

具有轻量AP和无线局域网控制器(WLC)的 Remote-Edge AP (REAP)与配置示例

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[背景信息](#)

[配置](#)

[网络图](#)

[配置WLC以执行基本操作并配置WLAN](#)

[将AP置于远程站点进行安装](#)

[配置2800路由器以建立WAN链路](#)

[在远程站点部署REAP AP](#)

[验证](#)

[故障排除](#)

[故障排除命令](#)

[相关信息](#)

简介

思科统一无线网络引入的远程边缘接入点(REAP)功能允许从无线局域网(WLAN)控制器(WLC)远程部署思科轻量接入点(LAP)。这使他们成为分支机构和小型零售场所的理想之选。本文档介绍如何使用Cisco 1030系列LAP和4400 WLC部署基于REAP的WLAN网络。

先决条件

要求

尝试进行此配置之前，请确保满足以下要求：

- 了解 WLC 和如何配置 WLC 基本参数
- 了解Cisco 1030 LAP中的REAP操作模式
- 了解外部DHCP服务器和/或域名系统(DNS)服务器的配置
- 了解 Wi-Fi 保护访问 (WPA) 概念

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 运行固件 4.2 版本的 Cisco 4400 系列 WLC
- 思科1030 LAP
- 运行Cisco IOS®软件版本12.2(13)T13的两台Cisco 2800系列路由器
- 运行固件版本3.0的思科Aironet 802.11a/b/g客户端适配器
- Cisco Aironet Desktop Utility 版本 3.0

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

[规则](#)

有关文档规则的详细信息，请参阅 [Cisco 技术提示规则](#)。

[背景信息](#)

REAP模式使LAP能够驻留在WAN链路上，并且仍然能够与WLC通信并提供常规LAP的功能。目前只有 1030 LAP 支持 REAP 模式。

为了提供此功能，1030 REAP将轻量接入点协议(LWAPP)控制平面与无线数据平面分离。Cisco WLC仍以与使用基于LWAPP的常规接入点(AP)相同的方式用于集中控制和管理，而所有用户数据都在AP本地桥接。在WAN中断期间，对本地网络资源的访问会得到维护。

REAP AP支持两种操作模式：

- 正常REAP模式
- 独立模式

当REAP AP和WLC之间的WAN链路打开时，LAP将在正常REAP模式下设置。当LAP在正常REAP模式下运行时，它们最多可支持16个WLAN。

当WLC和LAP之间的WAN链路断开时，启用REAP的LAP将切换到独立模式。在独立模式下，如果WLAN配置了有线等效保密(WEP)或任何本地身份验证方法，则REAP LAP只能独立支持一个WLAN而不支持WLC。在这种情况下，REAP AP支持的WLAN是AP(WLAN 1)上配置的第一个WLAN。这是因为大多数其他身份验证方法需要向控制器传递信息或从控制器传递信息，并且当WAN链路关闭时，此操作不可能。在独立模式下，LAP支持最少的功能集。下表显示REAP LAP在独立模式下支持的一组功能，与REAP LAP在正常模式下（当WAN链路打开且与WLC的通信打开时）支持的功能相比：

REAP LAP在正常REAP模式和独立模式下支持的功能

		REAP (normal mode)	REAP (standalone mode)
Protocols	IPv4	Yes	Yes
	IPv6	Yes	Yes
	All other protocols	Yes (only if client is also IP enabled)	Yes (only if client is also IP enabled)
	IP Proxy ARP	No	No
WLAN	Number of SSIDs	16	1 (the first one)
	Dynamic channel assignment	Yes	No
	Dynamic power control	Yes	No
	Dynamic load balancing	Yes	No
VLAN	Multiple interfaces	No	No
	802.1Q Support	No	No
WLAN Security	Rogue AP detection	Yes	No
	Exclusion list	Yes	Yes (existing members only)
	Peer-to-Peer blocking	No	No
	Intrusion Detection System	Yes	No
Layer 2 Security	MAC authentication	Yes	No
	802.1X	Yes	No
	WEP (64/128/152bits)	Yes	Yes
	WPA-PSK	Yes	Yes
	WPA2-PSK	No	No
	WPA-EAP	Yes	No
	WPA2-EAP	Yes	No
Layer 3 Security	Web Authentication	No	No
	IPsec	No	No
	L2TP	No	No
	VPN Pass-through	No	No
	Access Control Lists	No	No
QoS	QoS Profiles	Yes	Yes
	Downlink QoS (weighted round-robin queues)	Yes	Yes
	802.1p support	No	No
	Per-user bandwidth contracts	No	No
	WMM	No	No
	802.11e (future)	No	No
	AAA QoS Profile override	Yes	No
Mobility	Intra-subnet	Yes	Yes
	Inter-subnet	No	No
DHCP	Internal DHCP Server	No	No
	External DHCP Server	Yes	Yes
Topology	Direct connect (2006)	No	No

下表显示，在两种模式下，REAP LAP不支持多个VLAN。不支持多个VLAN，因为REAP LAP只能驻留在单个子网上，因为它们无法执行IEEE 802.1Q VLAN标记。因此，每个服务集标识符 (SSID)上的流量终止于与有线网络相同的子网。因此，即使无线流量可以在SSID之间的空中分段，有线端的数据流量也不会分离。

有关REAP部署以及如何管理REAP及其限制的详细信息，请参阅分支机构的REAP部署指南。

配置

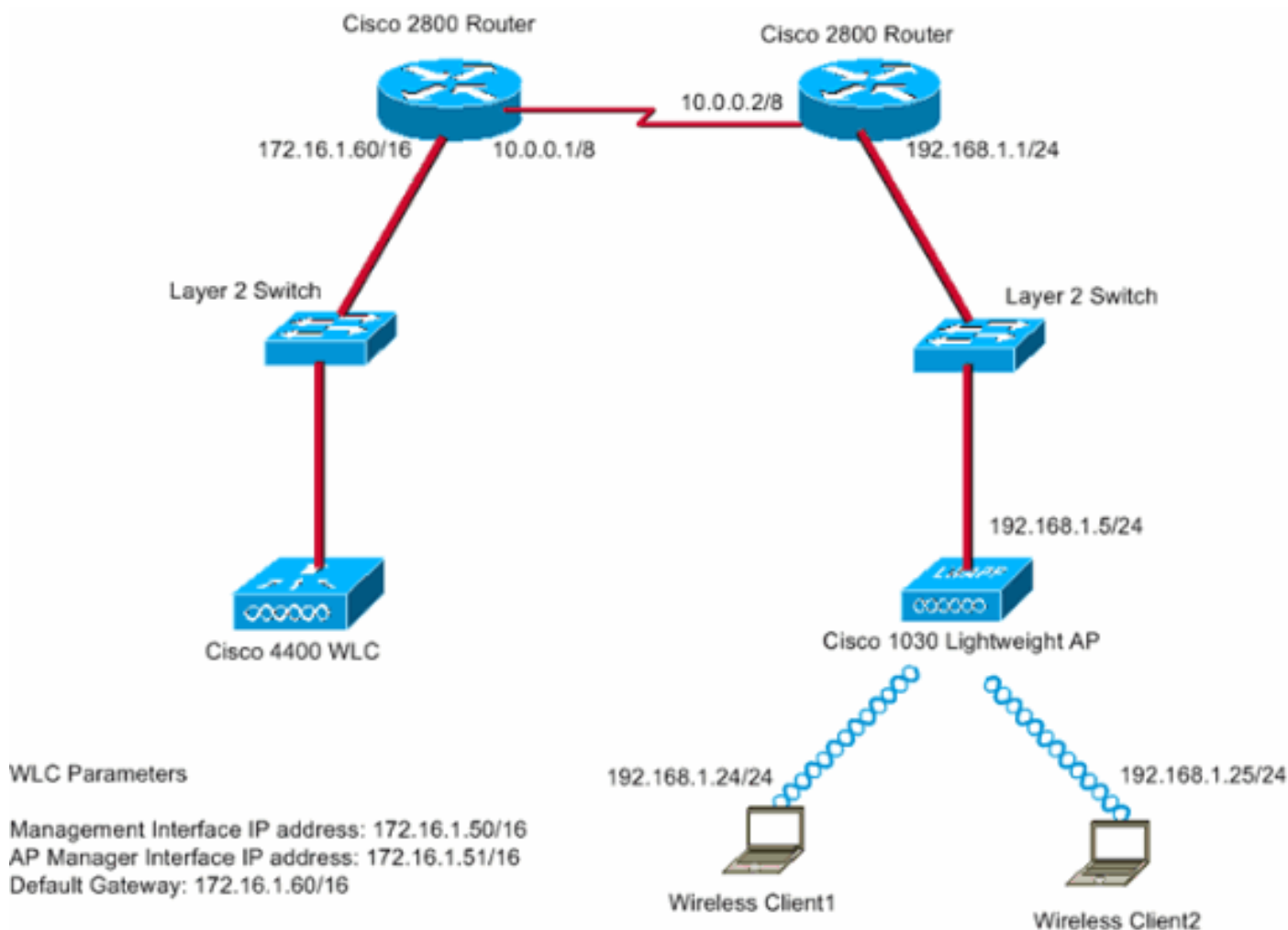
本部分提供有关如何配置本文档所述功能的信息。

要配置设备以实施网络设置，请完成以下步骤：

1. [配置WLC以执行基本操作并配置WLAN。](#)
2. [将AP置于远程站点进行安装。](#)
3. [配置2800路由器以建立WAN链路。](#)
4. [在远程站点部署REAP LAP。](#)

网络图

本文档使用以下网络设置：



总部使用租用线路连接到分支机构。租用线路在每端的2800系列路由器上终止。本示例使用开放最短路径优先(OSPF)协议在WAN链路上使用PPP封装路由数据。4400 WLC位于主办公室，1030 LAP必须部署在远程办公室。1030 LAP必须支持两个WLAN。以下是WLAN的参数：

- WLAN 1SSID - SSID1身份验证 — 打开加密 — 临时密钥完整性协议(TKIP) (WPA预共享密钥 [WPA-PSK])
- WLAN 2SSID - SSID2身份验证 — 可扩展身份验证协议(EAP)加密 — TKIP注意：对于WLAN 2，本文档中的配置使用WPA (802.1x身份验证和TKIP进行加密)。

您必须为此设置配置设备。

配置WLC以执行基本操作并配置WLAN

您可以在命令行界面(CLI)上使用启动配置向导来配置WLC以执行基本操作。此外，也可以使用 GUI

配置 WLC。本文档介绍使用CLI上的启动配置向导在WLC上进行的配置。

首次启动 WLC 之后，它将直接进入启动配置向导。使用配置向导配置基本设置。可以在 CLI 或 GUI 中运行该向导。以下是启动配置向导的示例：

```
Welcome to the Cisco Wizard Configuration Tool
Use the '-' character to backup
System Name [Cisco_33:84:a0]: WLC_MainOffice
Enter Administrative User Name (24 characters max): admin
Enter Administrative Password (24 characters max): *****
Management Interface IP Address: 172.16.1.50
Management Interface Netmask: 255.255.0.0
Management Interface Default Router: 172.16.1.60
Management Interface VLAN Identifier (0 = untagged):
Management Interface Port Num [1 to 4]: 1
Management Interface DHCP Server IP Address: 172.16.1.1
AP Manager Interface IP Address: 172.16.1.51
AP-Manager is on Management subnet, using same values
AP Manager Interface DHCP Server (172.16.1.1):
Virtual Gateway IP Address: 1.1.1.1
Mobility/RF Group Name: Main
Network Name (SSID): SSID1
Allow Static IP Addresses [YES][no]: Yes
Configure a RADIUS Server now? [YES][no]: no
Warning! The default WLAN security policy requires a RADIUS server.
Please see documentation for more details.
Enter Country Code (enter 'help' for a list of countries) [US]:
Enable 802.11b Network [YES][no]: Yes
Enable 802.11a Network [YES][no]: Yes
Enable 802.11g Network [YES][no]: Yes
Enable Auto-RF [YES][no]: Yes

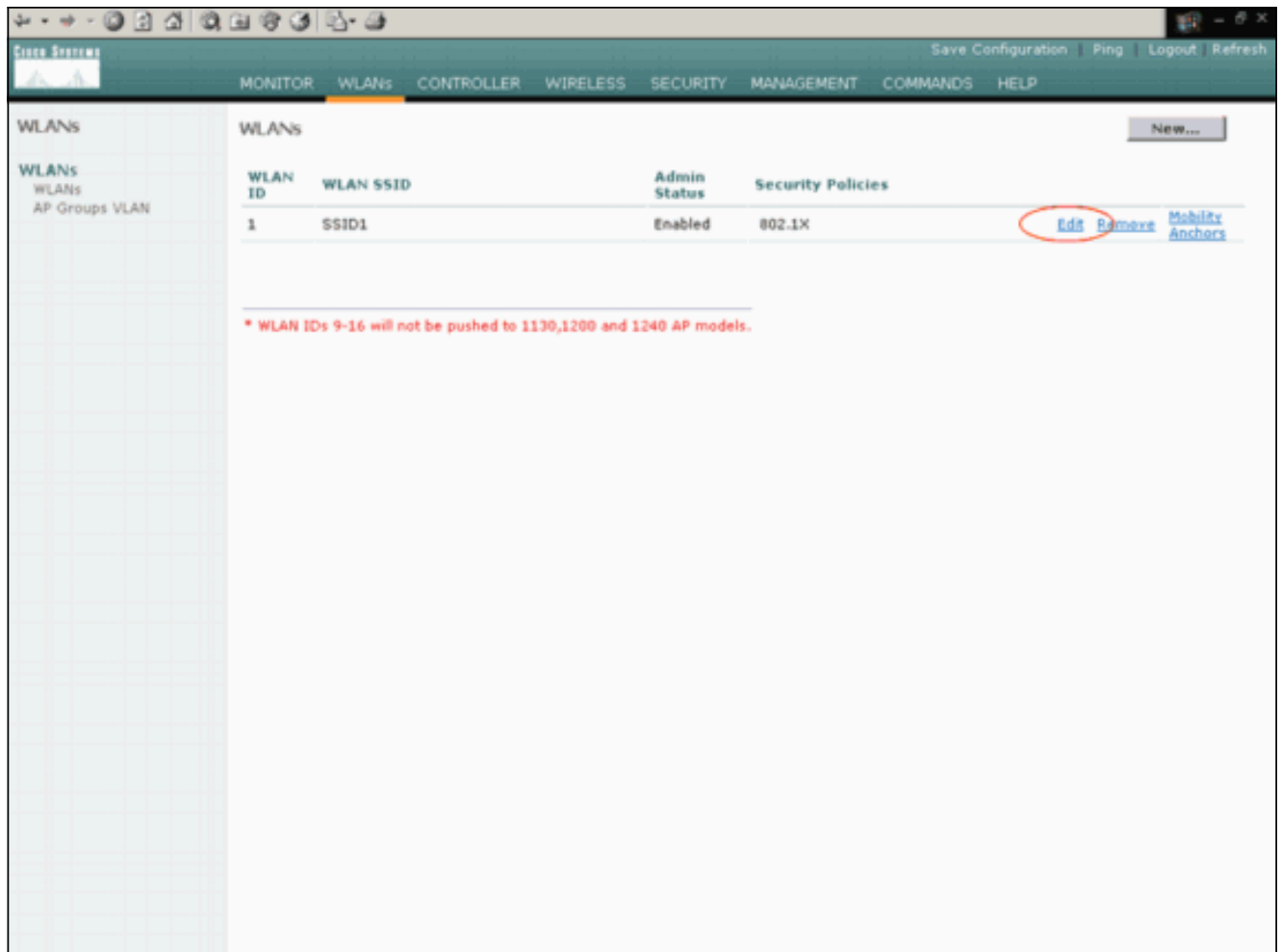
Configuration saved!
Resetting system with new configuration...
```

本示例在WLC上配置以下参数：

- 系统名称
- 管理接口 IP 地址
- AP管理器接口IP地址
- 管理接口端口号
- 管理接口VLAN标识符
- 移动组名称
- SSID
- 许多其他参数

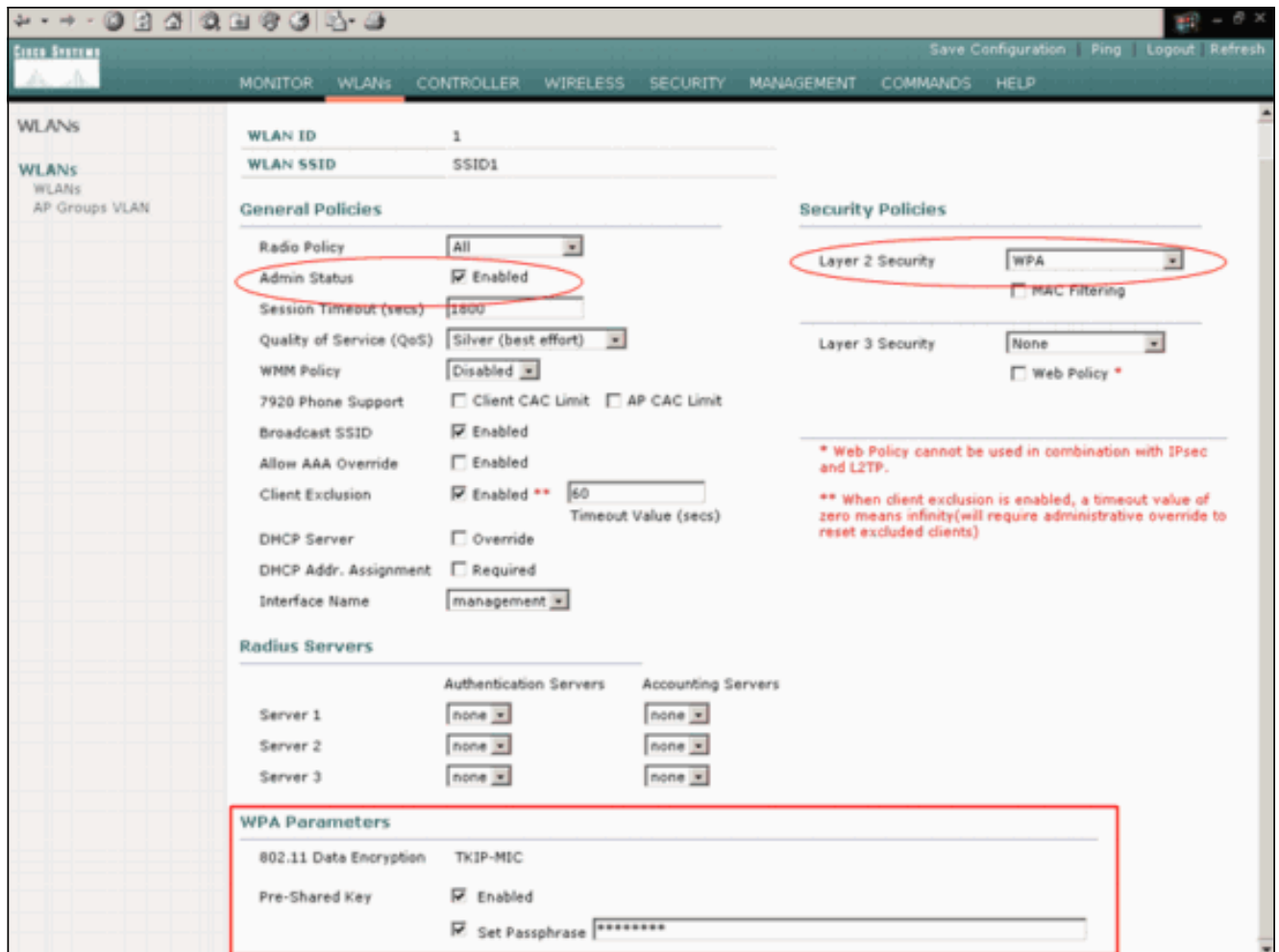
这些参数用于设置WLC以执行基本操作。如本节的WLC输出所示，WLC使用172.16.1.50作为管理接口IP地址，使用172.16.1.51作为AP管理器接口IP地址。要为网络配置两个WLAN，请在WLC上完成以下步骤：

1. 在WLC GUI中，单击窗口顶部菜单中的WLAN。随即显示 WLAN 窗口。此窗口列出在WLC上配置的WLAN。由于您使用启动配置向导配置了一个WLAN，因此必须为此WLAN配置其他参数。
2. 单击Edit查看WLAN SSID1。示例如下
：



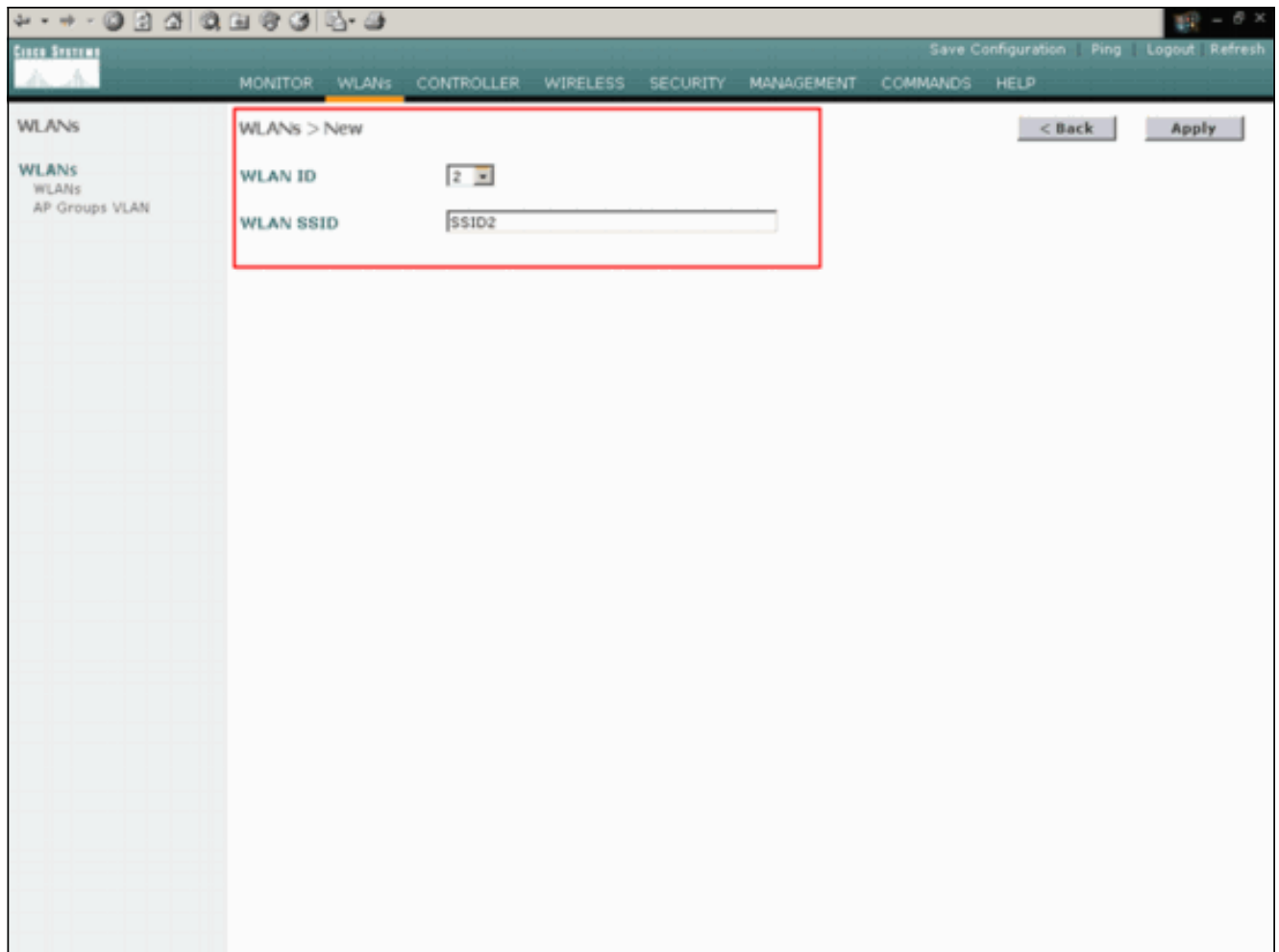
这时将显示“WLANs”>“Edit”窗口。在此窗口中，您可以配置特定于WLAN的参数，包括常规策略、安全策略、RADIUS服务器等。

3. 在WLANs > Edit窗口中进行以下选择：在General Policies区域，选中Admin Status旁边的 **Enabled**复选框以启用此WLAN。从第2层安全下拉菜单中选择**WPA**，以便将WPA用于WLAN 1。在窗口底部定义WPA参数。要在WLAN 1上使用WPA-PSK，请选中WPA Parameters区域中Pre-Shared Key旁的**Enabled**复选框，并输入WPA-PSK的口令。WPA-PSK将使用TKIP进行加密。**注意**：WPA-PSK密码必须与客户端适配器上配置的密码匹配，WPA-PSK才能正常工作。单击 **Apply**。示例如下：
：



您已为WPA-PSK加密配置了WLAN 1。

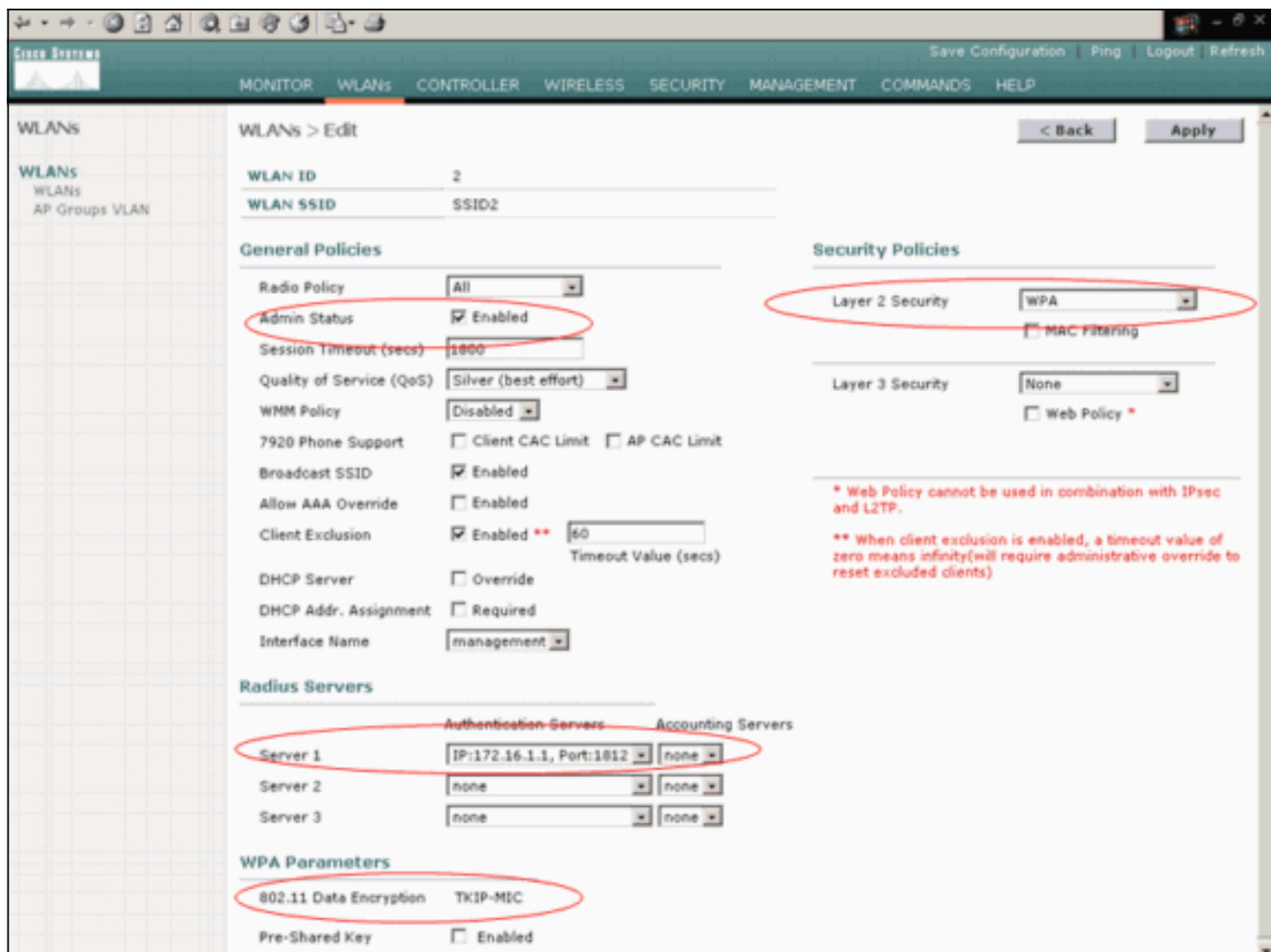
- 要定义WLAN 2，请在WLANs窗口中单击New。系统将显示WLAN > New窗口。
- 在WLAN > New窗口中，定义WLAN ID和WLAN SSID，然后单击Apply。示例如下：



系统将显示第二个WLAN的WLAN > Edit窗口。

6. 在WLANs > Edit窗口中进行以下选择：在General Policies区域，选中Admin Status旁边的**Enabled**复选框以启用此WLAN。从第2层安全下拉菜单中选择**WPA**，以便为此WLAN配置WPA。在Radius Servers区域中，选择用于客户端身份验证的适当RADIUS服务器。单击**Apply**。示例如下

:



注意：本文档不说明如何配置RADIUS服务器和EAP身份验证。有关如何使用WLC配置EAP身份验证的信息，请参阅[使用WLAN控制器\(WLC\)的EAP身份验证配置示例](#)。

将AP置于远程站点进行安装

启动是LAP获取控制器列表的过程，LAP可通过该列表连接控制器。LAP在连接到单个控制器后即会收到移动组中所有控制器的通知。这样，LAP将学习加入组中任何控制器所需的所有信息。

要优化支持REAP的AP，请将AP连接到总部的有线网络。此连接允许AP发现单个控制器。在LAP加入主办公室的控制器后，AP下载与WLAN基础设施和配置对应的AP操作系统(OS)版本。移动组中所有控制器的IP地址将传输到AP。当AP具有其所需的所有信息时，AP可以在远程位置连接。如果IP连接可用，AP可以从列表中发现并加入利用率最低的控制器。

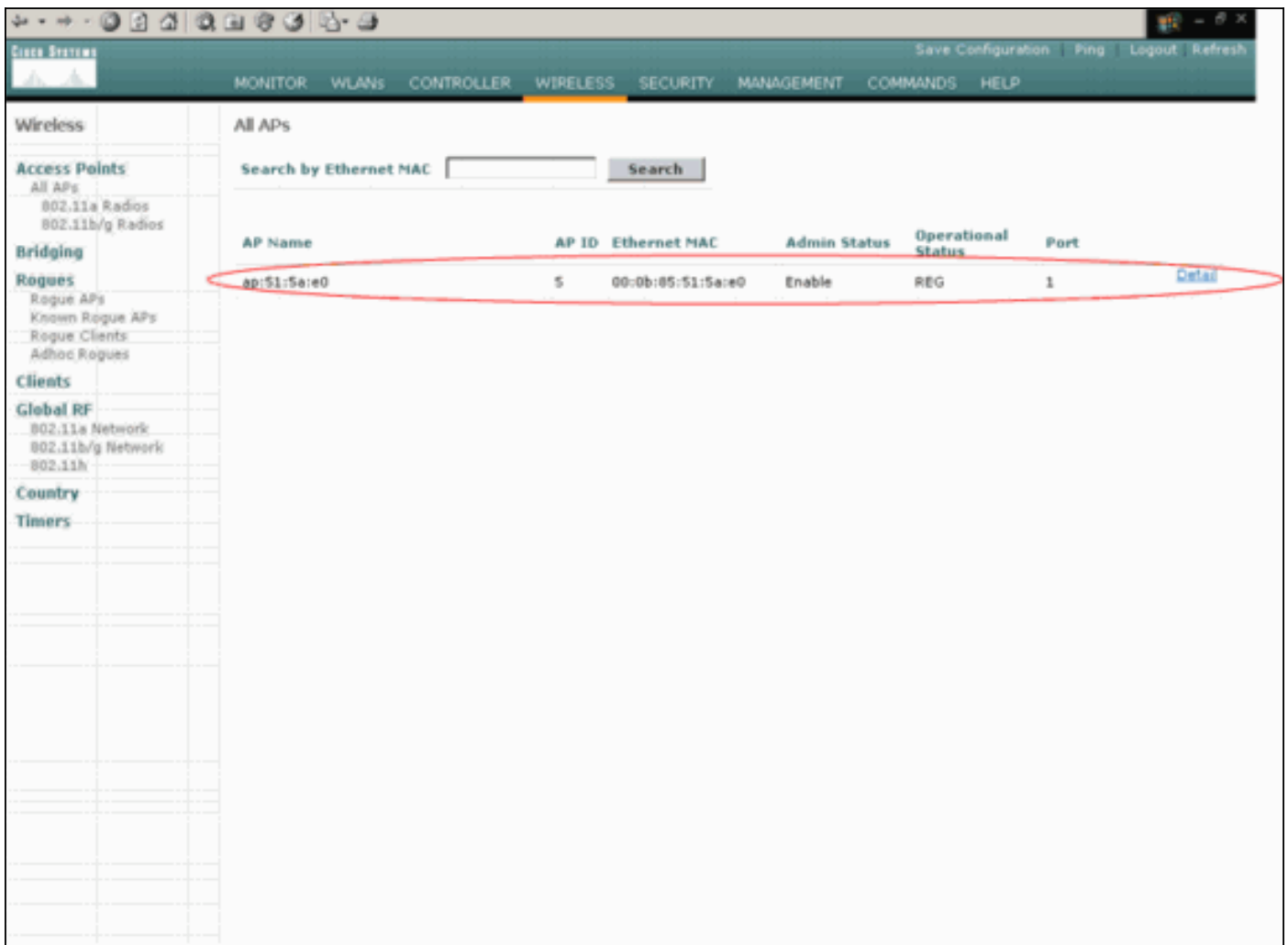
注意：确保在关闭AP之前将AP设置为“REAP”模式，以便将其发送到远程站点。您可以通过控制器CLI或GUI或使用无线控制系统(WCS)模板在AP级别设置模式。默认情况下，AP设置为执行常规“本地”功能。

LAP可以使用以下任一方法来发现控制器：

- **第2层发现**
- **第3层发现**使用本地子网广播使用DHCP选项43使用DNS服务器使用空中调配(OTAP)使用内部DHCP服务器注意：要使用内部DHCP服务器，LAP必须直接连接到WLC。

本文档假设LAP使用DHCP选项43发现机制注册到WLC。有关使用DHCP选项43将LAP注册到控制器以及其他发现机制的详细信息，请参阅[轻量AP\(LAP\)注册到无线LAN控制器\(WLC\)](#)。

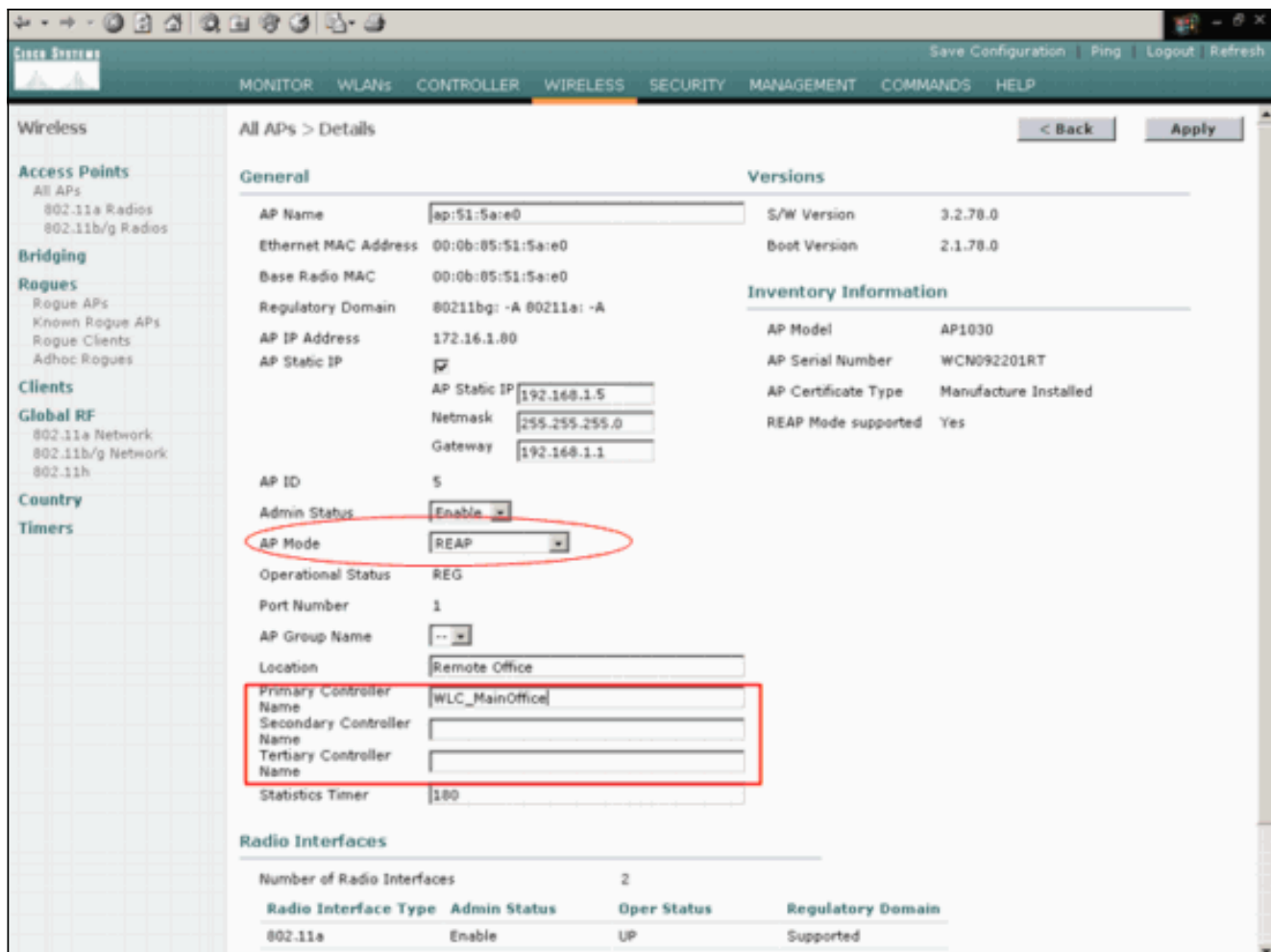
在LAP发现控制器后，您可以在WLC的Wireless（无线）窗口中看到AP已注册到控制器。示例如下



要为正常REAP模式配置LAP，请完成以下步骤：

1. 从 WLC GUI 中，单击 **Wireless**。系统将显示All APs窗口。此窗口列出注册到WLC的AP。
2. 选择必须为REAP模式配置的AP，然后单击**Detail**。系统将显示特定AP的All APs > Detail窗口。在此窗口中，您可以配置AP的各种参数，包括：AP 名称IP地址（您可以更改为静态地址）管理状态安全参数AP模式AP可连接的WLC列表其他参数
3. 从AP Mode下拉菜单中选择**REAP**。此模式仅在支持REAP的AP上可用。
4. 定义AP将用于注册的控制器名称，然后单击**Apply**。您最多可以定义三个控制器名称(主控制器、辅助控制器和第三控制器)。AP 将按照您在此窗口中提供的顺序搜索控制器。因为本示例只使用一个控制器，所以示例将该控制器定义为主控制器。示例如下

：



您已将AP设置为REAP模式，并可以在远程站点部署该模式。

注意：在本示例窗口中，您可以看到AP的IP地址已更改为静态，并且分配了静态IP地址192.168.1.5。这样分配是因为它是将在远程办公室中使用的子网。因此，您仅在启动阶段使用来自DHCP服务器172.16.1.80的IP地址。在AP注册到控制器后，将地址更改为静态IP地址。

配置2800路由器以建立WAN链路

为了建立WAN链路，本示例使用两台带OSPF的2800系列路由器在网络之间路由信息。以下是本文中示例场景中两台路由器的配置：

```

总部

MainOffice#show run
Building configuration...

Current configuration : 728 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname MainOffice
!
!
ip subnet-zero
!
!

```

```

!
!
interface Ethernet0
 ip address 172.16.1.60 255.255.0.0
 !--- This is the interface which acts as the default
 gateway to the WLC. ! interface Virtual-Templatel no ip
 address ! interface Serial0 no ip address ! interface
 Serial1 !--- This is the interface for the WAN link. ip
 address 10.0.0.1 255.0.0.0 encapsulation ppp !--- This
 example uses PPP. Use the appropriate !--- encapsulation
 for the WAN connection. ! router ospf 50 !--- Use OSPF
 to route data between the different networks. log-
 adjacency-changes network 10.0.0.0 0.255.255.255 area 0
 network 172.16.0.0 0.0.255.255 area 0 ! ! ip classless
 ip http server ! ! ! line con 0 line aux 0 line vty 0 4
 ! end

```

分支机构

```

BranchOffice#show run
Building configuration...

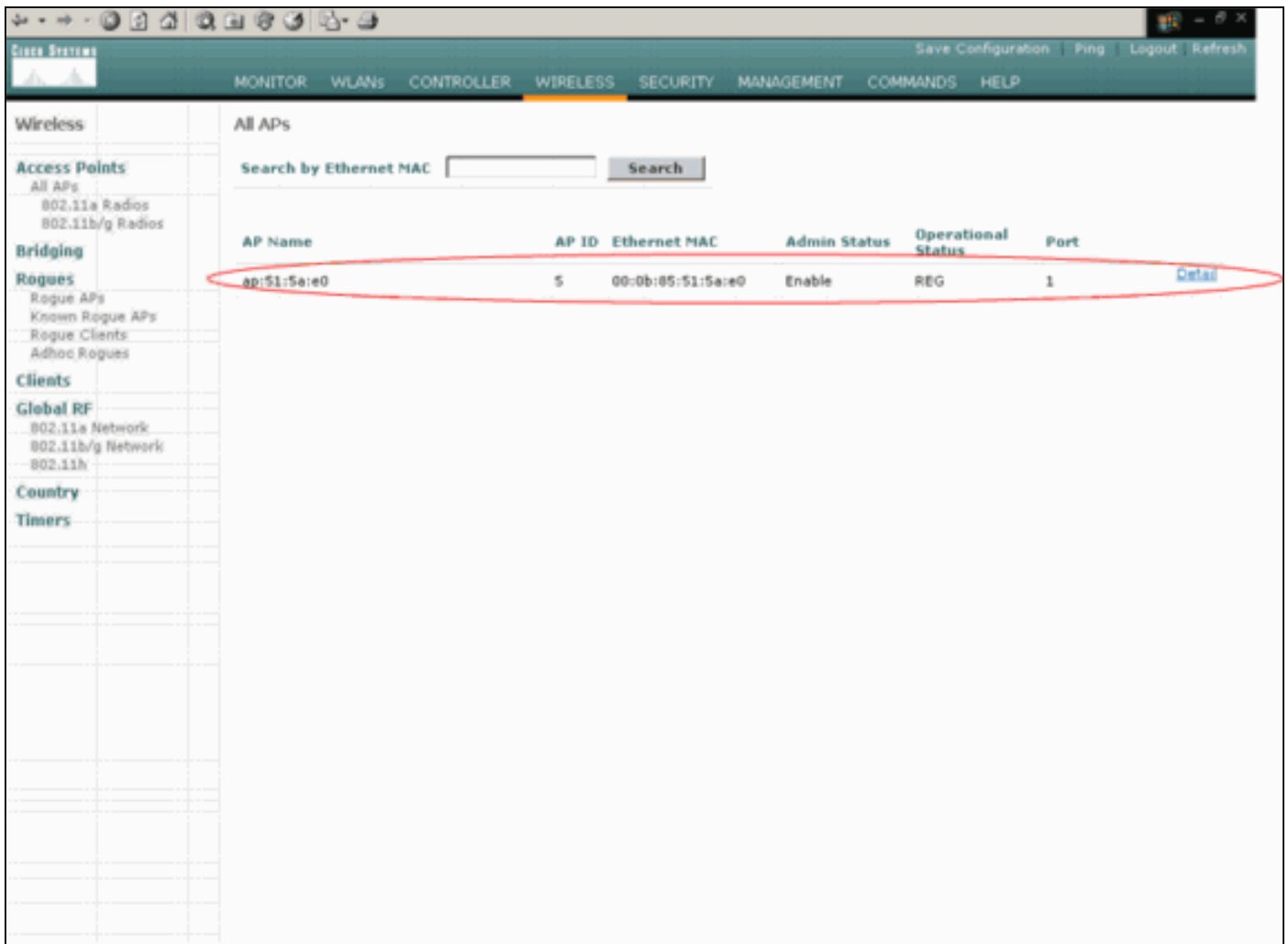
Current configuration : 596 bytes
!
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname BranchOffice
!
!
ip subnet-zero
!
!
!
!
interface Ethernet0
 ip address 192.168.1.1 255.255.255.0
 !--- This is the interface which acts as the default
 gateway to the LAP. ! interface Serial0 no ip address !
 interface Serial1 !--- This is the interface for the WAN
 link. ip address 10.0.0.2 255.0.0.0 encapsulation ppp
 clockrate 56000 ! router ospf 50 !--- Use OSPF to route
 data between the different networks. log-adjacency-
 changes network 10.0.0.0 0.255.255.255 area 0 network
 192.168.1.0 0.0.0.255 area 0 ! ip classless ip http
 server ! ! ! ! line con 0 line aux 0 line vty 0 4 login
 autocommand access enable-timeout 2 ! end

```

在远程站点部署REAP AP

现在，您已在WLC上配置WLAN，为LAP做好准备，并在总部和远程办公室之间建立了WAN链路，您已准备好在远程站点部署AP。

在远程站点启动AP后，AP会按您在启动阶段配置的顺序查找控制器。在AP找到控制器后，AP向控制器注册。下面是一个示例。从WLC中，您可以看到AP已在端口1上加入控制器：



启用了WPA-PSK的SSID SSID1的客户端与WLAN 1上的AP关联。启用了SSID SSID2和802.1x身份验证的客户端与WLAN 2上的AP关联。以下示例显示两个客户端。一个客户端连接到WLAN 1，另一个客户端连接到WLAN 2:

Save Configuration Ping Logout Ref Close

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP

Monitor Clients Items 1 to 2 of 2

Search by MAC address Search

Client MAC Addr	AP Name	AP MAC Addr	WLAN	Type	Status	Auth	Port	
00:40:96:ac:dd:05	ap:51:5a:e0	00:0b:85:51:5a:e0	SSID1	802.11a	Associated	Yes	1	Detail Link Test Disable Remove
00:40:96:ac:e6:57	ap:51:5a:e0	00:0b:85:51:5a:e0	SSID2	802.11a	Associated	Yes	1	Detail Link Test Disable Remove

Summary
Statistics
Controller Ports
Wireless
Rogue APs
Known Rogue APs
Rogue Clients
Adhoc Rogues
802.11a Radios
802.11b/g Radios
Clients
RADIUS Servers

验证

使用此部分确认您的REAP配置工作正常。

注意：在使用debug命令之前，请参阅有关Debug命令的重要信息。

关闭WAN链路。当WAN链路断开时，AP将失去与WLC的连接。然后，WLC会从其列表中注销AP。示例如下：

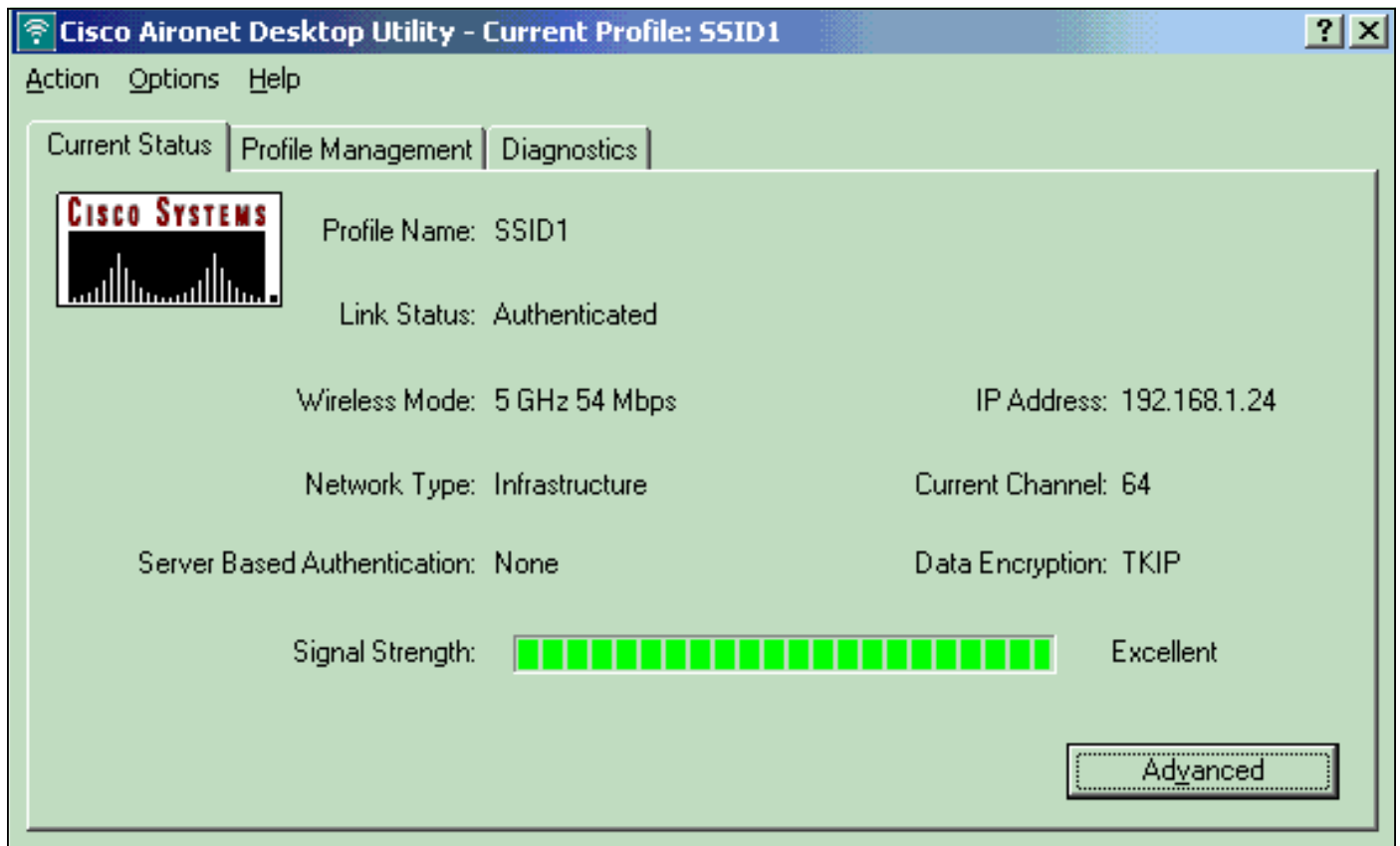
```
(Cisco Controller) >debug lwapp events enable
Wed May 17 15:04:22 2006: Did not receive heartbeat reply from AP 00:0B:85:51:5A:E0
Wed May 17 15:04:22 2006: Max retransmissions reached on AP 00:0B:85:51:5A:E0
(CONFIGURE_COMMAND, 1)
Wed May 17 15:04:22 2006: apfSpamProcessStateChangeInSpamContext: Down LWAPP event for
AP 00:0b:85:51:5a:e0 slot 0
Wed May 17 15:04:22 2006: apfSpamProcessStateChangeInSpamContext: Deregister LWAPP event
for AP 00:0b:85:51:5a:e0 slot 0
Wed May 17 15:04:22 2006: apfSpamProcessStateChangeInSpamContext: Down LWAPP event for
AP 00:0b:85:51:5a:e0 slot 1
Wed May 17 15:04:22 2006: apfSpamProcessStateChangeInSpamContext: Deregister LWAPP event
for AP 00:0b:85:51:5a:e0 slot 1
Wed May 17 15:04:22 2006: spamDeleteLCB: stats timer not initialized for AP
00:0b:85:51:5a:e0
Wed May 17 15:04:22 2006: Received LWAPP Down event for AP 00:0b:85:51:5a:e0 slot 0!
Wed May 17 15:04:22 2006: Deregister LWAPP event for AP 00:0b:85:51:5a:e0 slot 0
Wed May 17 15:04:22 2006: Received LWAPP Down event for AP 00:0b:85:51:5a:e0 slot 1!
```

Wed May 17 15:04:22 2006: Deregister LWAPP event for AP 00:0b:85:51:5a:e0 slot 1

从debug lwapp events enable命令输出中，您可以看到WLC取消注册AP，因为WLC未收到来自AP的心跳应答。检测信号应答类似于保活消息。控制器尝试五个连续的心跳，间隔1秒。如果WLC未收到应答，WLC将注销AP。

当AP处于独立模式时，AP电源LED闪烁。与第一个WLAN(WLAN 1)关联的客户端仍与AP关联，因为第一个WLAN中的客户端仅配置为WPA-PSK加密。LAP在独立模式下处理加密本身。以下示例显示连接到WLAN 1且带SSID1和WPA-PSK的客户端的状态（当WAN链路关闭时）：

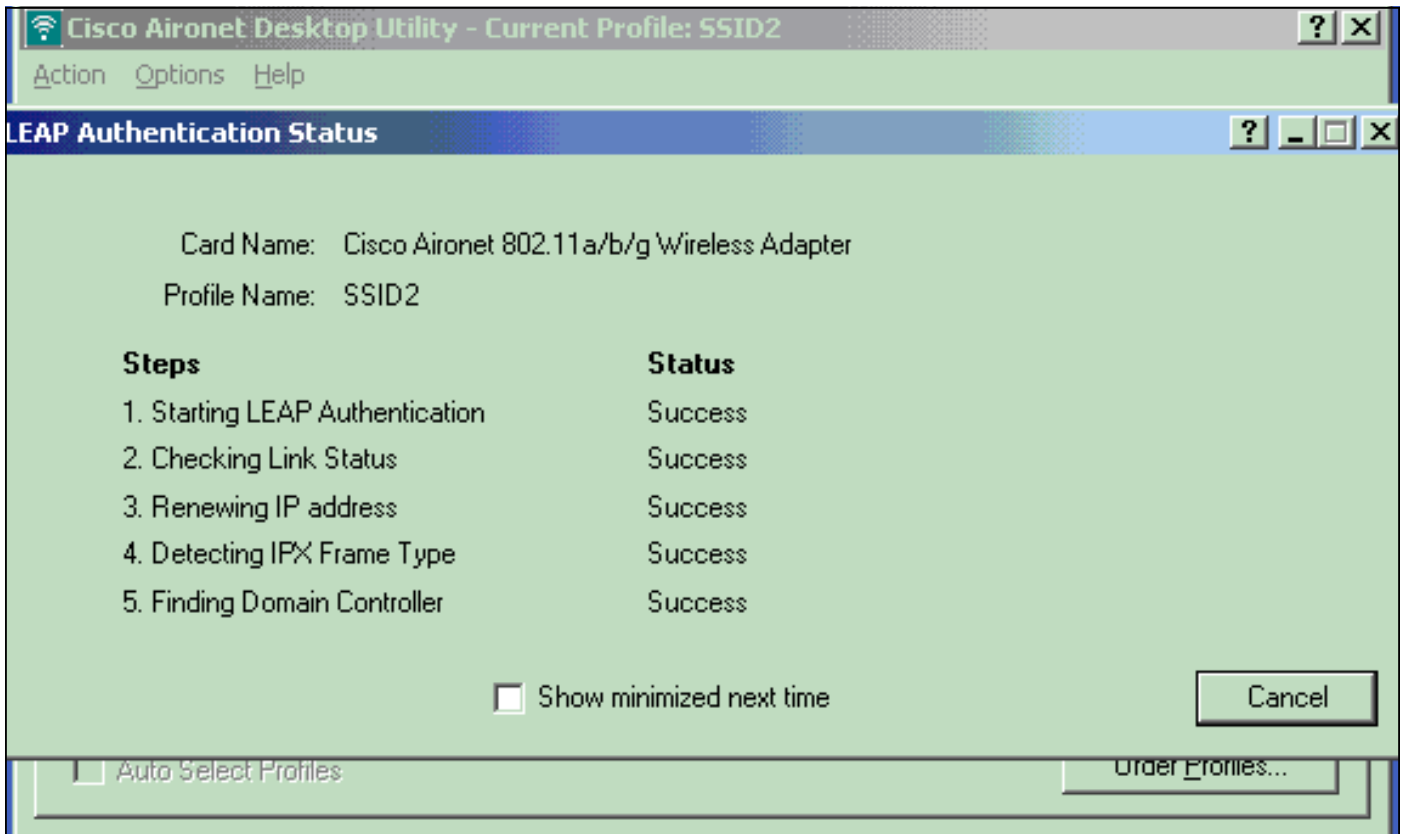
注意：TKIP是与WPA-PSK一起使用的加密。



由于WLAN 2使用EAP身份验证，因此与WLAN 2连接的客户端会断开连接。发生此断开是因为使用EAP身份验证的客户端需要与WLC通信。以下是一个示例窗口，显示WAN链路关闭时EAP身份验证失败：



在WAN链路启动后，AP会切换回正常LEAP模式并向控制器注册。使用EAP身份验证的客户端也会启动。示例如下：



控制器上debug lwapp events enable命令的此示例输出显示以下结果：

```
(Cisco Controller) >debug lwapp events enable
Wed May 17 15:06:40 2006: Successful transmission of LWAPP Discovery-Response
to AP 00:0b:85:51:5a:e0 on Port 1
Wed May 17 15:06:52 2006: Received LWAPP JOIN REQUEST from AP 00:0b:85:51:5a:e0to
00:0b:85:33:84:a0 on port '1'
Wed May 17 15:06:52 2006: LWAPP Join-Request MTU path from AP 00:0b:85:51:5a:e0is 1500,
remote debug mode is 0
Wed May 17 15:06:52 2006: Successfully added NPU Entry for AP 00:0b:85:51:5a:e0(index 51)
```


Switch IP: 172.16.1.51, Switch Port: 12223, intIfNum 1, vlanId 0AP IP: 192.168.1.5, AP Port: 5550, next hop MAC: 00:d0:58:ad:ae:cb
Wed May 17 15:06:52 2006: **Successfully transmission of LWAPP Join-Reply to AP 00:0b:85:51:5a:e0**
Wed May 17 15:06:52 2006: **Register LWAPP event for AP 00:0b:85:51:5a:e0 slot 0**
Wed May 17 15:06:52 2006: Register LWAPP event for AP 00:0b:85:51:5a:e0 slot 1
Wed May 17 15:06:54 2006: Received LWAPP CONFIGURE REQUEST from AP 00:0b:85:51:5a:e0 to 00:0b:85:33:84:a0
Wed May 17 15:06:54 2006: Updating IP info for AP 00:0b:85:51:5a:e0 -- static 1, 192.168.1.5/255.255.255.0, gtw 192.168.1.1

故障排除

使用本部分可排除配置故障。

故障排除命令

您可以使用这些debug命令对配置进行故障排除。

注意：在使用debug命令之前，请参阅有关Debug命令的重要信息。

- `debug lwapp events enable` — 显示LAP和WLC之间发生的事件顺序。
- `debug lwapp errors enable` — 显示LWAPP通信中出现的错误。
- `debug lwapp packet enable` — 显示LWAPP数据包跟踪的调试。
- `debug mac addr` — 为指定的客户端启用MAC调试。

相关信息

- [分支机构REAP部署指南](#)
- [WLAN 控制器 \(WLC\) 中 EAP 身份验证的配置示例](#)
- [无线 LAN 控制器和轻量接入点基本配置示例](#)
- [对轻量接入点进行 WLAN 控制器故障切换配置示例](#)
- [无线支持页](#)
- [技术支持和文档 - Cisco Systems](#)