

H-REAP 模式配置范例

介绍

本文介绍混合远端边缘 AP (H-REAP) 模式,并提供配置范例

配置条件

必要条件

在配置前, 请先确定掌握以下知识点:

- (1) WLC 的基础知识, 并且具有配置 WLC 的基础
- (2) 远程边缘 AP (REAP)
- (3) WPA
- (4) 外部 DHCP 以及 DNS 服务器
- (5) ACS 中配置用户
- (6) 基本的思科路由器广域网接口
- (7) 基本的路由协议

使用说明

本文涉及的信息基于以下软件及硬件版本:

- (1) 使用固件 4.0 的思科 2000 系列的 WLC
- (2) 思科 1131AG 的 LAP
- (3) 使用软件版本 12.4(11)T 的思科 2800 系列路由器
- (4) 使用固件 2.5 的思科 802.11a/b/g 无线客户端
- (5) 使用软件版本 2.5 的思科桌面软件
- (6) 使用软件版本 3.2 的思科准入控制 ACS

文档中描述的是在实验环境, 所有设备都是初始配置, 请先确定各命令的意义, 再做

配置。

规定

请参考以下网址，获得更多信息

http://www.cisco.com/en/US/tech/tk801/tk36/technologies_tech_note09186a0080121ac5.shtml

知识点

H-REAP 模式是解决分支办公机构无线覆盖的解决方案，当远端办公室没有本地 WLC 的时候，它允许通过 WAN 链路的连接，控制远端 AP。

当与 WLC 失去联系后，H-REAP 仍然可以传输本地数据，进行本地的认证，当恢复和 WLC 的连接后，H-REAP 可以将数据传输到 WLC。

以下设备支持 H-REAP：

- (1) 在 WLC 软件版本 4.0 及以后，1131,1242 以及 1250AP
- (2) 2000,4000 和 2106 系列 WLC
- (3) 内置 WLC 的思科 3750G 交换机
- (4) 思科 6500 系列的 WISM 模块
- (5) 内置 WLC 的思科 ISR 路由器

在 H-REAP 模式下，数据可以本地传输，或者发送到 WLC，这取决于无线网络的配置，本地传输的数据可以被封装成 802.1Q 的帧，并传递给有线网络。在广域网线路断开后，H-REAP 模式的 AP 仍然可以传输本地数据，并做认证。

【译者注】在 4.0 版本下，当 AP 工作在 H-REAP 模式，并且本地传输数据时，不支持通过 RADIUS 认证服务器做动态指定的 VLAN 功能，然而，可以通过在 AP 上配置 VLAN 与 SSID 的静态绑定，做相应的功能，因此，可以通过此功能，达到 VLAN 与 SSID 的对应关系。

【译者注】在 4.0 版本下，如果在 WLAN 中传输语音，AP 要工作在本地模式，以便支持 CCKM 和 CAC，这两个功能在 H-REAP 模式并不支持。

知识点

在 REAP 上的 H-REAP

请参考以下文档，察看更多 REAP 的信息

http://www.cisco.com/en/US/tech/tk722/tk809/technologies_configuration_example09186a008069da69.shtml

H-REAP 改进了很多 **REAP** 的功能：

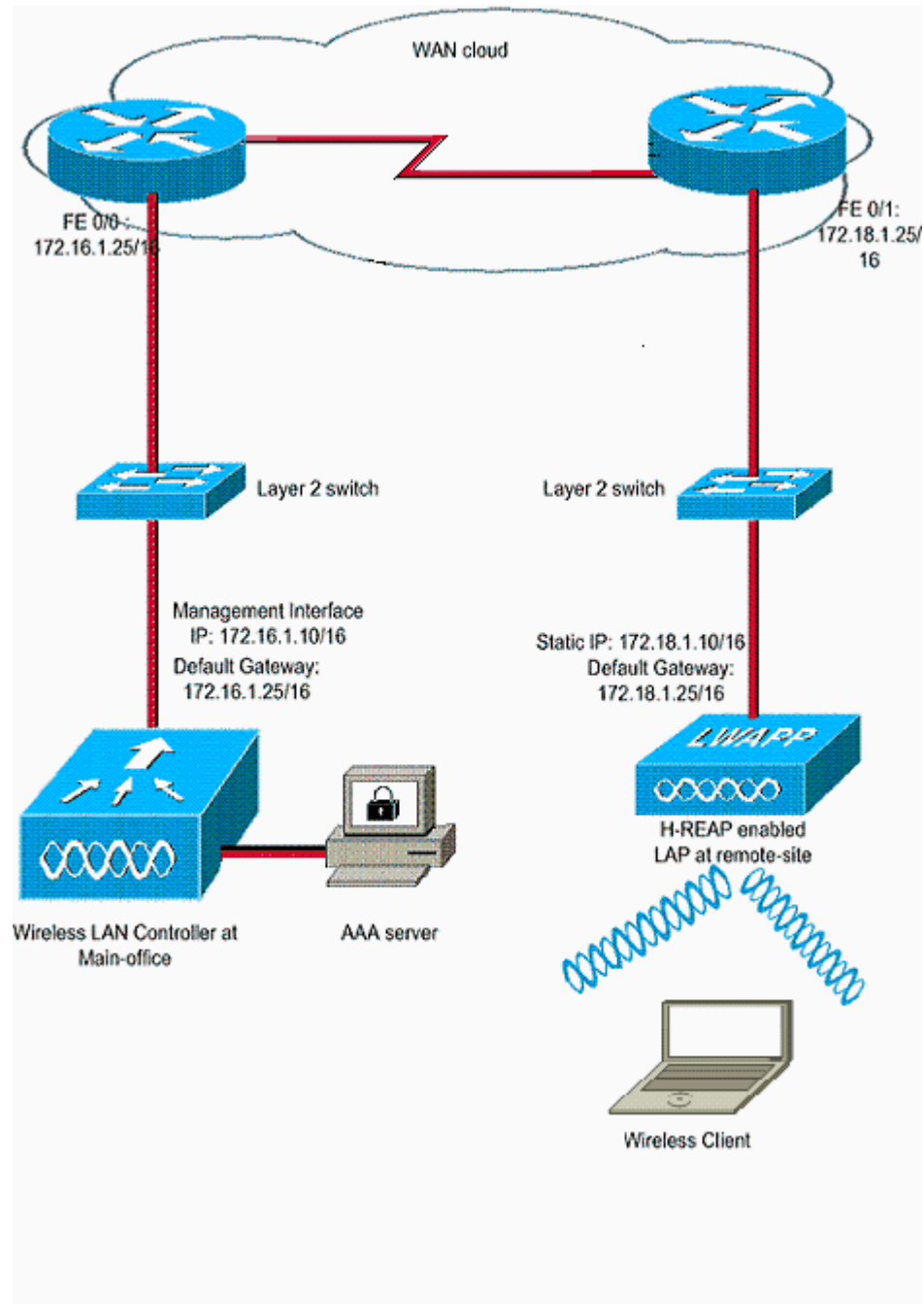
- (1) **REAP** 不支持有线网络的分离，这个取决于 **802.1Q** 的支持，数据在同一个有线网子网络中终结
- (2) 在 WAN 中断后，除了第一个在 WLC 中定义的 WLAN 网络，其他 WLAN 网络将不能在 **REAP** 的 AP 中提供服务，

H-REAP 通过以下方法解决前两个问题：

- (1) 提供 **dot1Q** 支持和 **VLAN** 与 **SSID** 的绑定支持，配置此功能前，请先确定连接的交换机和路由器端口已被配置好相应的 **VLAN**
- (2) 可为本地的数据转发提供连续的、不中断的服务

配置

网络拓扑



配置

WLC 上的基本配置：

- (1) 管理 IP-172.16.1.10/16
- (2) AP 管理 IP-172.16.1.11/16

(3) 默认网关 IP-172.16.1.25/16

(4) 虚拟网关地址-1.1.1.1

【译者注】此文档中不包含 WAN 的路由器，以及连接 AP 的交换机的配置

配置 AP 成为 H-REAP

如果在 LWAPP 发现协议无法使用的远程网络中，你可以采用手工指定的方式确保 AP 连接到指定的控制器。

将具有 H-REAP 功能的 AP 连接后，在启动过程中，首先找到的 IP 地址作为自己的 IP 地址，一旦通过 DHCP 获得 IP 地址后，它将启动，并执行注册到 WLC 的过程。

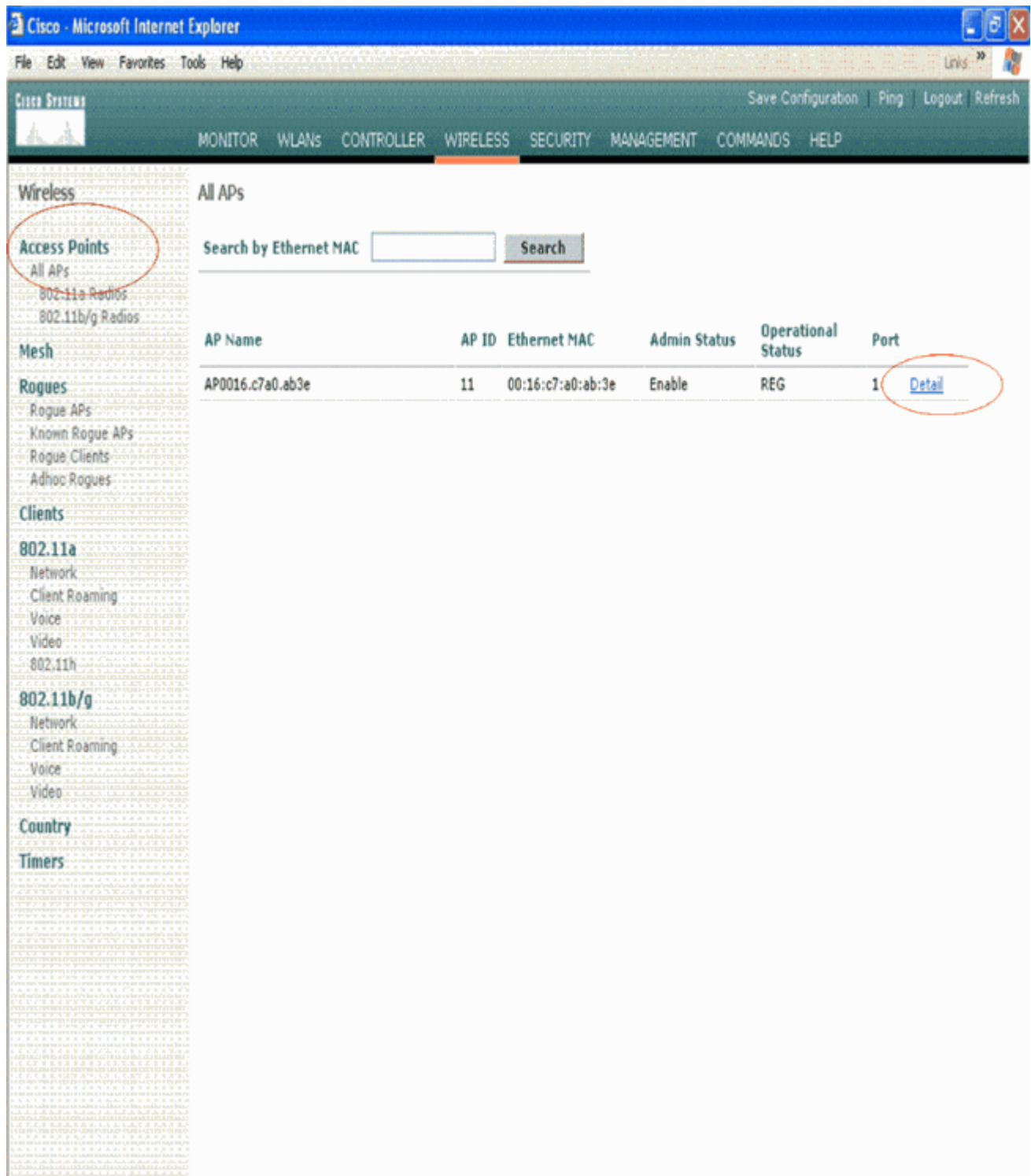
H-REAP 的 AP 可以通过以下方法获得 WLC 的地址：

http://www.cisco.com/en/US/tech/tk722/tk809/technologies_tech_note09186a00806c9e51.shtml

其中一个方法是通过 DHCP 选项 43 获得 WLC 的地址，然后加入到 WLC，下载最新的软件版本和配置文件，初始化射频接口，保存相应的配置到自己的非易失性的内存中，以便在独立模式下使用。

当 AP 注册到 WLC 后，执行以下步骤：

1. 在 WLC 界面，点击 **Wireless>Access Points**.
2. 找到相应的 AP 点击 **Details**



3. 在 APs>Details 界面，定义 WLC 的名字，点击 **Apply**
可以定义三个 WLC 的名字（分为主，中，次），AP 会根据配置找寻相应的 WLC

【译者注】在以上截图中，你可以看到 AP 被指定为静态模式，配置的是静态的 IP 地址，因为这个 AP 要工作在远程办公区域，所以在第一次通过 DHCP 得到 IP 地址后，要手工定义模式，以便以后再远程办公区域中使用。

在 APs>Details 界面，选择 **AP mode** 定义 H-R E A P



http://www.cisco.com/en/US/products/ps6087/products_tech_note09186a0080736123.shtml#t11

H-REAP 的操作理论

H-REAP 的 AP 具有以下两种模式

- (1) 连接模式
当 WLC 与 AP 可以进行 LWAPP 通讯，意味着广域网（WAN）链路完好
- (2) 独立模式
当 WLC 与 AP 不能进行通讯

认证的方法可以被定义为中心或者本地：

- (1) 中心-通过 WLC 进行认证
- (2) 本地-不经过 WLC 进行

【译者注】不论 AP 是什么模式，所有 802.11 的认证方法或者关联都发生在 H-REAP 下。在连接模式下，AP 通过 WLC 执行认证和关联。

在 H-REAP 下，在 WLC 的无线配置可以有以下两种：

- (1) 中心交换-在 H-REAP 下的 AP，通过隧道与 WLC 联系
- (2) 本地交换-在 H-REAP 下的 AP，通过本地连接，传输本地数据

【译者注】只有 VLAN1-8 可以应用在 H-REAP，因为只有 1130, 1240 和 1250 支持 H-REAP

H-REAP 交换状态

结合认证以及前面提到的模式，H-REAP 可以被定义为以下状态

- (1) 中心认证，中心交换
- (2) 认证失败，交换失败
- (3) 中心认证，本地交换
- (4) 认证失败，本地交换
- (5) 本地认证，本地交换

中心认证，中心交换

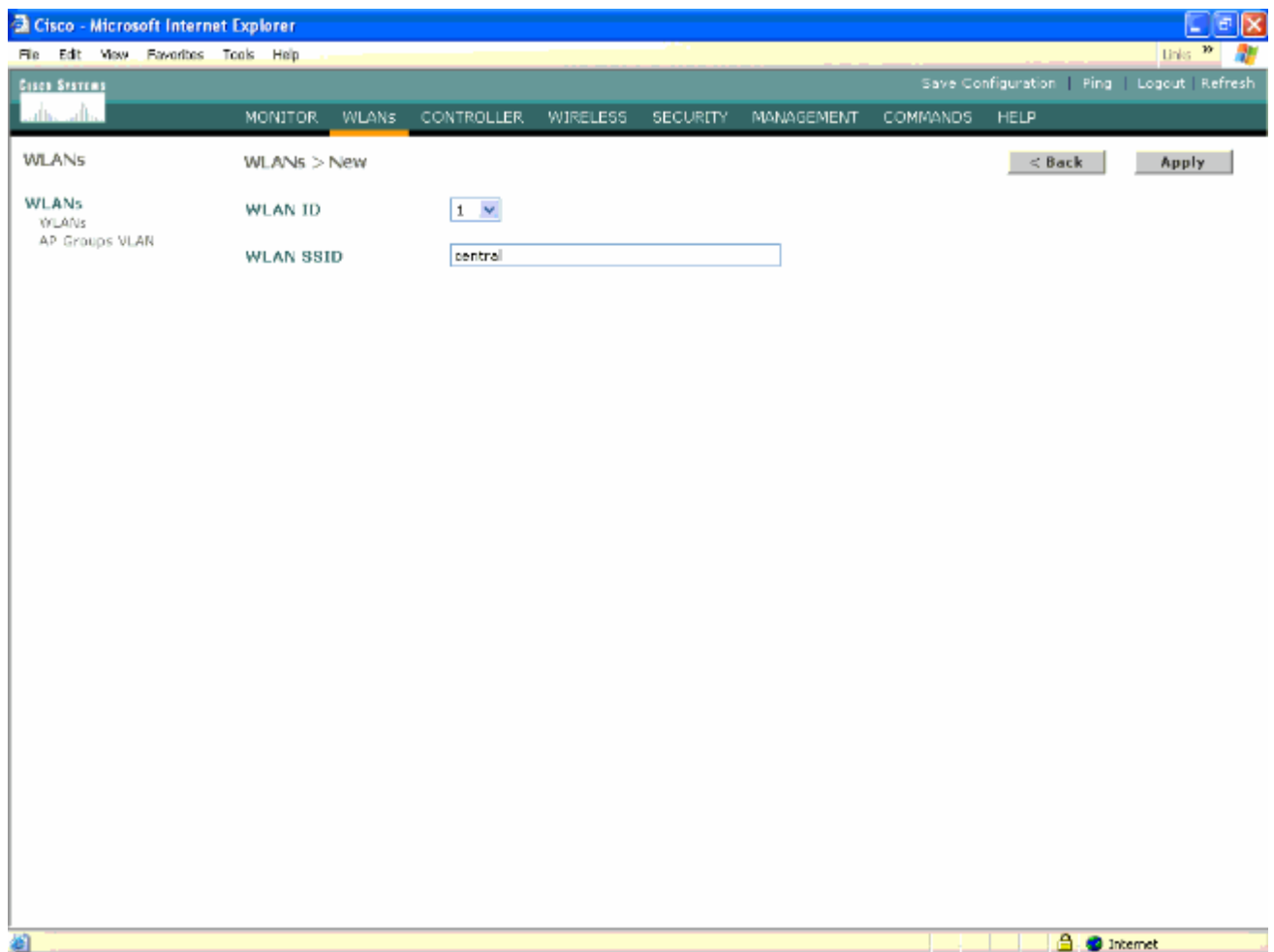
在此模式下，AP 转发所有的客户认证以及数据信息到 WLC，只有在连接模式下，H-REAP 才支持此状态。

配置以下信息：

- (1) SSID 名称：central
- (2) 二层安全：802.1x/LEAP
- (3) H-REAP 本地交换模式：disable

配置 WLC 的相应设置

- 1. 点击 **WLANs** 配置 WLAN



2. 因为使用中心认证，所以在二层安全选择 **802.1x** 认证
3. 在认证服务器选项处，填写服务器地址
4. 因为使用中心交换，需要关闭本地交换选项

Cisco - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Links

Cisco Systems Save Configuration Ping Logout Refresh

MONITOR **WLANs** CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP

WLANs

WLANs

AP Groups VLAN

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 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.

Layer 2 Security 802.1X ☐ MAC Filtering

Layer 3 Security None ☐ 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

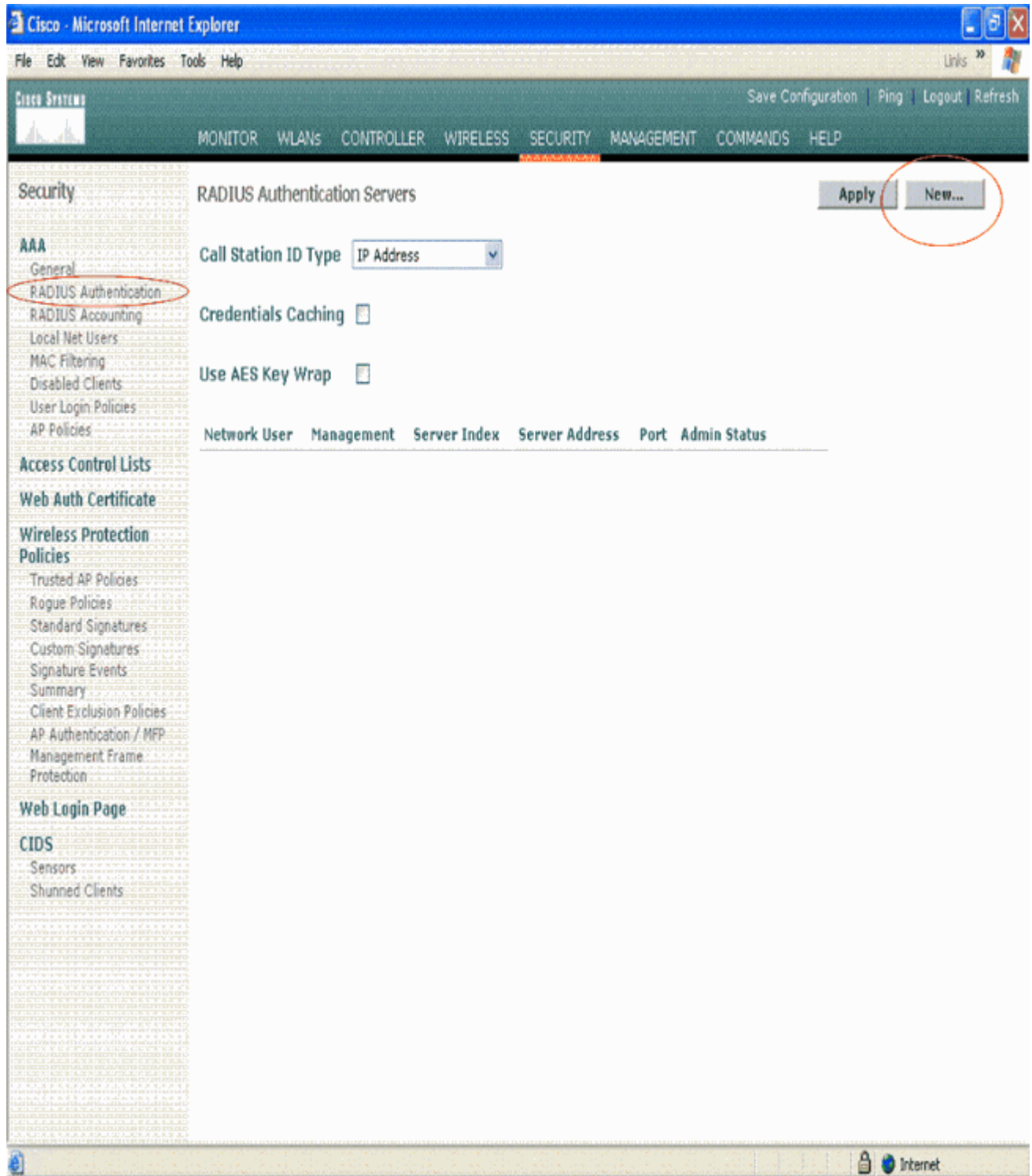
Radius Servers

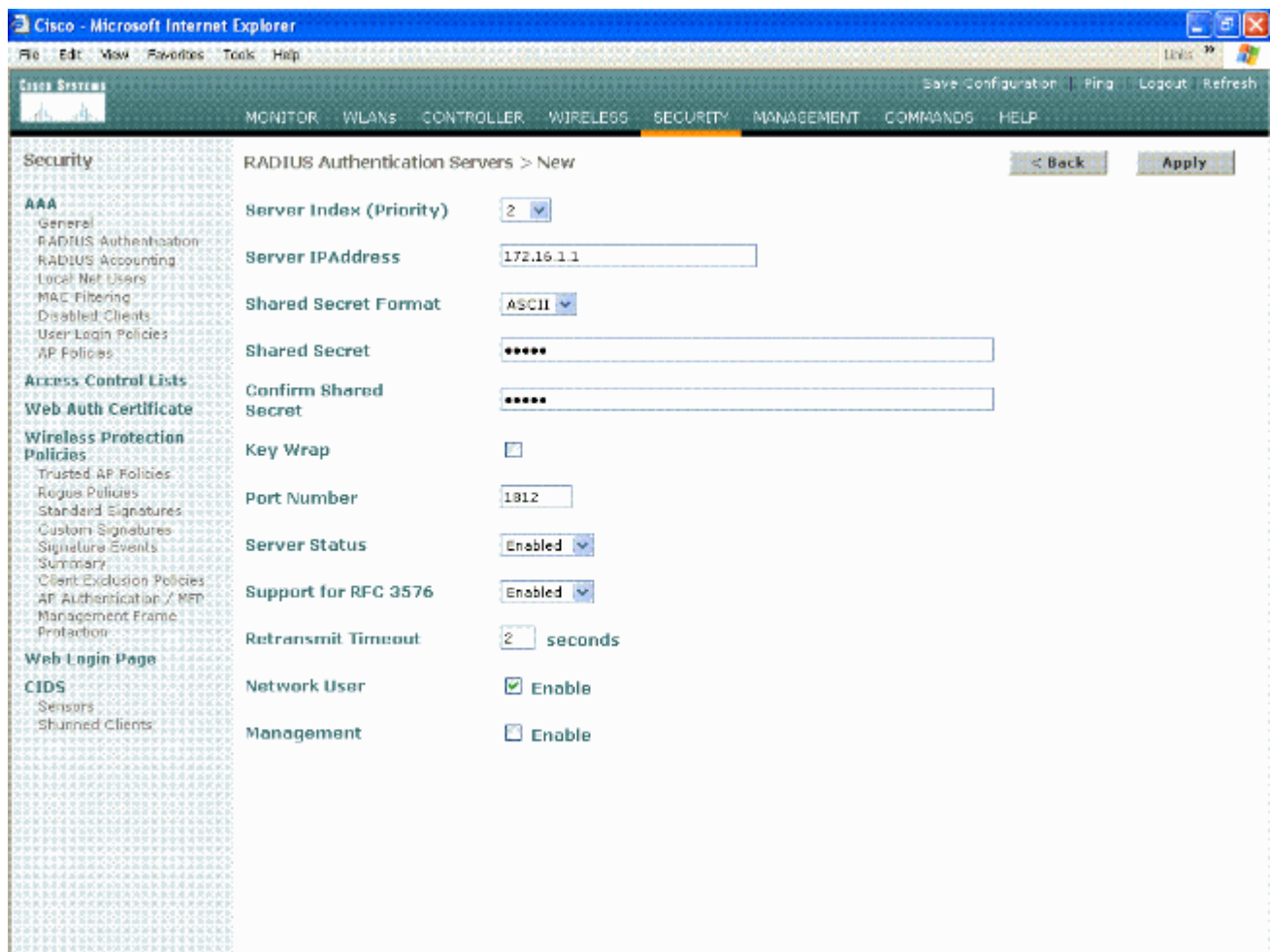
	Authentication Servers	Accounting Servers
Server 1	none	none
Server 2	IP:172.16.1.1, Port:1812	none
Server 3	none	none

802.1X Parameters

802.11 Data Encryption	Type	Key Size
☒ WEP	WEP	104 bits

5. 选择 **Security > Radius Authentication** 配置服务器信息



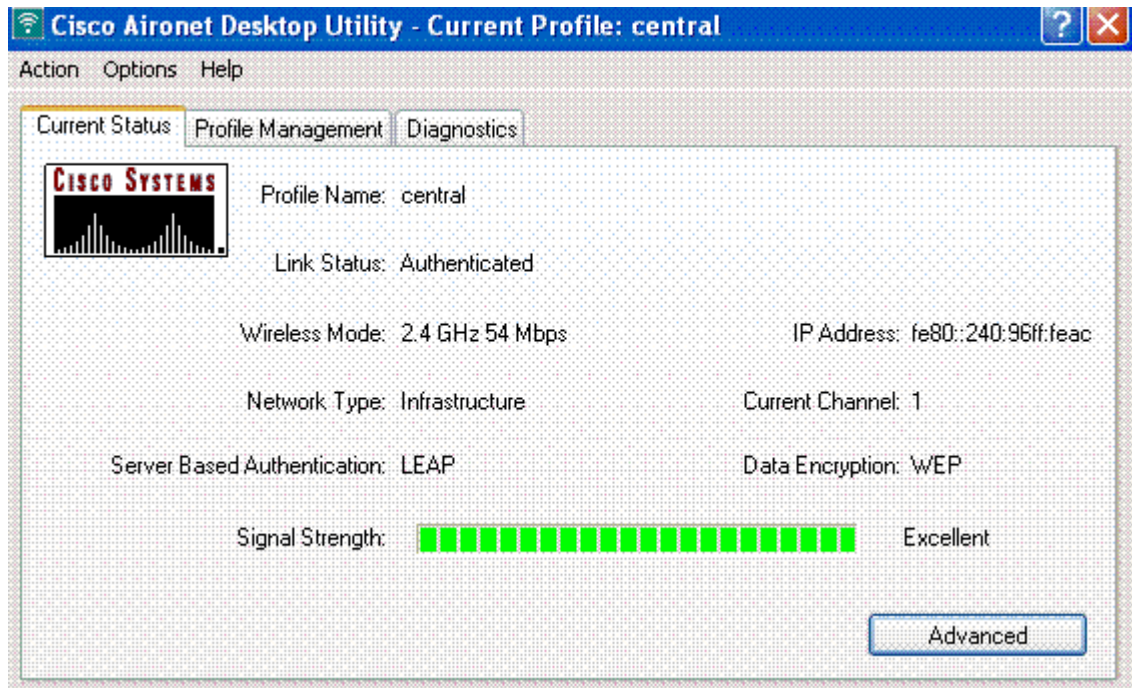
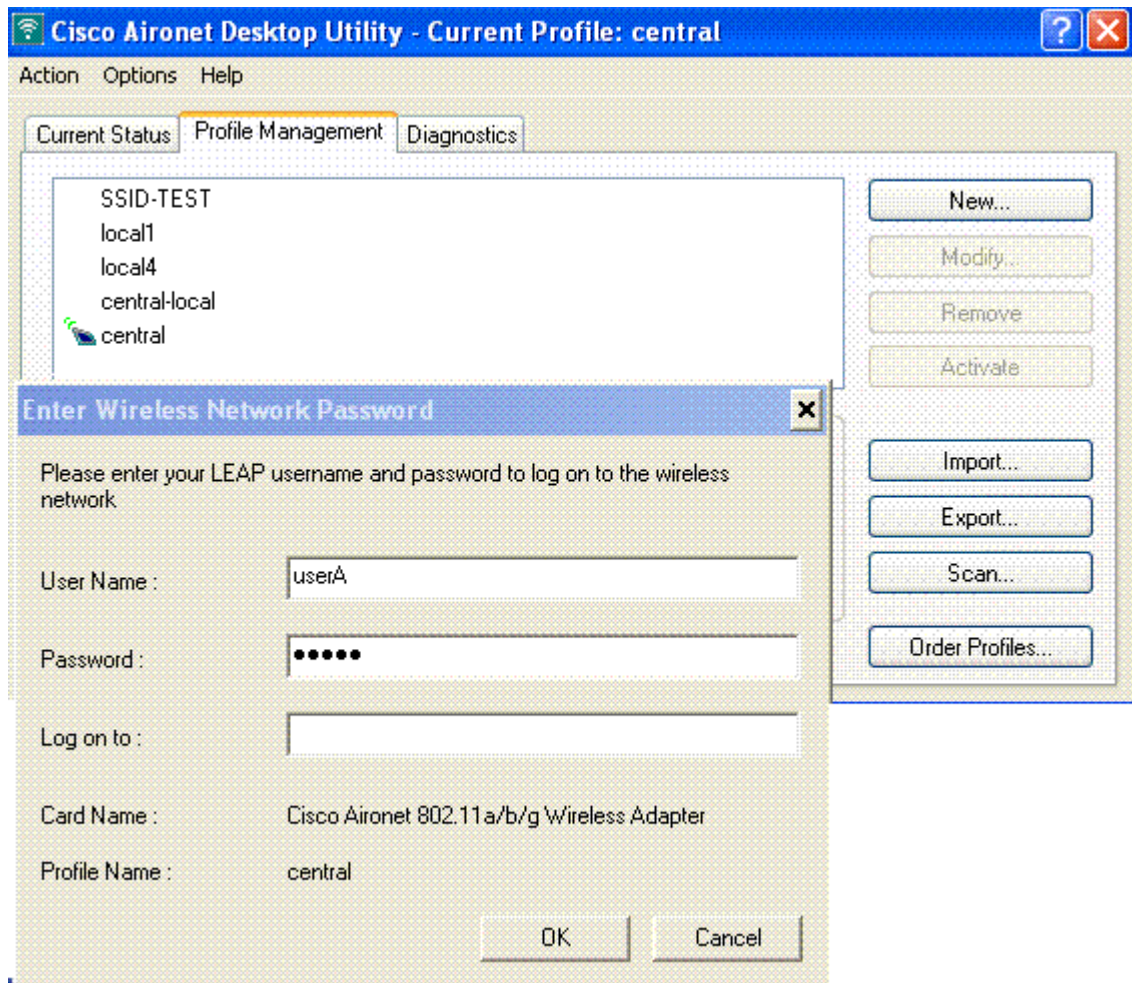


【译者注】使用相同的共享密钥在 WLC 与 ACS 之间，此文档中没有涉及使用 EAP 的认证方法，获取相关信息，请参考

http://www.cisco.com/en/US/tech/tk722/tk809/technologies_configuration_example09186a0080665d18.shtml

检测中心认证，中心交换

1. 配置无线客户端同样的 SSID 以及安全设置
2. 输入用户名与密码激活在 ACS 上配置的用户



【译者注】此文档中的客户端使用静态 IP 地址 172.18.1.5，也可以使用 DHCP 配置

认证失败，本地交换失败

WLC 使用每秒一次，共五次心跳，检测 AP 与 WLC 的联系。

如果没有收到，将停止 AP 与 WLC 的注册

在 WLC 上 **debug lwapp events enable** 后，相应的输出：

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 apfSpamProcessStateChangeInSpamContext: 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 apfSpamProcessStateChangeInSpamContext: 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 apfSpamProcessStateChangeInSpamContext: 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 apfSpamProcessStateChangeInSpamContext: 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!

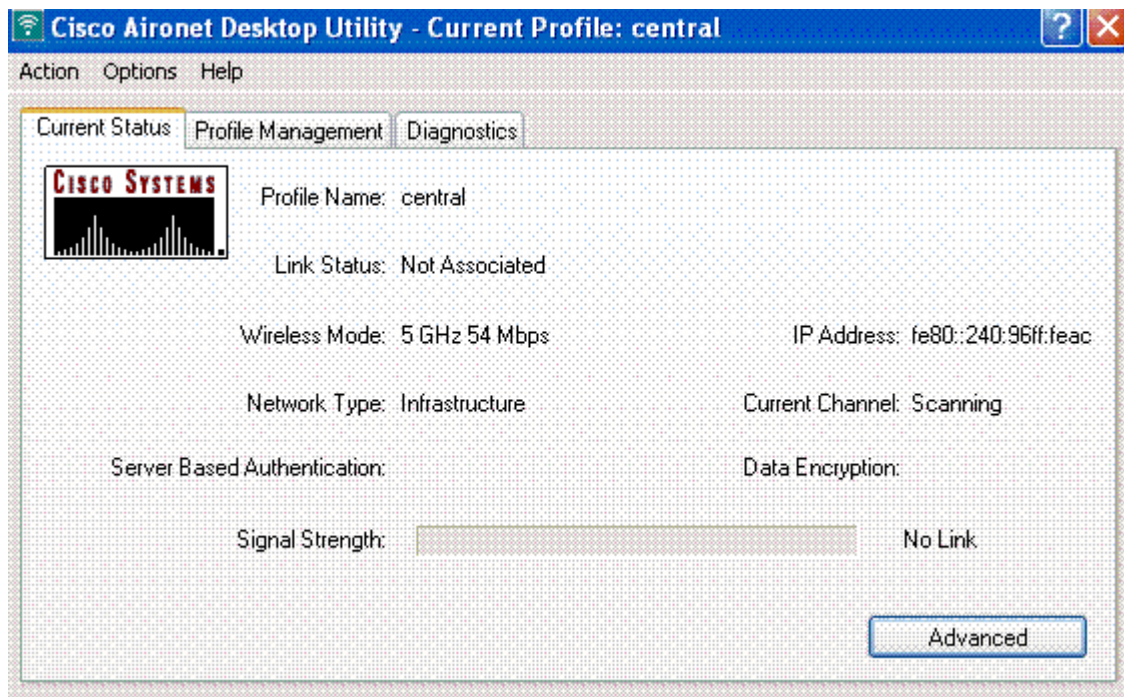
Thu Jan 18 03:19:32 2007: 00:15:c7:ab:55:90 **Deregister LWAPP event for AP 00:15:c7:ab:55:90 slot 0**

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

H-REAP 变为独立模式，**debug lwapp reap** 可以检测到相应输出

因为之前的数据已经被中心认证，中心交换，控制信息和数据都被转发到 WLC，因此，没有 WLC 的存在，客户端不能保持相应的连接，一下是相应的客户端显示



中心认证，本地交换

在这个模式下，WLC 认证所有客户信息，但是 H-REAP 本地交换数据。在客户端成功认证后，WLC 发送控制信息到 H-REAP，使其本地交换数据，每当一个客户被成功认证后，就会发送相应的控制信息，这个状态只能用在连接模式。

配置信息：

- (1) SSID 名称: **central-local**
- (2) 二层安全: **802.1x/LEAP**.
- (3) H-REAP 本地交换-**Enabled**

配置 WLC

1. 配置 WLAN 的 SSID，点击 **WLANs**
2. 因为使用中心认证，所以在二层安全选项中选上 **802.1x authentication**
3. 在认证服务器相应选项中，配置认证服务器信息
4. 选中 **H-REAP Local Switching**

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

AP Groups VLAN

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 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.

Layer 2 Security 802.1X ☐ MAC Filtering

Layer 3 Security None ☐ 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

Radius Servers

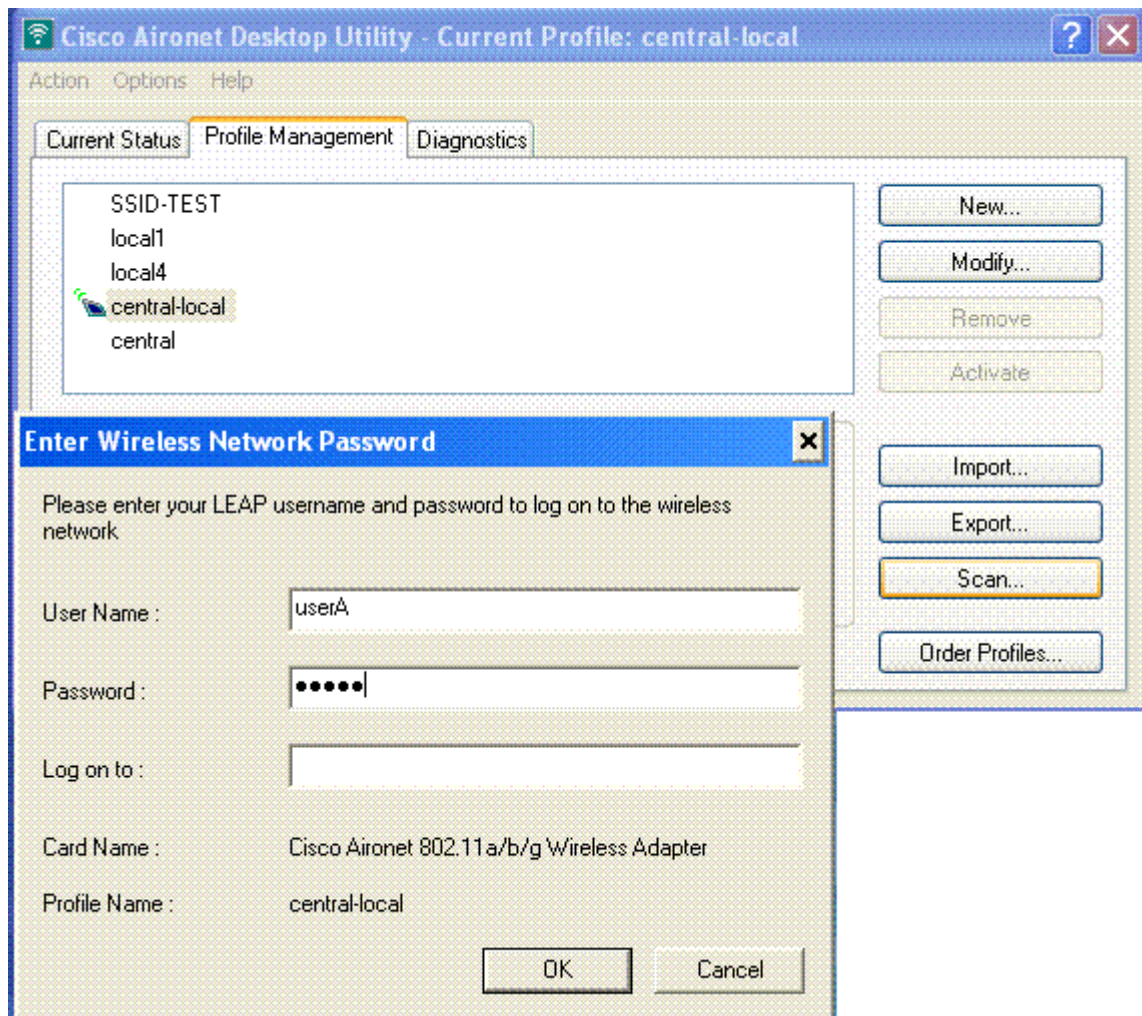
	Authentication Servers	Accounting Servers
Server 1	IP:172.16.1.1, Port:1812	none
Server 2	IP:172.16.1.1, Port:1812	none
Server 3	none	none

802.1X Parameters

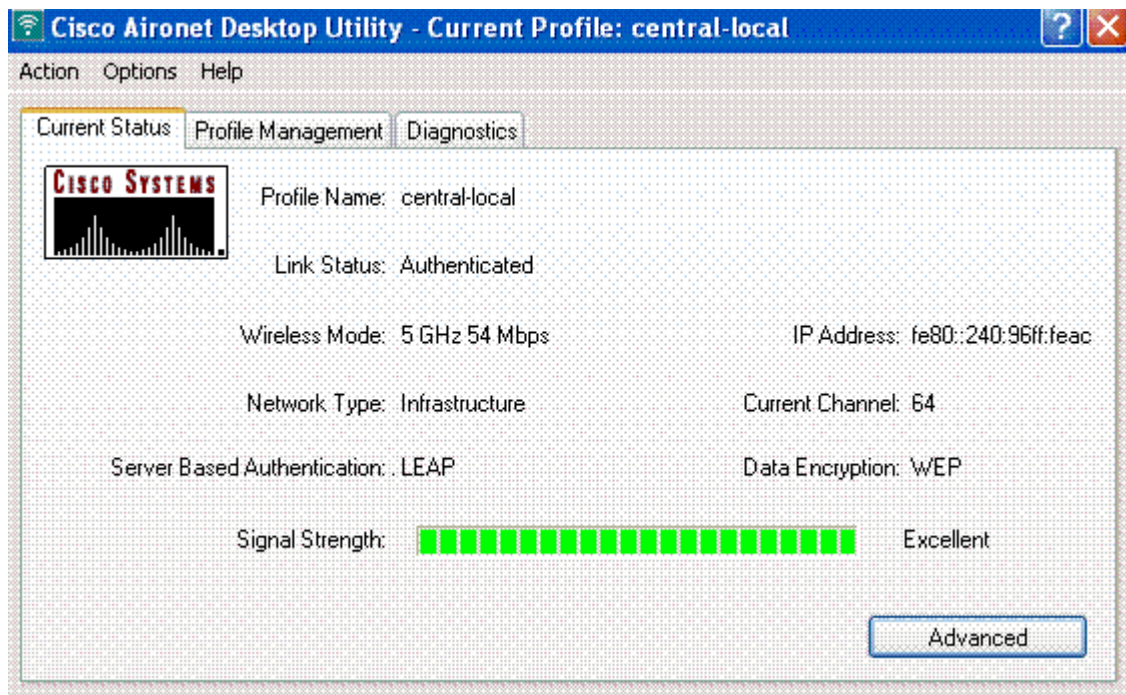
802.11 Data Encryption	Type	Key Size
☒ WEP		104 bits

检测中心认证，本地交换

1. 配置无限客户端的 SSID 与 WLC 的配置相同
2. 输入用户名和密码，要和在认证服务器上配置的一致



3. 点击 ok



认证失败，本地交换

如果在 WLC 上配置了任何认证方式的本地数据交换（比如 EAP 认证，动态 WEP/WPA/WPA2/802.11i，web 认证，或是 NAC），在 WAN 断线后，会转变为认证失败，本地交换的状态，在这个状态下，H-REAP 拒绝新的试图认证的客户端，然而，继续为已经连接上的客户端转发数据，此状态只能在独立模式下运行。

如果 WAN 链路断开，WLC 停止 H-REAP 的注册。

一旦没有注册到 WLC，H-REAP 会运行至独立模式，这个转换的过程可以通过在 CLI 命令下，通过 **debug lwapp REAP** 察看。

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

已经连接上的客户仍然能保持连接，但由于和 WLC 不能通讯，无法进行新客户的认证，H-REAP 停止新客户的连接。

可以通过利用新客户端连接 WLAN 网络，进行上述的验证。

【译者注】当没有客户连接到 WLAN 时，H-REAP 上的 802.11 功能将会停止，将转换为下一个 H-REAP 的状态：认证停止，交换停止。

本地认证，本地交换

在这个状态下，H-REAP 的 AP 会本地认证客户端，本地交换数据。这个状态只能在独立模式，并且配置为本地认证的情况下存在。

先前讲述的中心认证，本地交换的状态，如果要转换到此状态，要配置 A P 为独立本地认证方式，如果没有配置本地认证状态，例如 802.1x 的认证，在独立模式下，H-REAP 进入停止认证，本地交换的模式。

以下是 A P 在独立模式下常用的几种认证方法：

- (1) 开放式
- (2) 共享式
- (3) WPA-PSK
- (4) WPA2-PSK

【译者注】当 A P 在连接模式下，所以得认证都会经过 W L C 进行，当 H-REAP 在独立模式下，以上的认证模式都会本地进行。

范例中使用以下配置：

- (1) S S I D: **local1**
- (2) 二层安全: **WPA-PSK**
- (3) H-REAP 本地交换: **enabled**

在 W L C 上配置以下步骤：

1. 点击 **WLANS** 配置 W L A N
2. 因为使用本地认证方法，选择二层的本地认证方法，例如 **WPA-PSK**
3. 配置 Pre-shared Key，确定客户端与 A P 配置的相同
4. 配置 H-REAP 的模式，**H-REAP Local Switching**

Cisco - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Links

Save Configuration Ping Logout Refresh

CISCO SYSTEMS

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP

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, CRAMITE 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

Layer 3 Security: Static WEP

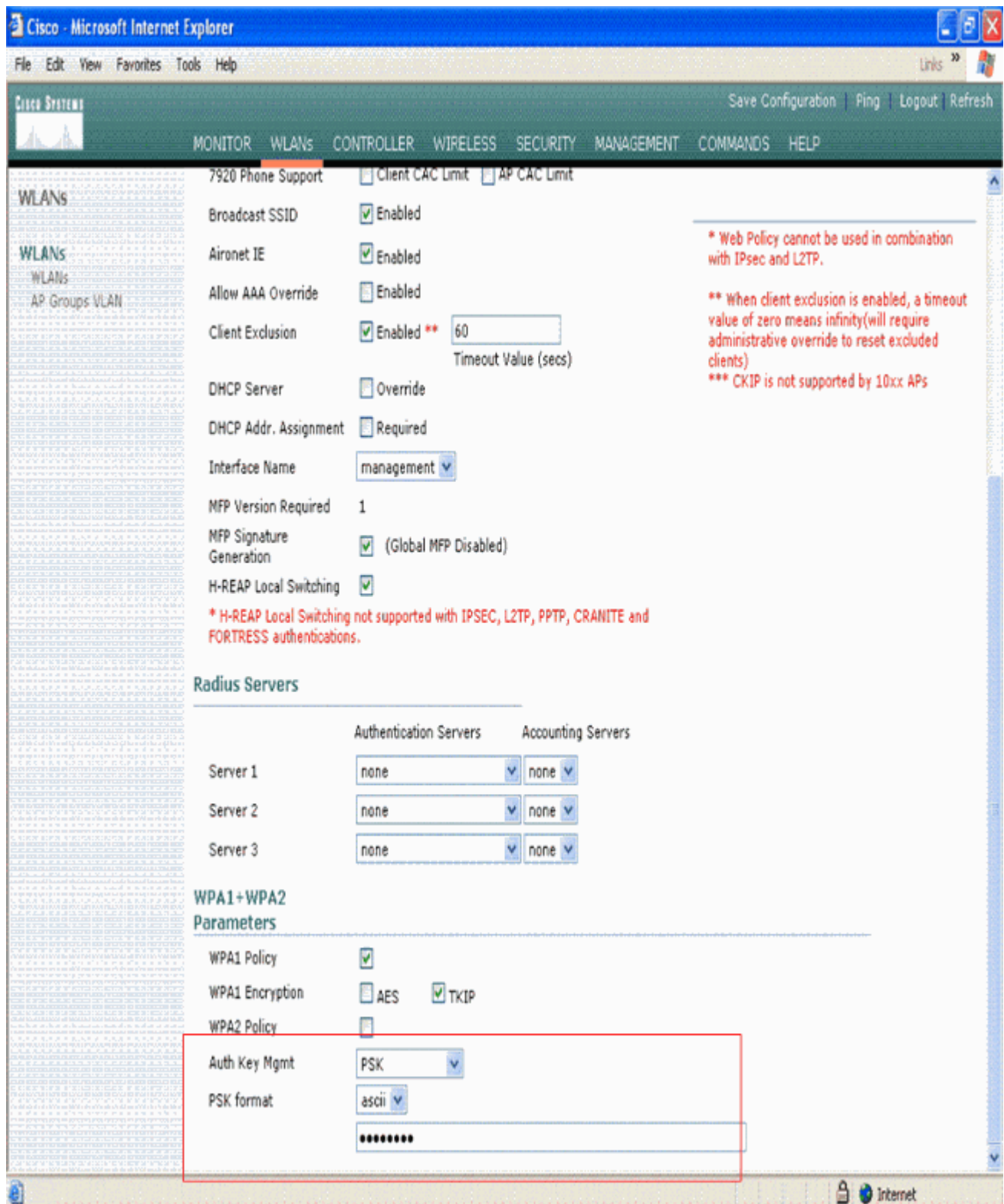
* Web Policy cannot be used in combination with IPsec and L2TP.

** 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



检测本地认证，本地交换

完成以下步骤：

- （1）配置同样的 S S I D 和认证方法，此例中使用 SSID:local1 认证方法：WPA-PSK
- （2）配置客户端的 S S I D
- （3）关闭 W A N 的链路

- W L C 停止注册 H-REAP, H-REAP 进入独立模式
- (4) 转换过程可以通过 CLI 命令 **debug lwapp RE** 察看
 - (5) 使用其它客户端登陆 WLAN,检测认证情况

排错

使用以下命令

show lwapp reap association

debug lwapp clients