

Remote-Edge AP (REAP) mit einfachen APs und WLCs (Wireless LAN Controller) - Konfigurationsbeispiel

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konventionen](#)

[Hintergrundinformationen](#)

[Konfigurieren](#)

[Netzwerkdiagramm](#)

[WLC für den Basisbetrieb konfigurieren und WLANs konfigurieren](#)

[Prime den Access Point für die Installation an einem Remote-Standort](#)

[Konfigurieren der 2800-Router zum Herstellen der WAN-Verbindung](#)

[Bereitstellen des REAP am Remote-Standort](#)

[Überprüfen](#)

[Fehlerbehebung](#)

[Befehle zur Fehlerbehebung](#)

[Zugehörige Informationen](#)

Einführung

REAP-Funktionen (Remote Edge Access Point), die mit dem Cisco Unified Wireless Network eingeführt wurden, ermöglichen die Remote-Bereitstellung der Cisco Lightweight Access Points (LAPs) vom WLAN-Controller (WLC) aus. Damit sind sie ideal für Zweigstellen- und kleine Einzelhandelsstandorte geeignet. In diesem Dokument wird die Bereitstellung eines REAP-basierten WLAN-Netzwerks mithilfe der Cisco LAPs der Serie 1030 und 4400 WLCs erläutert.

Voraussetzungen

Anforderungen

Stellen Sie sicher, dass Sie diese Anforderungen erfüllen, bevor Sie versuchen, diese Konfiguration durchzuführen:

- Kenntnis der WLCs und Konfiguration der WLC-Basisparameter
- Kenntnis des REAP-Betriebsmodus in einer Cisco 1030 LAP
- Kenntnis der Konfiguration eines externen DHCP-Servers und/oder DNS-Servers (Domain

Name System)

- Kenntnisse über Wi-Fi Protected Access (WPA)-Konzepte

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco WLC der Serie 4400 mit Firmware-Version 4.2
- Cisco LAP 1030
- Zwei Cisco Router der Serie 2800 mit Cisco IOS® Software Release 12.2(13)T13
- Cisco Aironet 802.11a/b/g Client-Adapter mit Firmware-Version 3.0
- Cisco Aironet Desktop Utility Version 3.0

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter [Cisco Technical Tips Conventions](#) (Technische Tipps zu Konventionen von Cisco).

Hintergrundinformationen

Der REAP-Modus ermöglicht es einer LAP, sich über eine WAN-Verbindung aufzuhalten, mit dem WLC zu kommunizieren und die Funktionalität einer regulären LAP bereitzustellen. Der REAP-Modus wird derzeit nur auf den 1030 LAPs unterstützt.

Um diese Funktionalität bereitzustellen, trennt der REAP 1030 die LWAPP-Kontrollebene (Lightweight Access Point Protocol) von der Wireless-Datenebene. Cisco WLCs werden weiterhin für die zentrale Steuerung und Verwaltung verwendet, und zwar in der gleichen Weise wie reguläre LWAPP-basierte Access Points (APs), während alle Benutzerdaten lokal am Access Point überbrückt werden. Der Zugriff auf lokale Netzwerkressourcen wird bei WAN-Ausfällen aufrechterhalten.

REAPs unterstützen zwei Betriebsmodi:

- Normaler REAP-Modus
- Standalone-Modus

Die LAP wird im normalen REAP-Modus eingerichtet, wenn die WAN-Verbindung zwischen dem REAP und dem WLC aktiv ist. Wenn LAPs im normalen REAP-Modus arbeiten, können sie bis zu 16 WLANs unterstützen.

Wenn die WAN-Verbindung zwischen dem WLC und der LAP ausfällt, wechselt die REAP-fähige LAP in den Standalone-Modus. Im Standalone-Modus können die REAP-LAPs nur ein WLAN unabhängig und ohne WLC unterstützen, wenn das WLAN entweder mit Wired Equivalent Privacy (WEP) oder einer anderen lokalen Authentifizierungsmethode konfiguriert ist. In diesem Fall ist das vom REAP unterstützte WLAN das erste WLAN, das auf dem WAP konfiguriert ist, WLAN 1. Dies liegt daran, dass die meisten anderen Authentifizierungsmethoden Informationen an den

Controller und von diesem weitergeben müssen. Wenn die WAN-Verbindung ausfällt, ist dieser Vorgang nicht möglich. Im Standalone-Modus unterstützen die LAPs eine minimale Anzahl von Funktionen. In dieser Tabelle sind die Funktionen aufgeführt, die eine REAP LAP im Standalone-Modus unterstützt, im Vergleich zu den Funktionen, die eine REAP LAP im normalen Modus unterstützt (wenn die WAN-Verbindung aktiv ist und die Kommunikation mit dem WLC aktiv ist):

Funktionen, die eine REAP-LAP im normalen REAP-Modus und im Standalone-Modus unterstützt

		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

Die Tabelle zeigt, dass mehrere VLANs in beiden Modi auf REAP LAPs nicht unterstützt werden. Mehrere VLANs werden nicht unterstützt, da REAP-LAPs nur in einem Subnetz untergebracht werden können, da sie kein IEEE 802.1Q VLAN-Tagging durchführen können. Aus diesem Grund wird der Datenverkehr an jedem der Service Set Identifiers (SSIDs) im gleichen Subnetz wie das

kabelgebundene Netzwerk terminiert. Daher wird der Datenverkehr nicht auf der kabelgebundenen Seite getrennt, obwohl der Wireless-Datenverkehr zwischen den SSIDs über die Luft segmentiert werden kann.

Weitere Informationen zur [REAP-Bereitstellung](#) und zur Verwaltung von REAP und seinen Einschränkungen finden Sie im [REAP-Bereitstellungsleitfaden für Zweigstellen](#).

Konfigurieren

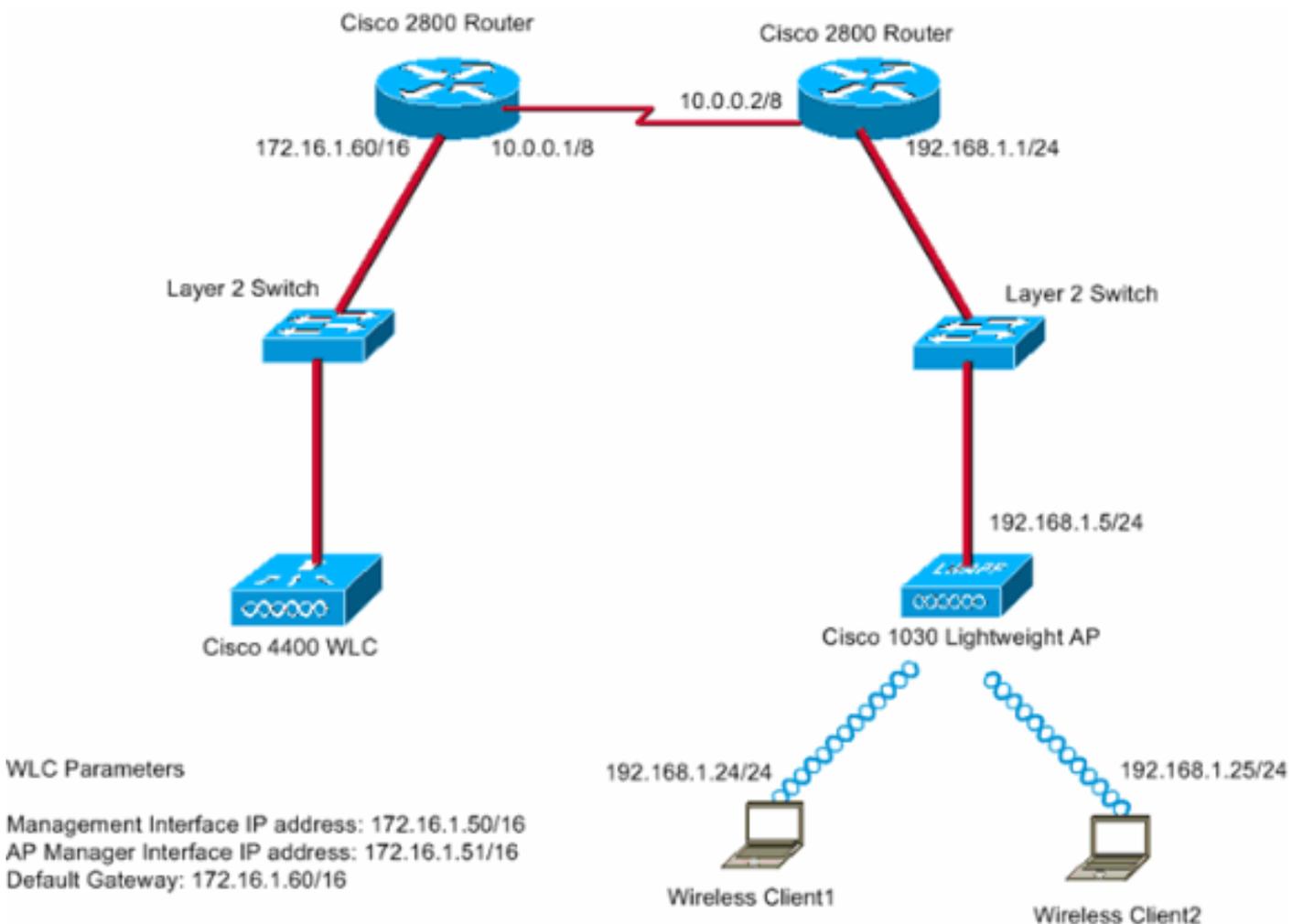
In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

Gehen Sie wie folgt vor, um die Geräte für die Implementierung der Netzwerkeinrichtung zu konfigurieren:

1. [Konfigurieren Sie den WLC für den Basisbetrieb, und konfigurieren Sie WLANs.](#)
2. [Prime den Access Point für die Installation am Remote-Standort.](#)
3. [Konfigurieren Sie die 2800-Router, um die WAN-Verbindung herzustellen.](#)
4. [Bereitstellen der REAP-LAP am Remote-Standort.](#)

Netzwerkdigramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



Die Hauptniederlassung ist über eine Mietleitung mit der Außenstelle verbunden. Die Mietleitung endet an beiden Enden mit Routern der Serie 2800. In diesem Beispiel wird das Open Shortest Path First (OSPF)-Protokoll verwendet, um Daten auf der WAN-Verbindung mit der PPP-Kapselung weiterzuleiten. Der 4400-WLC befindet sich in der Hauptniederlassung, und die 1030-LAP muss in der Außenstelle bereitgestellt werden. Die LAP 1030 muss zwei WLANs unterstützen. Die Parameter für die WLANs sind wie folgt:

- **WLAN 1**SSID - SSID1Authentifizierung - **Öffnen**Verschlüsselung - **Temporal Key Integrity Protocol (TKIP) (WPA Pre-Shared Key [WPA-PSK])**
- **WLAN 2**SSID - SSID2Authentifizierung - **Extensible Authentication Protocol (EAP)**Verschlüsselung - **TKIPHinweis:** Für WLAN 2 wird für die Konfiguration in diesem Dokument WPA (802.1x-Authentifizierung und TKIP für Verschlüsselung) verwendet.

Sie müssen die Geräte für diese Konfiguration konfigurieren.

[WLC für den Basisbetrieb konfigurieren und WLANs konfigurieren](#)

Sie können den Startup Configuration Wizard (Start-Konfigurationsassistent) in der Befehlszeilenschnittstelle (CLI) verwenden, um den WLC für den Basisbetrieb zu konfigurieren. Alternativ können Sie auch die Benutzeroberfläche verwenden, um den WLC zu konfigurieren. In diesem Dokument wird die Konfiguration auf dem WLC mithilfe des Startup Configuration Wizard (Start-Konfigurationsassistent) in der CLI erläutert.

Nachdem der WLC zum ersten Mal gestartet wurde, wird er direkt in den Startup Configuration Wizard (Startup-Konfigurationsassistent) eingegeben. Mit dem Konfigurationsassistenten können Sie die Grundeinstellungen konfigurieren. Sie können den Assistenten über die Kommandozeile oder die Benutzeroberfläche ausführen. Im Folgenden finden Sie ein Beispiel für den Assistenten zur Startkonfiguration:

```
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!

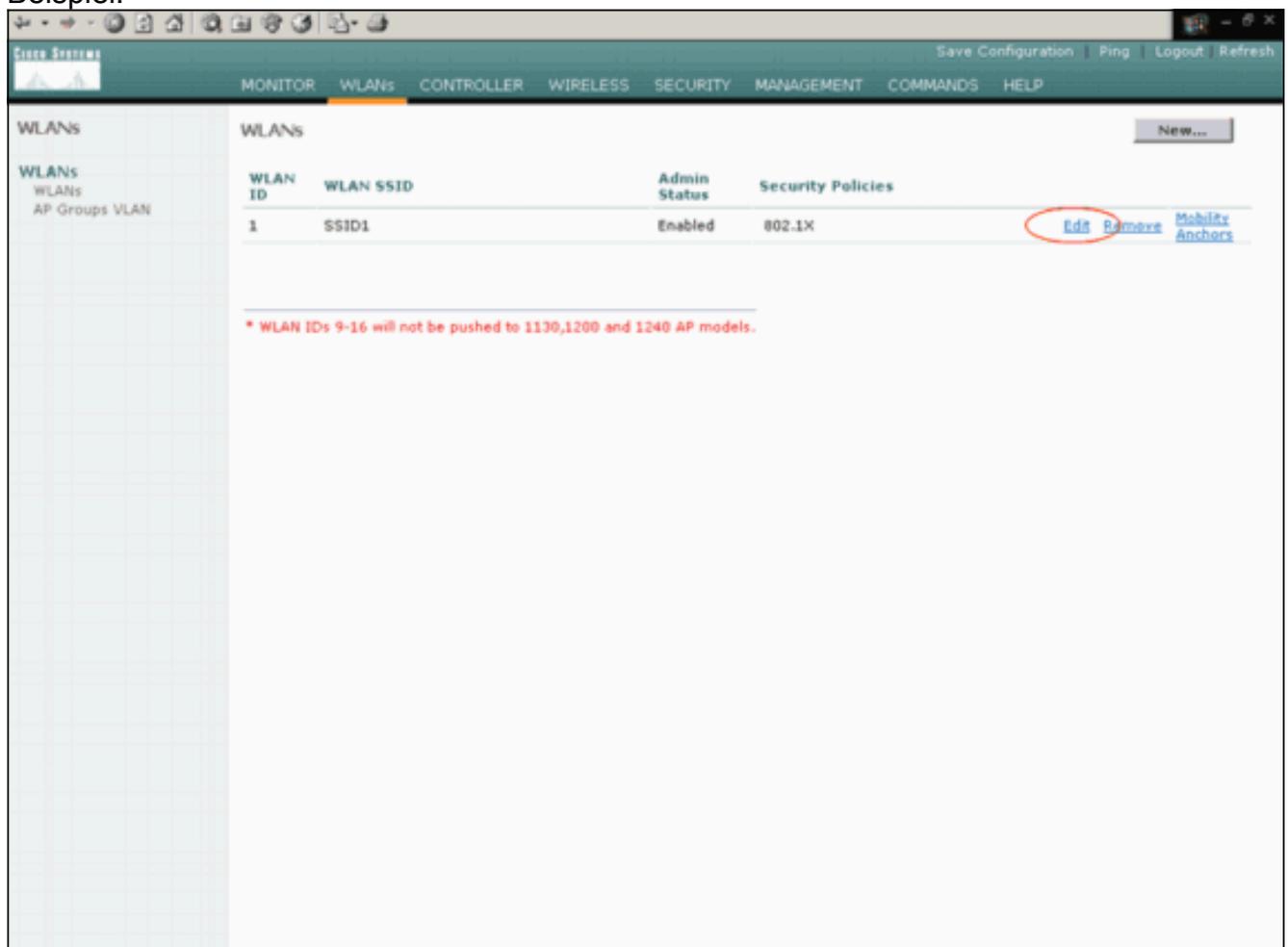
Resetting system with new configuration...

In diesem Beispiel werden diese Parameter auf dem WLC konfiguriert:

- Systemname
- IP-Adresse der Verwaltungsschnittstelle
- IP-Adresse der AP-Manager-Schnittstelle
- Port-Nummer der Management-Schnittstelle
- VLAN-ID der Verwaltungsschnittstelle
- Name der Mobilitätsgruppe
- SSID
- Viele andere Parameter

Diese Parameter werden verwendet, um den WLC für den Basisbetrieb einzurichten. Wie die WLC-Ausgabe in diesem Abschnitt zeigt, verwendet der WLC die IP-Adresse der Verwaltungsschnittstelle 172.16.1.50 und die IP-Adresse 172.16.1.51 als IP-Adresse der AP-Manager-Schnittstelle. Führen Sie die folgenden Schritte im WLC aus, um die beiden WLANs für Ihr Netzwerk zu konfigurieren:

1. Klicken Sie in der WLC-GUI im Menü am oberen Fensterrand auf **WLANs**. Das Fenster WLANs wird angezeigt. In diesem Fenster werden die WLANs aufgelistet, die auf dem WLC konfiguriert sind. Da Sie ein WLAN mithilfe des Assistenten für die Startkonfiguration konfiguriert haben, müssen Sie die anderen Parameter für dieses WLAN konfigurieren.
2. Klicken Sie für die WLAN-SSID1 auf **Bearbeiten**. Hier ein Beispiel:

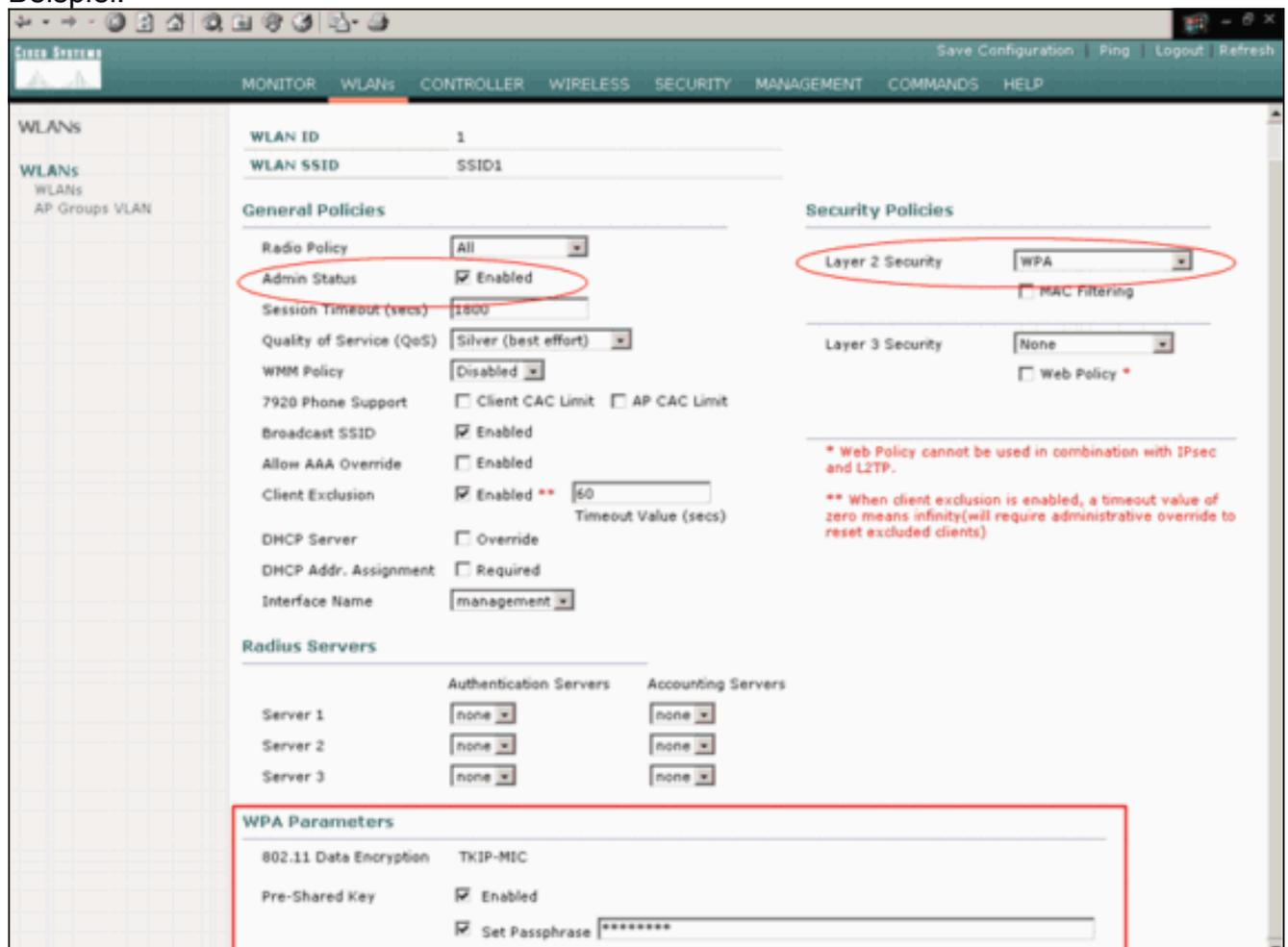


Das Fenster WLANs > Edit (WLANs > Bearbeiten) wird angezeigt. In diesem Fenster können

Sie die für das WLAN spezifischen Parameter konfigurieren, z. B. allgemeine Richtlinien, Sicherheitsrichtlinien, RADIUS-Server usw.

3. Wählen Sie diese Optionen im Fenster WLANs > Edit (WLANs > Bearbeiten) aus: Aktivieren Sie im Bereich Allgemeine Richtlinien das Kontrollkästchen **Aktiviert** neben Admin Status, um dieses WLAN zu aktivieren. Wählen Sie **WPA** aus dem Dropdown-Menü "Layer 2 Security" aus, um WPA für WLAN 1 zu verwenden. Definieren Sie die WPA-Parameter am unteren Rand des Fensters. Um WPA-PSK in WLAN 1 zu verwenden, aktivieren Sie im Bereich WPA-Parameter das Kontrollkästchen **Aktiviert** neben Pre-Shared Key (Vorinstallierter Schlüssel), und geben Sie die Passphrase für WPA-PSK ein. WPA-PSK verwendet TKIP für die Verschlüsselung. **Hinweis:** Die WPA-PSK-Passphrase muss mit der auf dem Client-Adapter konfigurierten Passphrase übereinstimmen, damit WPA-PSK funktioniert. Klicken Sie auf **Übernehmen**. Hier ein

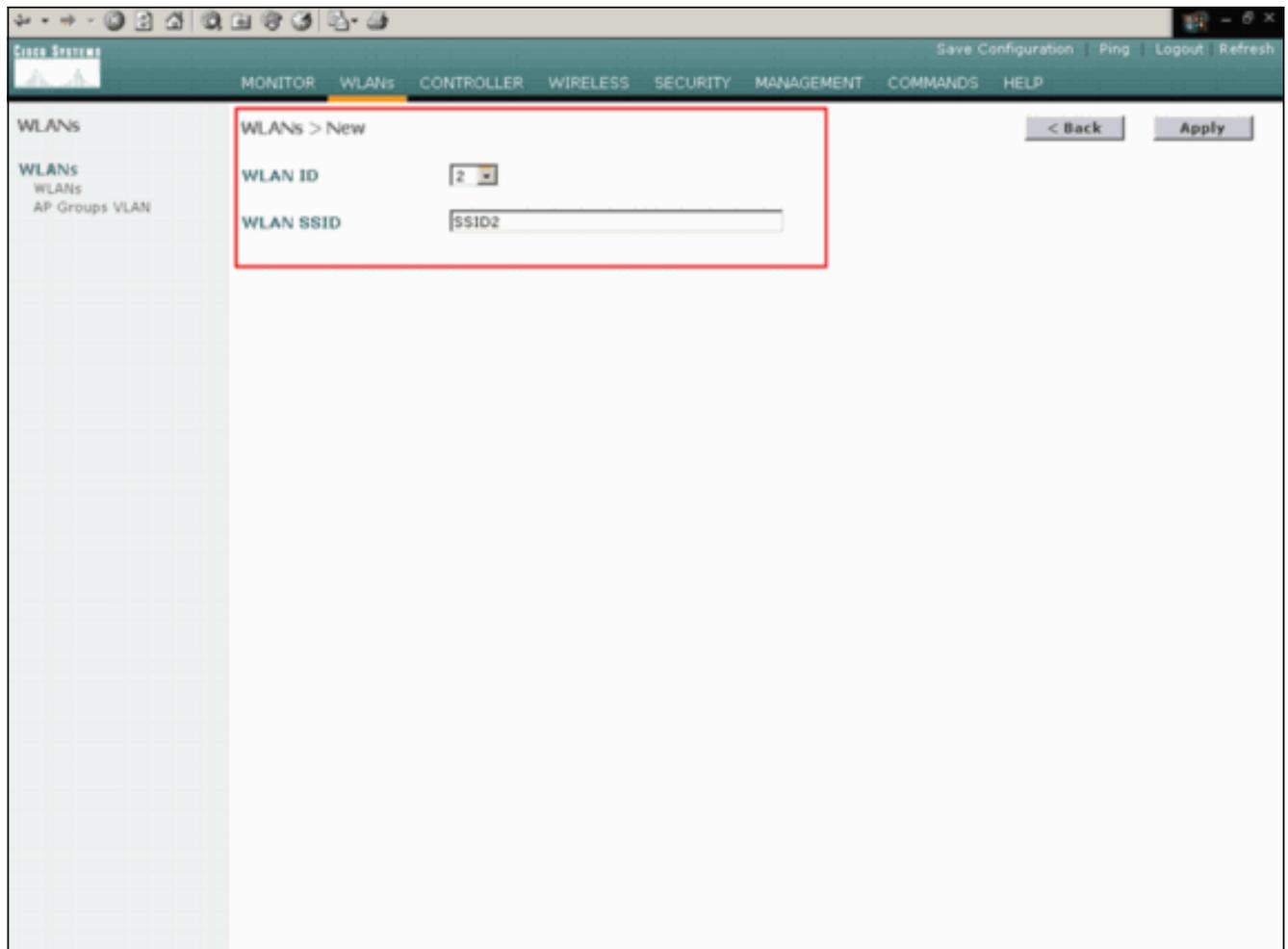
Beispiel:



Sie haben WLAN 1 für die WPA-PSK-Verschlüsselung konfiguriert.

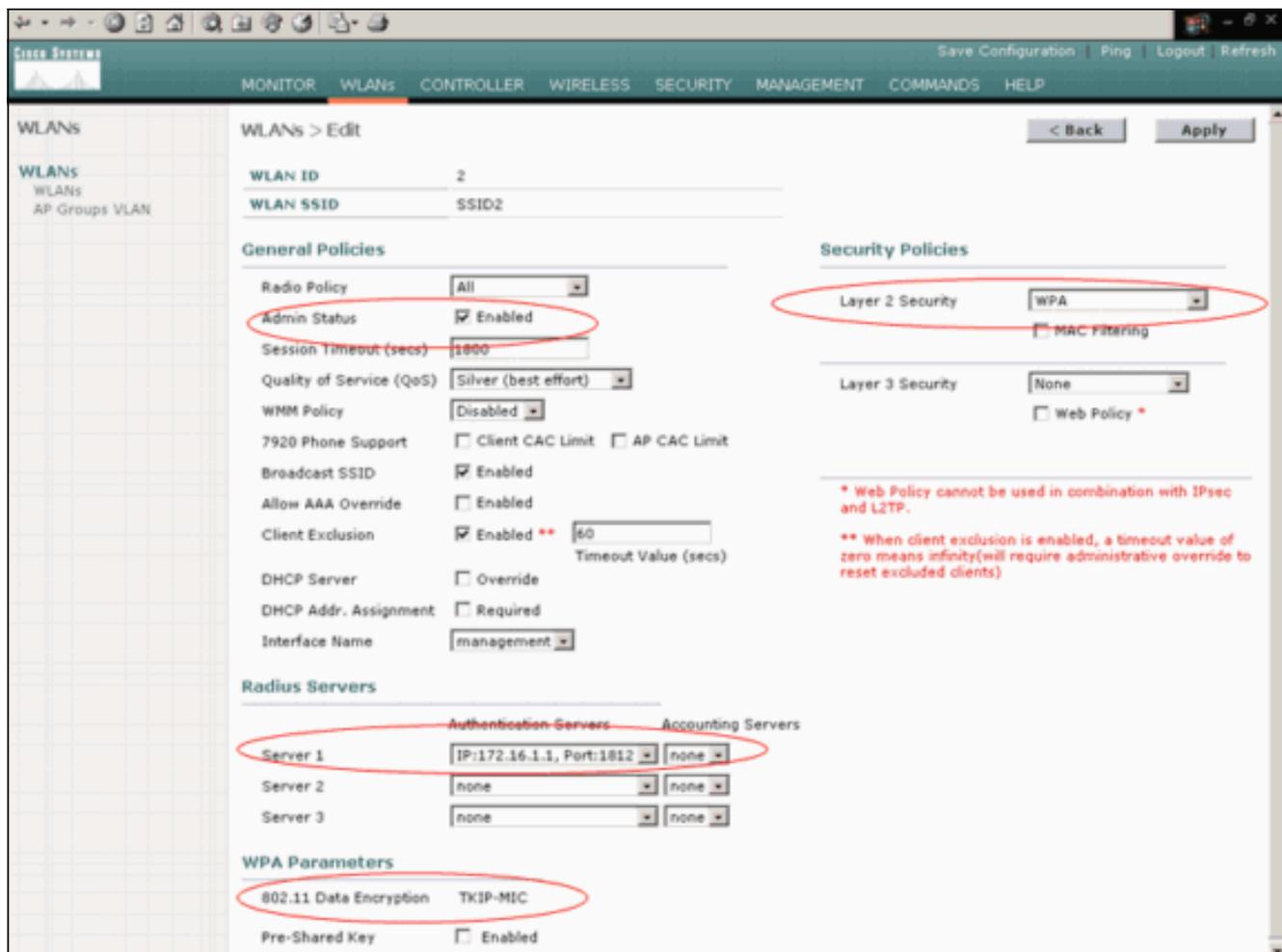
4. Um WLAN 2 zu definieren, klicken Sie im Fenster WLANs auf **Neu**. Das Fenster WLAN > New (WLAN > Neu) wird angezeigt.
5. Definieren Sie im Fenster WLAN > New die WLAN-ID und die WLAN-SSID, und klicken Sie auf **Apply**. Hier ein

Beispiel:



Das Fenster WLAN > Edit (WLAN > Bearbeiten) für das zweite WLAN wird angezeigt.

6. Wählen Sie diese Optionen im Fenster WLANs > Edit (WLANs > Bearbeiten) aus: Aktivieren Sie im Bereich Allgemeine Richtlinien das Kontrollkästchen **Aktiviert** neben Admin Status, um dieses WLAN zu aktivieren. Wählen Sie **WPA** im Dropdown-Menü "Layer 2 Security" (Sicherheit) aus, um WPA für dieses WLAN zu konfigurieren. Wählen Sie im Bereich Radius-Server den geeigneten RADIUS-Server für die Authentifizierung der Clients aus. Klicken Sie auf **Übernehmen**. Hier ein Beispiel:



Hinweis: In diesem Dokument wird nicht erläutert, wie die RADIUS-Server und die EAP-Authentifizierung konfiguriert werden. Weitere Informationen zum Konfigurieren der EAP-Authentifizierung mit WLCs finden Sie im [Konfigurationsbeispiel für die EAP-Authentifizierung mit WLAN-Controllern \(WLC\)](#).

[Prime den Access Point für die Installation an einem Remote-Standort](#)

Beim Priming erhalten LAPs eine Liste von Controllern, mit denen sie eine Verbindung herstellen können. LAPs werden über alle Controller in der Mobilitätsgruppe informiert, sobald sie eine Verbindung zu einem einzelnen Controller herstellen. Auf diese Weise erhalten die LAPs alle Informationen, die sie benötigen, um einem Controller in der Gruppe beizutreten.

Um einen REAP-fähigen Access Point zu bedienen, verbinden Sie den Access Point mit dem kabelgebundenen Netzwerk in der Hauptniederlassung. Durch diese Verbindung kann der Access Point einen einzelnen Controller erkennen. Nachdem die LAP dem Controller in der Hauptniederlassung beitritt, lädt der Access Point die Version des AP-Betriebssystems herunter, die der WLAN-Infrastruktur und der Konfiguration entspricht. Die IP-Adressen aller Controller in der Mobilitätsgruppe werden an den AP übertragen. Wenn der Access Point über alle erforderlichen Informationen verfügt, kann der Access Point am Remote-Standort angeschlossen werden. Der Access Point kann dann den am wenigsten genutzten Controller aus der Liste erkennen und ihm beitreten, wenn eine IP-Verbindung verfügbar ist.

Hinweis: Stellen Sie sicher, dass Sie die Access Points auf den REAP-Modus setzen, bevor Sie sie ausschalten, um sie an die Remote-Standorte zu senden. Sie können den Modus auf AP-Ebene über die CLI oder GUI des Controllers oder mithilfe von WCS-Vorlagen (Wireless Control System) festlegen. Die APs sind standardmäßig so konfiguriert, dass sie standardmäßig "lokale" Funktionen ausführen.

Die LAPs können eine der folgenden Methoden verwenden, um den Controller zu erkennen:

- **Layer-2-Erkennung**
- **Layer-3-Erkennung** Bei Verwendung einer lokalen Subnetz-Broadcast Bei Verwendung der DHCP-Option 43 Bei Verwendung eines DNS-Servers Mit OTAP (Over-the-Air Provisioning) Bei Verwendung eines internen DHCP-Servers **Hinweis:** Um einen internen DHCP-Server zu verwenden, muss die LAP eine direkte Verbindung zum WLC herstellen.

In diesem Dokument wird davon ausgegangen, dass sich die LAP mithilfe des Erkennungsmechanismus der DHCP-Option 43 beim WLC registriert. Weitere Informationen zur Verwendung der DHCP-Option 43 zur Registrierung der LAP beim Controller sowie der anderen Erkennungsmechanismen finden Sie unter [LAP-Registrierung bei einem Wireless LAN Controller \(WLC\)](#).

Nachdem die LAP den Controller erkannt hat, sehen Sie, dass der Access Point im Wireless-Fenster des WLC am Controller registriert ist. Hier ein Beispiel:

The screenshot shows the Cisco WLC GUI with the 'Wireless' tab selected. The 'All APs' page is displayed, showing a table of registered APs. The first row is highlighted with a red oval.

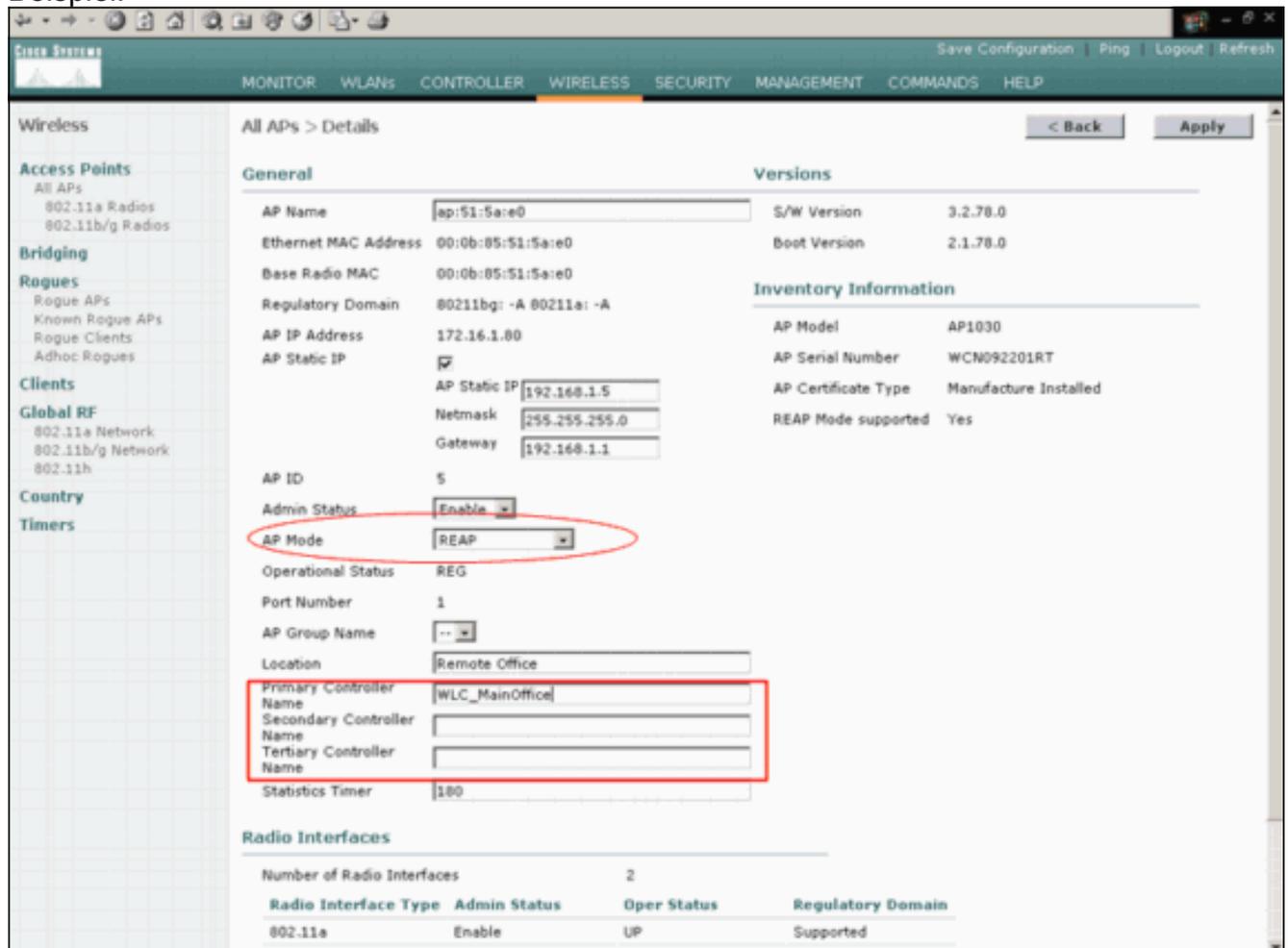
AP Name	AP ID	Ethernet MAC	Admin Status	Operational Status	Port	
ap:51:5ae0	5	00-0b:05-51:5ae0	Enable	REG	1	Detail

Gehen Sie wie folgt vor, um die LAP für den normalen REAP-Modus zu konfigurieren:

1. Klicken Sie in der WLC-GUI auf **Wireless**. Das Fenster Alle APs wird angezeigt. In diesem Fenster werden die APs aufgelistet, die für den WLC registriert sind.
2. Wählen Sie den AP aus, den Sie für den REAP-Modus konfigurieren müssen, und klicken Sie auf **Detail**. Das Fenster Alle APs > Detail (Alle APs > Details) für den jeweiligen Access Point wird angezeigt. In diesem Fenster können Sie die verschiedenen Parameter des Access Points konfigurieren, z. B.: AP-Name IP-Adresse (die Sie in statisch ändern

können) Admin-Status Sicherheitsparameter AP-Modus Liste der WLCs, mit denen der AP verbunden werden kann Andere Parameter

3. Wählen Sie **REAP** aus dem Dropdown-Menü "AP Mode" aus. Dieser Modus ist nur auf REAP-fähigen APs verfügbar.
4. Definieren Sie die Controller-Namen, die die Access Points zur Registrierung verwenden, und klicken Sie auf **Apply**. Sie können bis zu drei Controller-Namen definieren (primär, sekundär und tertiär). Die APs suchen den Controller in der gleichen Reihenfolge wie in diesem Fenster. Da in diesem Beispiel nur ein Controller verwendet wird, wird im Beispiel der Controller als primärer Controller definiert. Hier ein Beispiel:



Sie haben den Access Point für den REAP-Modus eingerichtet und können ihn am Remote-Standort bereitstellen.

Hinweis: In diesem Beispielfenster können Sie sehen, dass die IP-Adresse des Access Points in static geändert und eine statische IP-Adresse 192.168.1.5 zugewiesen wird. Diese Zuweisung erfolgt, da es sich um das Subnetz handelt, das in der Außenstelle verwendet wird. Sie verwenden also die IP-Adresse des DHCP-Servers 172.16.1.80, nur während der Priorisierungsphase. Nachdem der Access Point am Controller registriert wurde, ändern Sie die Adresse in eine statische IP-Adresse.

[Konfigurieren der 2800-Router zum Herstellen der WAN-Verbindung](#)

Zur Einrichtung der WAN-Verbindung werden in diesem Beispiel zwei Router der Serie 2800 mit OSPF verwendet, um Informationen zwischen den Netzwerken weiterzuleiten. Im Folgenden finden Sie die Konfiguration der beiden Router für das Beispielszenario in diesem Dokument:

Hauptniederlassung

```
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
```

Zweigstelle

```
BranchOffice#show run
Building configuration...

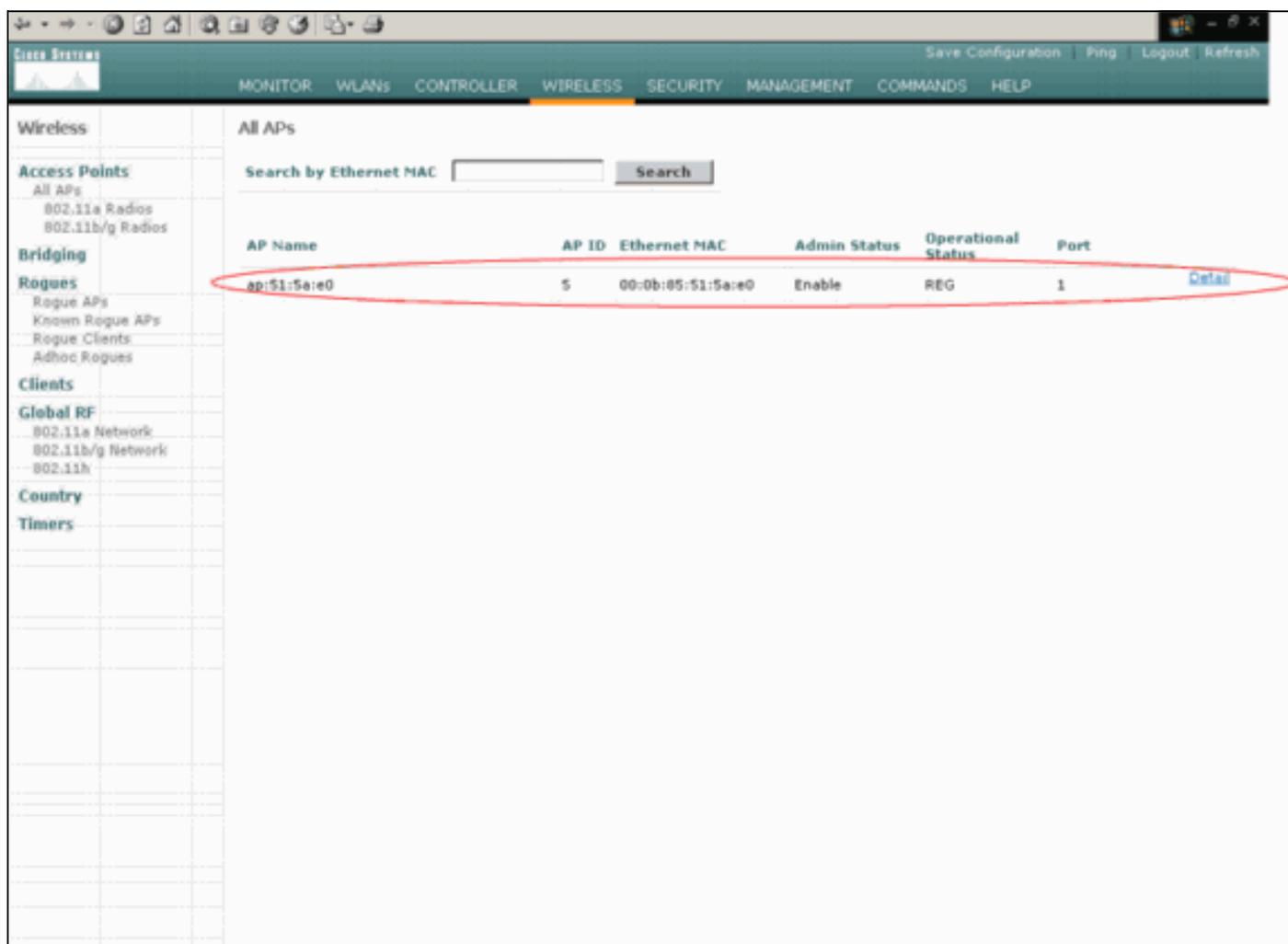
Current configuration : 596 bytes
!
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname BranchOffice
!
!
ip subnet-zero
!
!
!
interface Ethernet0
 ip address 192.168.1.1 255.255.255.0
 !--- This is the interface which acts 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
```

Bereitstellen des REAP am Remote-Standort

Nachdem Sie WLANs auf den WLCs konfiguriert, die LAP aktiviert und die WAN-Verbindung zwischen der Hauptniederlassung und der Außenstelle eingerichtet haben, können Sie den Access Point am Remote-Standort bereitstellen.

Nachdem Sie den Access Point am Remote-Standort hochgefahren haben, sucht der Access Point nach dem Controller in der Reihenfolge, in der Sie den Access Point im Rahmen des Startvorgangs konfiguriert haben. Nachdem der Access Point den Controller gefunden hat, wird der Access Point beim Controller registriert. Hier ein Beispiel. Aus dem WLC können Sie sehen, dass der Access Point dem Controller an Port 1 angeschlossen ist:



AP Name	AP ID	Ethernet MAC	Admin Status	Operational Status	Port
ap:51:5a:e0	5	00-0b:85-51:5a:e0	Enable	REG	1

Clients, die über die SSID **SSID1** verfügen und für die WPA-PSK aktiviert ist, stellen eine Verbindung zum WLAN 1 her. Clients mit SSID **SSID2**, die über eine 802.1x-Authentifizierung verfügen, stellen eine Verbindung zum WLAN 2 her. Im folgenden Beispiel werden zwei Clients angezeigt. Ein Client ist mit WLAN 1 verbunden, der andere mit WLAN 2:

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

Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre REAP-Konfiguration ordnungsgemäß funktioniert.

Hinweis: Beachten Sie [vor der](#) Verwendung von **Debug**-Befehlen die [Informationen](#) zu [Debug-Befehlen](#).

Deaktivieren Sie die WAN-Verbindung. Wenn die WAN-Verbindung ausfällt, verliert der WAP die Verbindung zum WLC. Der WLC löscht dann die Registrierung des Access Points aus seiner Liste. Hier ein Beispiel:

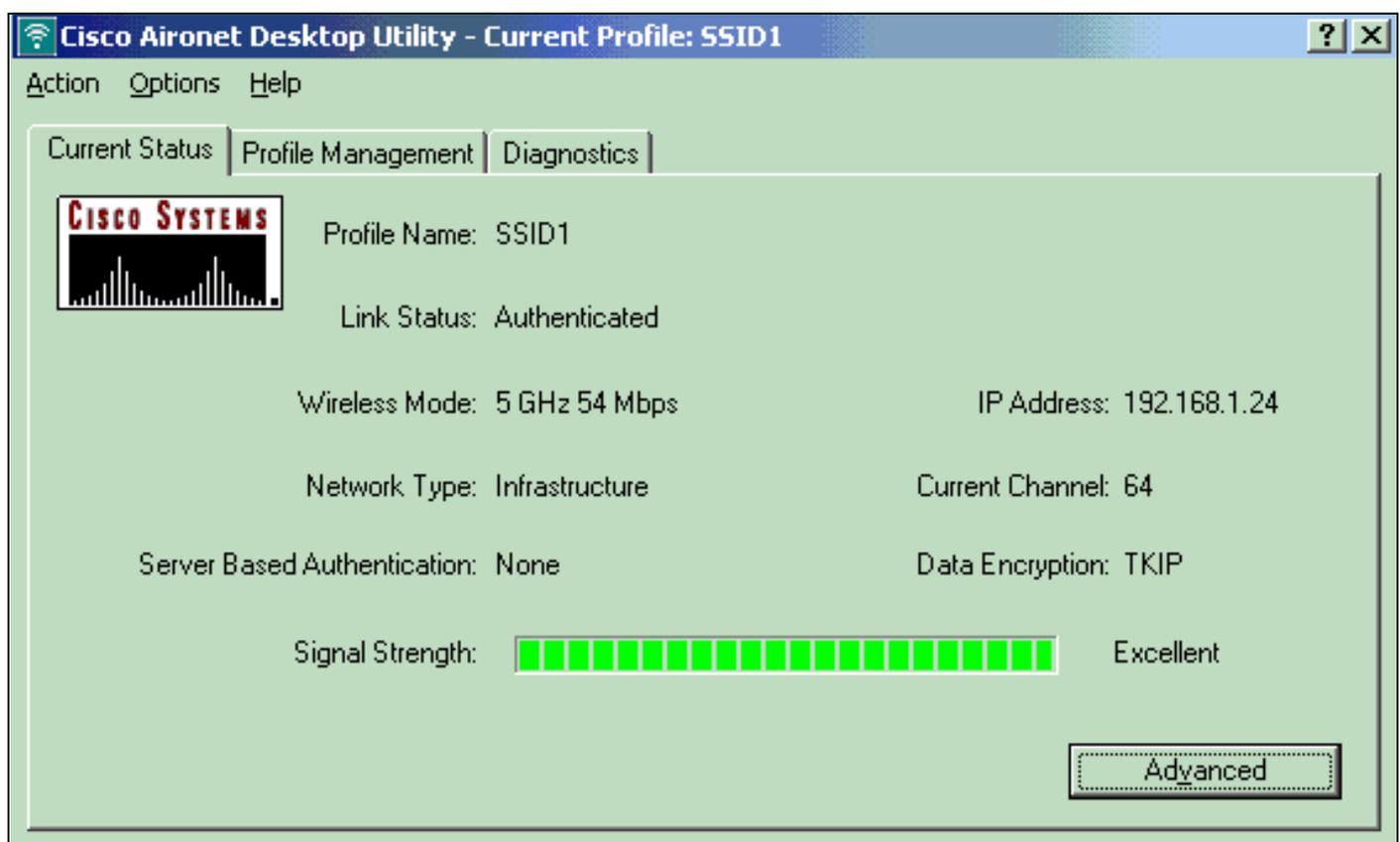
```
(Cisco Controller) >debug lwapp events enable
Wed May 17 15:04:22 2006: Did not receive heartbeat reply from AP 00:0B:85:51:5A:E0
Wed May 17 15:04:22 2006: Max retransmissions reached on AP 00:0B:85:51:5A:E0
(CONFIGURE_COMMAND, 1)
Wed May 17 15:04:22 2006: apfSpamProcessStateChangeInSpamContext: 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

Aus den **debug lwapp-Ereignissen, die die Befehlsausgabe aktivieren**, können Sie sehen, dass der WLC die Registrierung des Access Points aufhebt, da der WLC keine Heartbeat-Antwort vom Access Point erhalten hat. Eine Heartbeat-Antwort ähnelt Keepalive-Nachrichten. Der Controller versucht fünf aufeinander folgende Heartbeats, einen Abstand von einer Sekunde. Wenn der WLC keine Antwort erhält, wird der Access Point vom WLC freigegeben.

Wenn sich der Access Point im Standalone-Modus befindet, blinkt die LED-Betriebsanzeige des Access Points. Die Clients, die mit dem ersten WLAN (WLAN 1) verbunden sind, sind weiterhin dem WAP zugeordnet, da die Clients im ersten WLAN nur für die WPA-PSK-Verschlüsselung konfiguriert sind. Die LAP verarbeitet die Verschlüsselung selbst im Standalone-Modus. Das folgende Beispiel zeigt den Status (wenn die WAN-Verbindung unterbrochen ist) eines Clients, der mit WLAN 1 mit SSID1 und WPA-PSK verbunden ist:

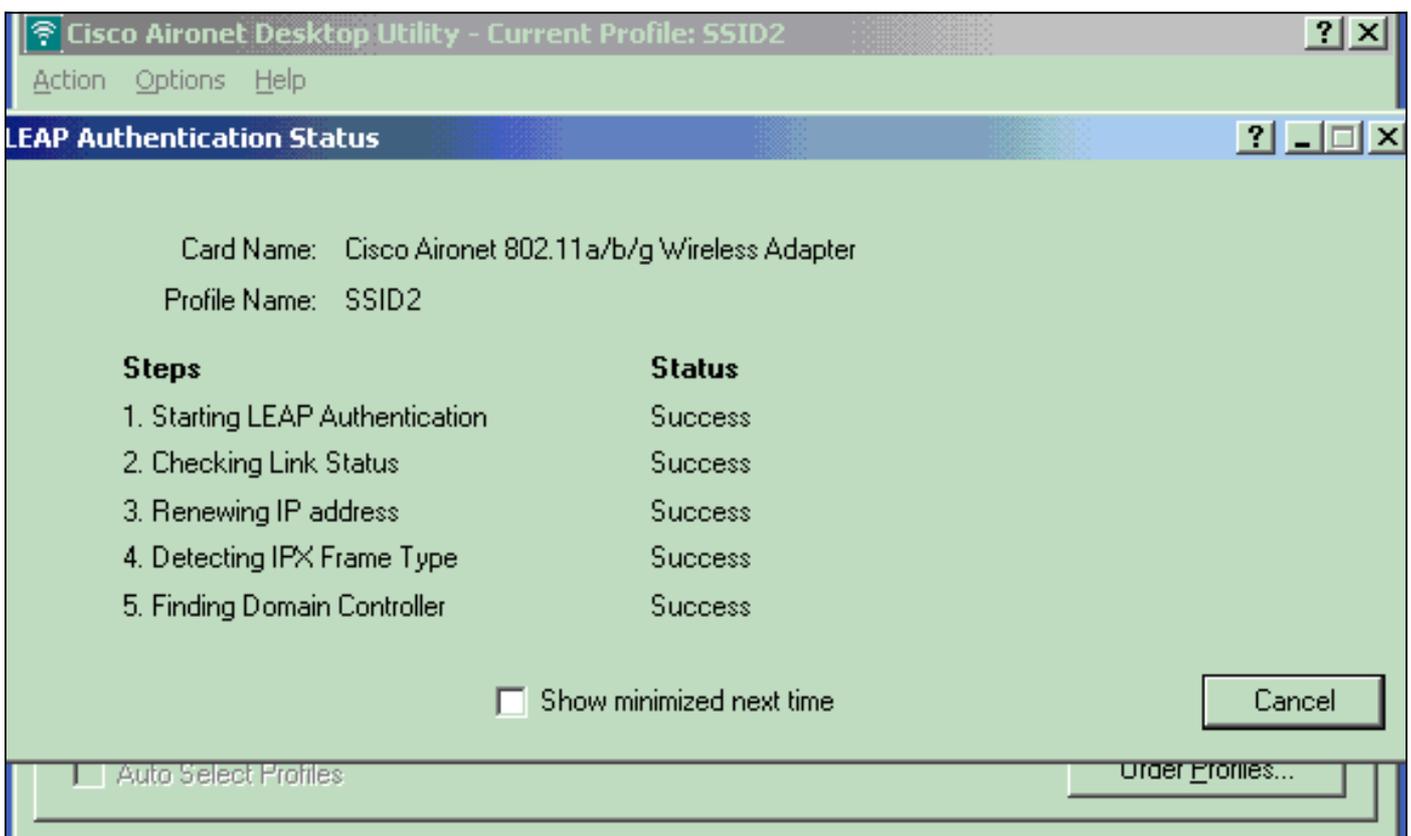
Hinweis: TKIP ist die Verschlüsselung, die mit WPA-PSK verwendet wird.



Die Clients, die mit WLAN 2 verbunden sind, sind getrennt, da WLAN 2 die EAP-Authentifizierung verwendet. Diese Trennung erfolgt, weil Clients, die EAP-Authentifizierung verwenden, mit dem WLC kommunizieren müssen. Das folgende Beispiel zeigt, dass die EAP-Authentifizierung fehlschlägt, wenn die WAN-Verbindung unterbrochen ist:



Wenn die WAN-Verbindung aktiv ist, schaltet der Access Point zurück in den normalen REAP-Modus und registriert sich beim Controller. Der Client, der die EAP-Authentifizierung verwendet, wird ebenfalls angezeigt. Hier ein Beispiel:



Diese Beispielausgabe des Befehls **debug lwapp events enable** auf dem Controller zeigt folgende Ergebnisse:

```
(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
```

Fehlerbehebung

In diesem Abschnitt finden Sie eine Fehlerbehebung für Ihre Konfiguration.

Befehle zur Fehlerbehebung

Sie können diese **Debug**-Befehle verwenden, um die Konfiguration zu beheben.

Hinweis: Beachten Sie [vor der](#) Verwendung von **Debug**-Befehlen die [Informationen](#) zu [Debug-Befehlen](#).

- **debug lwapp events enable:** Zeigt die Abfolge von Ereignissen an, die zwischen der LAP und dem WLC auftreten.
- **debug lwapp errors enable:** Zeigt die Fehler an, die in der LWAPP-Kommunikation auftreten.
- **debug lwapp packet enable:** Zeigt das Debuggen einer LWAPP-Paketverfolgung an.
- **debug mac addr:** Aktiviert das MAC-Debuggen für den Client, den Sie angeben.

Zugehörige Informationen

- [REAP-Implementierungsleitfaden für Zweigstellen](#)
- [Konfigurationsbeispiel für EAP-Authentifizierung mit WLAN-Controllern \(WLC\)](#)
- [Grundlegende Konfigurationsbeispiel für Wireless LAN Controller und Lightweight Access Point](#)
- [Konfigurationsbeispiel für WLAN-Controller-Failover für Lightweight Access Points](#)
- [Wireless-Support-Seite](#)
- [Technischer Support und Dokumentation - Cisco Systems](#)