
802.1X
Static WEP
Static-WEP + 802.1X
CKIP
Layer 3 Security
Web Policy *
* Web Policy cannot be used in combination with IPsec and L2TP.
** When client exclusion is enabled, a timeout value of zero means infinity(will require administrative override to reset excluded clients)
*** CKIP is not supported by 10xx APs
Done
Internet



Verify Local Authentication, Local Switching

Complete these steps:

1. Configure the client with the same SSID and security configurations.

   Here, the SSID is *local1* and the security method is *WPA−PSKSSID*.
2. Activate the local1 SSID in the client.

   The client gets authenticated centrally at the controller and associates with the H−REAP. The client

traffic is configured to switch locally. Now, the H−REAP is in Central Authentication, Local Switching state.

3. Disable the WAN link that connects to the controller.

   The controller as usual goes through the deregistration process. H−REAP is deregistered from the controller.

   Once deregistered, H−REAP goes into standalone mode.
4. This transition from H−REAP mode to standalone mode can be verified at the H−REAP CLI with the **debug lwapp REAP** command.

   However, the client that belongs to this WLAN still maintains association with H−REAP.

   Also, because the authentication type here can be handled locally at the AP without the controller, H−REAP does allow associations from any new wireless client through this WLAN.
5. In order to verify this, activate any other wireless client on the same WLAN.

   You can see that the client is authenticated and associated successfully.

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

Troubleshooting Commands

These commands can be useful:

- **show lwapp reap association**
- **debug lwapp clients**

Related Information

- **Wireless LAN Controller and Lightweight Access Point Basic Configuration Example**
- **WPA Configuration Overview**
- **VLANs on Wireless LAN Controllers Configuration Example**
- **Cisco Wireless LAN Controller Configuration Guide, Release 4.0**
- **Hybrid REAP Design and Deployment Guide**
- **Hybrid Remote Edge Access Point (H−REAP) Basic Troubleshooting**
- **Cisco Aironet 1130AG Series− Q and A**
- **Release Notes for Cisco Aironet 1130AG LAP**
- **LEAP Authentication with Local RADIUS Server**
- **WLAN Controller Failover for Lightweight Access Points Configuration Example**
- **Wireless Product Support**
- **Technical Support & Documentation − Cisco Systems**

Contacts & Feedback | Help | Site Map
© 2009 − 2010 Cisco Systems, Inc. All rights reserved. Terms & Conditions | Privacy Statement | Cookie Policy | Trademarks of Cisco Systems, Inc.

Updated: Oct 30, 2008 Document ID: 81680