

# Configuratievoorbeeld van Remote-Edge AP (REAP) met lichtgewicht AP's en draadloze LAN-controllers (WLC's)

## Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Conventies](#)

[Achtergrondinformatie](#)

[Configureren](#)

[Netwerkdigram](#)

[De WLC configureren voor basisbediening en WLAN's configureren](#)

[Prime de AP voor installatie op de Remote Site](#)

[Configureer de 2800 routers om de WAN-link in te stellen](#)

[AP op de Remote Site implementeren](#)

[Verifiëren](#)

[Problemen oplossen](#)

[Opdrachten voor troubleshooting](#)

[Gerelateerde informatie](#)

## [Inleiding](#)

Remote-Edge access point (REAP)-functies die met Cisco Unified Wireless Network worden geïntroduceerd, maken een externe implementatie van Cisco lichtgewicht access points (LAP's) via de Wireless LAN-controller (WLC) mogelijk. Dit maakt ze ideaal voor filiaal-kantoor en kleine detailhandelslocaties. Dit document legt uit hoe u een op REAP gebaseerd WLAN-netwerk kunt implementeren met gebruik van Cisco 1030 Series LAP en 4400 WLCs.

## [Voorwaarden](#)

### [Vereisten](#)

Zorg ervoor dat u aan deze vereisten voldoet voordat u deze configuratie probeert:

- Kennis van WLC's en hoe u de WLC-fundamentele parameters kunt configureren
- Kennis van de REAP-werkingswijze in een Cisco 1030 LAP
- Kennis van de configuratie van een externe DHCP-server en/of Domain Name System (DNS)-

server

- Kennis van Wi-Fi Protected Access (WPA) concepten

## Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco 4400 Series WLC-software met firmware release 4.2
- Cisco 1030 LAP
- Twee Cisco 2800 Series routers die Cisco IOS®-software release 12.2(13)T13 uitvoeren
- Cisco Aironet 802.11a/b/g clientadapter voor firmware release 3.0
- Cisco Aironet desktop hulpprogramma versie 3.0

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

## Conventies

Raadpleeg [Cisco Technical Tips Conventions \(Conventies voor technische tips van Cisco\) voor meer informatie over documentconventies.](#)

## Achtergrondinformatie

In de REAP-modus kan een LAP over een WAN-link wonen en kan hij nog met de WLC communiceren en de functionaliteit van een gewone LAP leveren. De REAP-modus wordt op dit punt alleen op de 1030 LAP's ondersteund.

Om deze functionaliteit te bieden, scheidt de 1030 REAP het lichtgewicht Access Point Protocol (LWAPP) besturingsplane van het draadloze gegevensvliegtuig. Cisco WLCs worden nog steeds gebruikt voor gecentraliseerd beheer en beheer op dezelfde manier dat de regelmatige op LWAPP gebaseerde access points (APs) worden gebruikt, terwijl alle gebruikersgegevens lokaal bij de AP worden aangesloten. De toegang tot lokale netwerkbronnen wordt door WAN-uitgangen behouden.

REAPs ondersteunt twee werkingsmodi:

- Normale REAP-modus
- Standalone

De LAP wordt ingesteld in de normale REAP-modus wanneer de WAN-link tussen de REAP en de WLC omhoog is. Wanneer LAPs in normale REAP-modus werken, kunnen ze tot 16 WLAN's ondersteunen.

Wanneer de WAN-verbinding tussen de WLC en de LAP omlaag gaat, de LAP met REAP-enabled switches naar de standalone modus. Terwijl in de standalone modus, kunnen de REAP-APENS slechts één WLAN onafhankelijk ondersteunen zonder de WLC, als de WLAN wordt geconfigureerd met ofwel Wired Equivalent Privacy (WEP) of enige lokale authenticatiemethode. In dit geval, is het WLAN dat de REAP ondersteunt het eerste WLAN dat wordt geconfigureerd op AP, WLAN 1. Dit is omdat de meeste andere echtheidsmethoden informatie moeten doorgeven aan en van de controller en, wanneer de WAN-link omlaag is, deze operatie niet mogelijk is. In de

standalone modus ondersteunen de LAP's een minimale reeks functies. Deze tabel toont de reeks functies die een REAP LAP ondersteunt wanneer deze in standalone modus is in vergelijking met de functies die een REAP LAP in normale modus ondersteunt (wanneer de WAN-link omhoog is en de communicatie naar WLC omhoog is):

#### Functies die een REAP LAP in normale REAP-modus en in standalone ondersteunt

		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
Layer 3 Security	WPA2-EAP	Yes	No
	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
Mobility	AAA QoS Profile override	Yes	No
	Intra-subnet	Yes	Yes
DHCP	Inter-subnet	No	No
	Internal DHCP Server	No	No
	External DHCP Server	Yes	Yes
Topology	Direct connect (2006)	No	No

De tabel laat zien dat meerdere VLAN's niet op REAP LAP's in beide modi worden ondersteund. Meervoudige VLAN's worden niet ondersteund omdat REAP-LAP's alleen op één subnetwerk kunnen verblijven omdat zij de codering van IEEE 802.1Q VLAN niet kunnen uitvoeren. Daarom eindigt het verkeer op elk van de Service set identificatoren (SSID's) op hetzelfde net als het bekabelde netwerk. Als resultaat hiervan wordt het gegevensverkeer niet van de verbonden kant

gescheiden alhoewel het draadloze verkeer over de lucht tussen SSID's kan worden gesegmenteerd.

Raadpleeg de [REAP Deployment Guide bij het Vestigingskantoor](#) voor meer informatie over de REAP-implementatie en hoe u REAP en zijn beperkingen beheert.

## Configureren

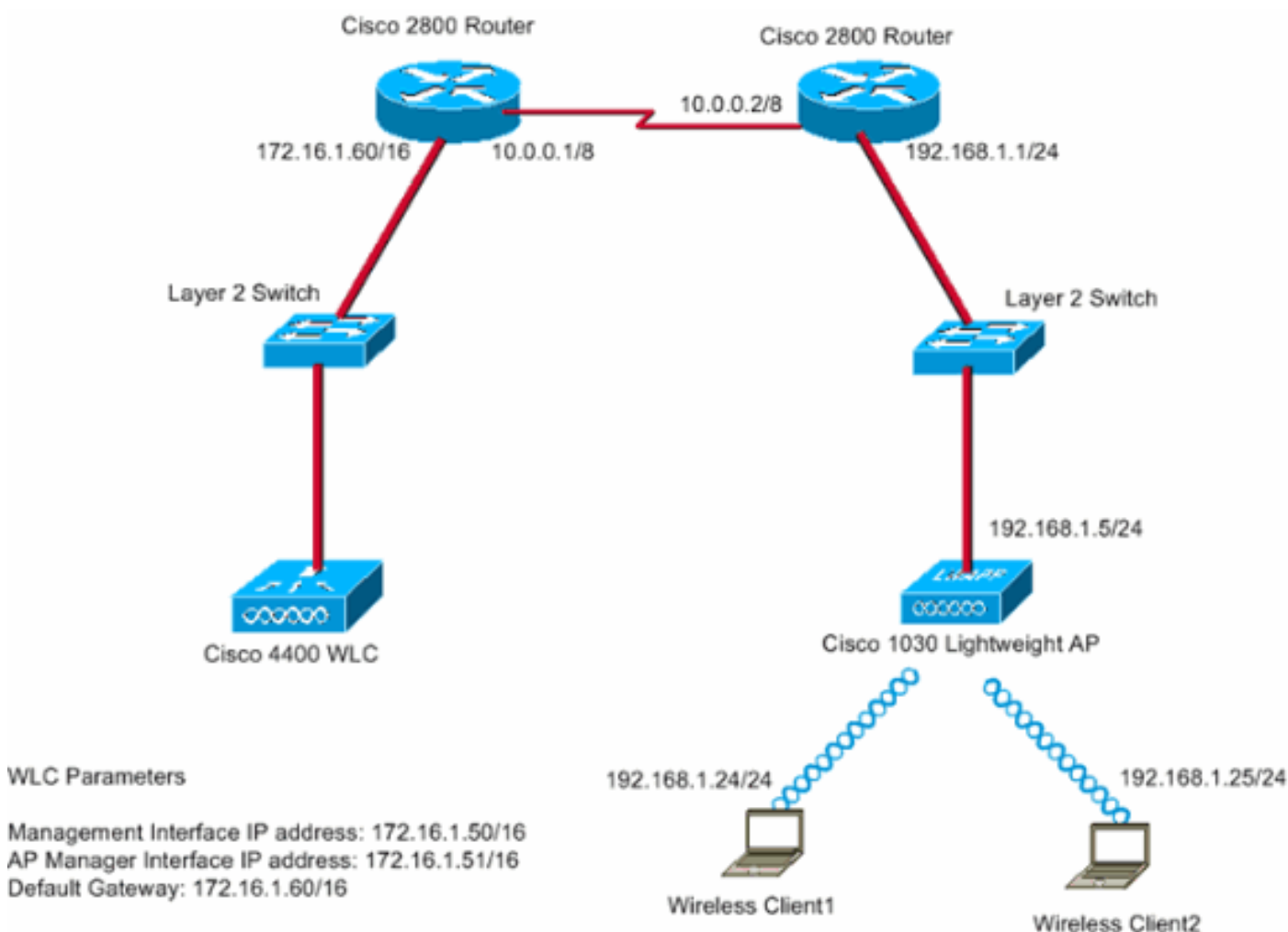
Deze sectie bevat informatie over het configureren van de functies die in dit document worden beschreven.

Voltooi de volgende stappen om de instellingen van het netwerk te configureren:

1. [Configureer de WLC voor basisbediening en stel WLAN's in.](#)
2. [Prime het AP voor installatie op de verre plaats.](#)
3. [Configureer de 2800 routers om de WAN-link in te stellen.](#)
4. [Stel het REAP LAP in op de verafgelegen plaats.](#)

## Netwerkdigram

Het netwerk in dit document is als volgt opgebouwd:



Het hoofdkantoor sluit zich aan bij het bijkantoor met behulp van een huurlijn. De huurlijn eindigt op 2800 Series routers aan elk eind. Dit voorbeeld gebruikt Open Snelst Path First (OSPF)

Protocol om gegevens op de WAN-link met PPP-insluiting te verzenden. Het 4400 WLC bevindt zich in het hoofdkantoor en de 1030 LAP moet worden gebruikt op het afstandsbediening. De LAP 1030 moet twee WLAN's ondersteunen. Hier zijn de parameters voor WLAN's:

- **WLAN 1 SSID—SSID1 Verificatie—openen Encryptie-tijdelijk toetsingspakket (TKIP) (vóór gedeelde sleutel [WAP-PSK])**
- **WLAN 2 SSID—SSID2 Verificatie-uitvoerbaar verificatieprotocol (EAP) Encryptie-TKIP** Opmerking: voor WLAN 2 gebruikt de configuratie in dit document WAP (802.1x-verificatie en TKIP voor encryptie).

U dient de apparaten voor deze instelling te configureren.

## [De WLC configureren voor basisbediening en WLAN's configureren](#)

U kunt de wizard opstartconfiguratie gebruiken in de opdrachtregel-interface (CLI) om de WLC te configureren voor een eenvoudige bediening. In plaats hiervan kunt u ook de GUI gebruiken om de WLC te configureren. Dit document verklaart de configuratie op de WLC met gebruik van de opstartconfiguratie wizard op de CLI.

Nadat de WLC voor het eerst start, gaat het direct in de opstartconfiguratie wizard. U gebruikt de configuratiewizard om basisinstellingen te configureren. U kunt de wizard op de CLI of de GUI uitvoeren. Hier is een voorbeeld van de wizard opstartconfiguratie:

```
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...
```

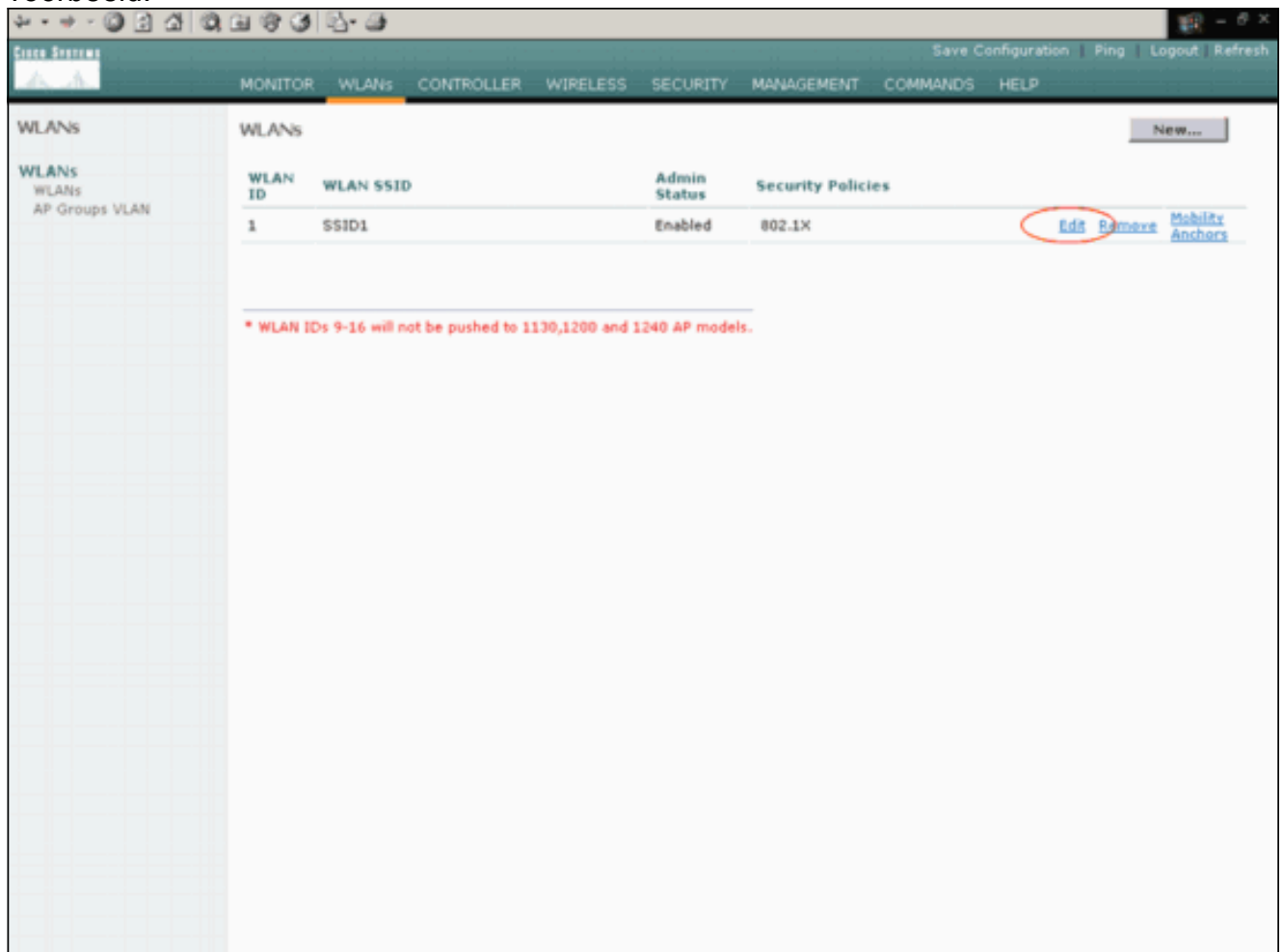
Dit voorbeeld vormt deze parameters op de WLC:

- **Systeemnaam**
- **IP-adres van de beheerinterface**

- IP-adres voor AP-interface-beheer
- Beheer interfacepoortnummer
- Identificatiecode van de beheerinterface VLAN
- Mobiliteitsgroepnaam
- SSID
- Veel andere parameters

Deze parameters worden gebruikt om de WLC voor basisbediening in te stellen. Zoals de uitvoer van WLC in deze sectie toont, gebruikt WLC 172.16.1.50 als het IP-adres van de beheersinterface en 172.16.1.51 als het IP-adres van de AP-Manager. Voltooi de volgende stappen op de WLC om de twee WLAN's voor uw netwerk te configureren:

1. Klik vanuit de WLC GUI op **WLAN's** in het menu boven in het venster. Het WLAN-venster verschijnt. Dit venster maakt een lijst van WLAN's die op de WLC zijn geconfigureerd. Omdat u één WLAN hebt ingesteld met gebruik van de wizard opstarten, moet u de andere parameters voor deze WLAN configureren.
2. Klik op **Bewerken** voor WLAN SSID1. Hierna volgt een voorbeeld:



Het WLAN's > Bewerken venster verschijnt. In dit venster kunt u de parameters configureren die specifiek zijn voor WLAN, wat algemeen beleid, beveiligingsbeleid, RADIUS-server en anderen omvat.

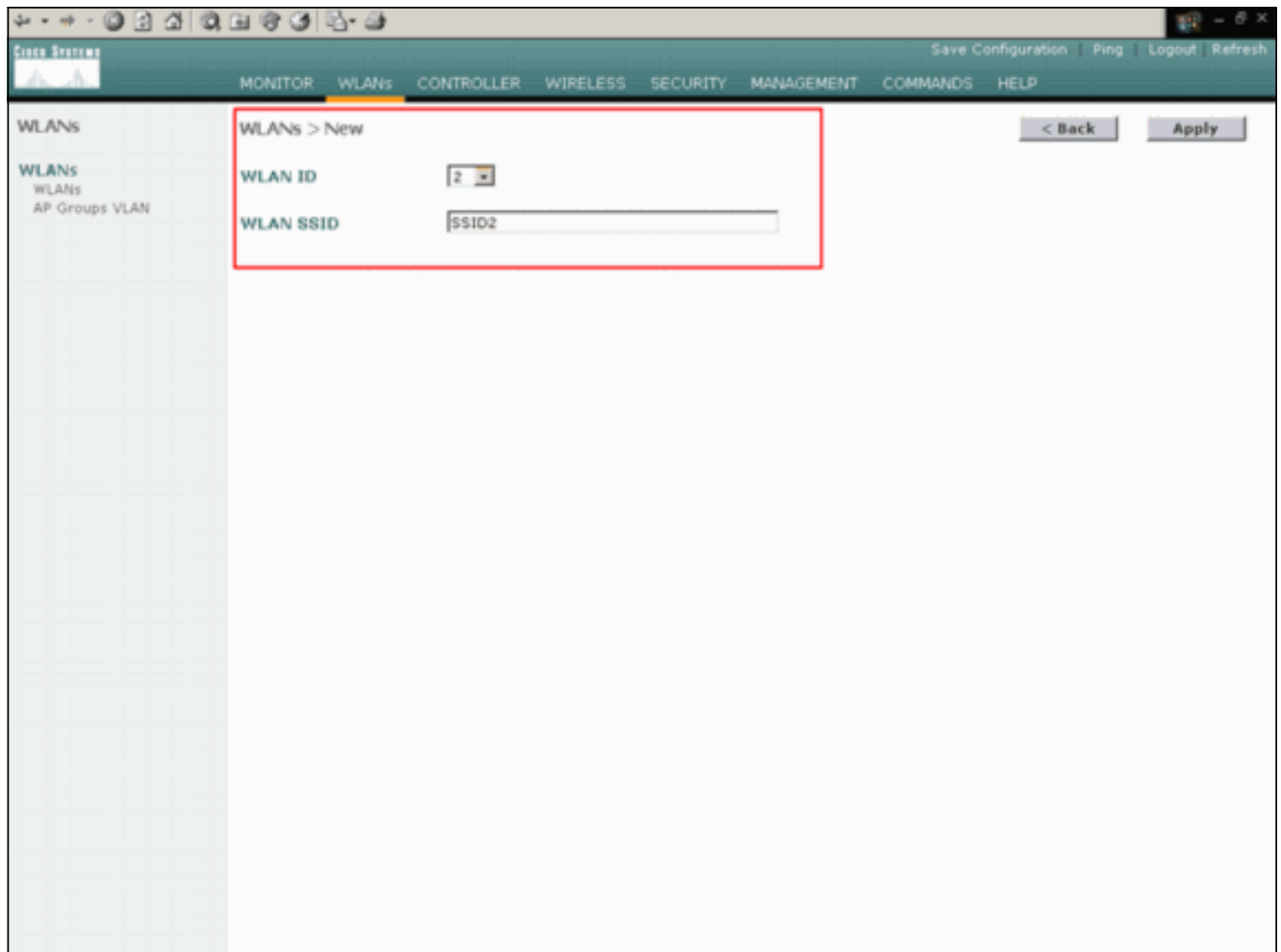
3. Maak deze selectie in het WLAN's > Bewerken venster: In het gebied Algemeen beleid, controleert u het vakje **Enabled** naast de Admin Status om dit WLAN in te schakelen. Kies **WAP** uit het vervolgkeuzemenu Layer 2 Security om WAP voor WLAN 1 te gebruiken. Definieert de parameters van WAP onder in het venster. Als u WAP-PSK op WLAN 1 wilt gebruiken, controleert u het dialoogvenster **Ingeschakeld** naast de voorgedeelde

slutel in het gebied met WAP-parameters en voert u het wachtwoord voor WAP-PSK in. WAP-PSK gebruikt TKIP voor encryptie. **Opmerking:** het wachtwoord voor WAP-PSK moet overeenkomen met het wachtwoord dat op de clientadapter is ingesteld zodat WAP-PSK kan werken. Klik op **Apply** (Toepassen). Hierna volgt een voorbeeld:

The screenshot displays the Cisco Systems configuration interface for WLAN 1. The 'General Policies' section includes 'Admin Status' set to 'Enabled' (circled in red). The 'Security Policies' section shows 'Layer 2 Security' set to 'WPA' (circled in red). The 'WPA Parameters' section (boxed in red) shows '802.11 Data Encryption' as 'TKIP-MIC', 'Pre-Shared Key' as 'Enabled', and 'Set Passphrase' as '\*\*\*\*\*'. Other settings include 'Radio Policy' (All), 'Session Timeout (secs)' (1800), 'Quality of Service (QoS)' (Silver (best effort)), 'WMM Policy' (Disabled), '7920 Phone Support' (Client CAC Limit and AP CAC Limit), 'Broadcast SSID' (Enabled), 'Allow AAA Override' (Enabled), 'Client Exclusion' (Enabled \*\*), 'DHCP Server' (Override), 'DHCP Addr. Assignment' (Required), and 'Interface Name' (management).

U hebt WLAN 1 ingesteld voor WAP-PSK-encryptie.

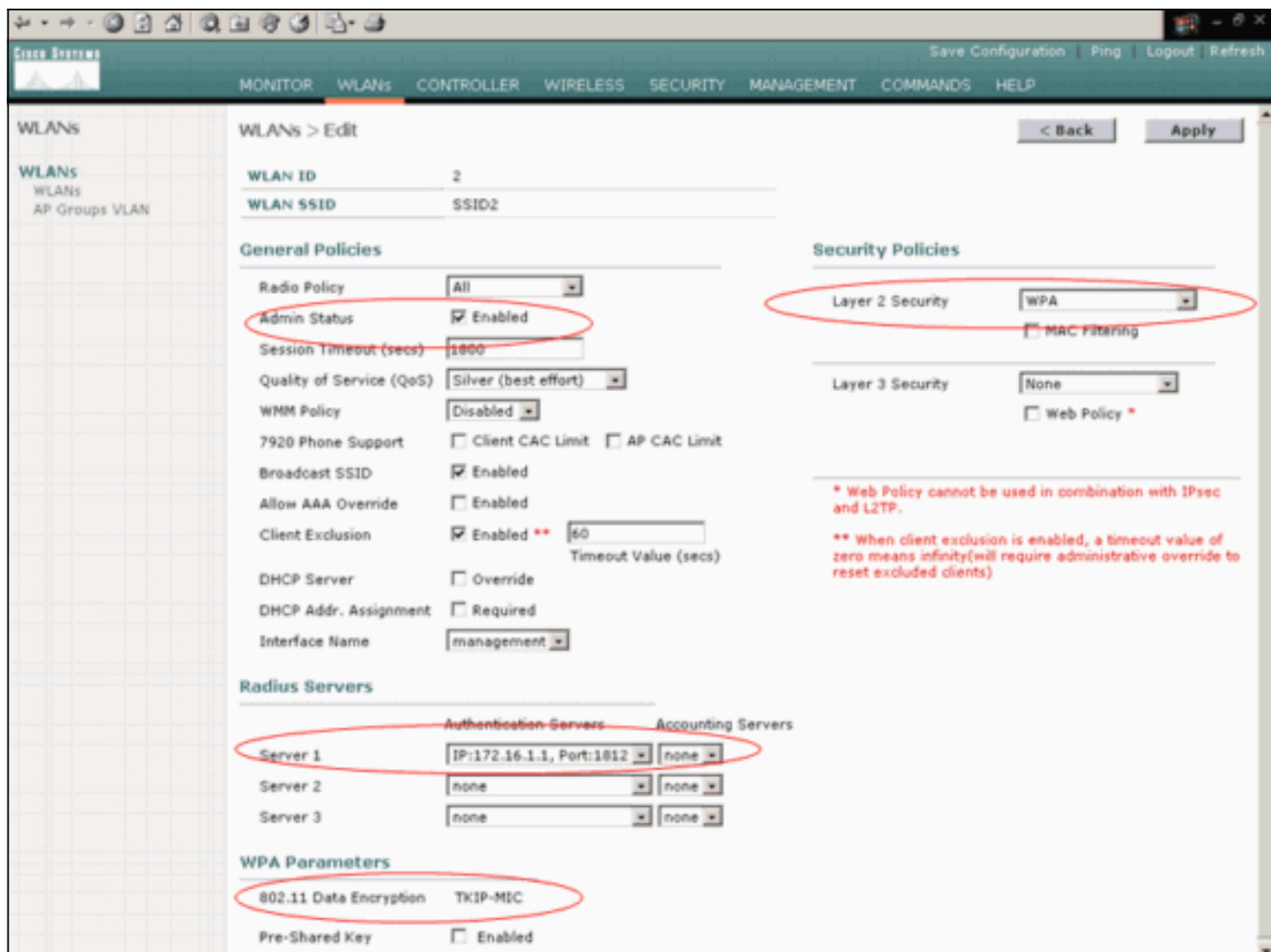
- Om WLAN 2 te definiëren, klikt u op **Nieuw** in het venster van WLAN's. Het WLAN > Nieuw venster verschijnt.
- In het WLAN > New venster, definieer de WLAN-id en de WLAN-sid en klik op **Toepassen**. Hierna volgt een voorbeeld:



Het WLAN > Bewerken venster voor de tweede WLAN verschijnt.

6. Maak deze selectie in het WLAN's > Bewerken venster: In het gebied Algemeen beleid, controleert u het vakje **Enabled** naast de Admin Status om dit WLAN in te schakelen. Kies **WAP** uit het vervolgkeuzemenu Layer 2 Security om WAP voor dit WLAN te configureren. Kies in het gebied RADIUS-servers de juiste RADIUS-server om te gebruiken voor verificatie van de klanten. Klik op **Apply** (Toepassen). Hierna volgt een voorbeeld:





**Opmerking:** In dit document wordt niet uitgelegd hoe u de RADIUS-servers en de EAP-verificatie moet configureren. Raadpleeg voor informatie over de manier waarop u EAP-verificatie met WLC's kunt configureren [EAP-verificatie met WLAN-controllers \(WLC\) configuratievoorbeeld](#).

## [Prime de AP voor installatie op de Remote Site](#)

Priming is een proces waardoor LAP's een lijst krijgen van controllers waarmee ze kunnen verbinden. LAP's worden op de hoogte gebracht van alle controllers in de mobiliteitsgroep zodra zij zich aansluiten op één enkele controller. Op deze manier leren de LAP's alle informatie die ze nodig hebben om zich bij een controller in de groep aan te sluiten.

Om een AP-Geschikt AP te gebruiken, sluit AP aan op het bedraad netwerk bij het hoofdbureau. Met deze verbinding kan AP één controller ontdekken. Nadat de LAP zich bij de controller in het hoofdkantoor heeft aangesloten, downloads de AP-versie van het AP-besturingssysteem die overeenkomt met de WLAN-infrastructuur en de configuratie. De IP-adressen van alle controllers in de mobiliteitsgroep worden overgedragen naar de AP. Wanneer AP alle informatie heeft die het nodig heeft, kan AP op de verre plaats worden aangesloten. AP kan dan de minst gebruikte controller van de lijst ontdekken en aansluiten, als IP connectiviteit beschikbaar is.

**N.B.:** Stel AP's in op "REAP"-modus voordat u ze uitzet om ze naar de afgelegen locaties te verschepen. U kunt de modus op het AP-niveau instellen via de CLI of GUI van de controller, of met het gebruik van WCS-sjablonen (Wireless Control System). AP's worden ingesteld om regelmatige, "lokale" functionaliteit standaard uit te voeren.

De LAP's kunnen elk van deze methoden gebruiken om de controller te vinden:

- Layer 2 ontdekking

- **Layer 3 ontdekking** Met het gebruik van een lokale netto uitzending Met gebruik van DHCP-optie 43 Met het gebruik van een DNS-server Met behulp van overair Provisioning (OTAP) Met het gebruik van een interne DHCP-server **Opmerking:** om een interne DHCP-server te kunnen gebruiken, moet de LAP direct op de WLC worden aangesloten.

In dit document wordt ervan uitgegaan dat de LAP-gegevens bij de WLC worden geregistreerd met behulp van het DHCP-optie 43 discovery-mechanisme. Raadpleeg voor meer informatie over het gebruik van DHCP-optie 43 om de LAP te registreren bij de controller en de andere zoekmechanismen [lichtgewicht AP \(LAP\)-registratie bij een draadloze LAN-controller \(WLC\)](#).

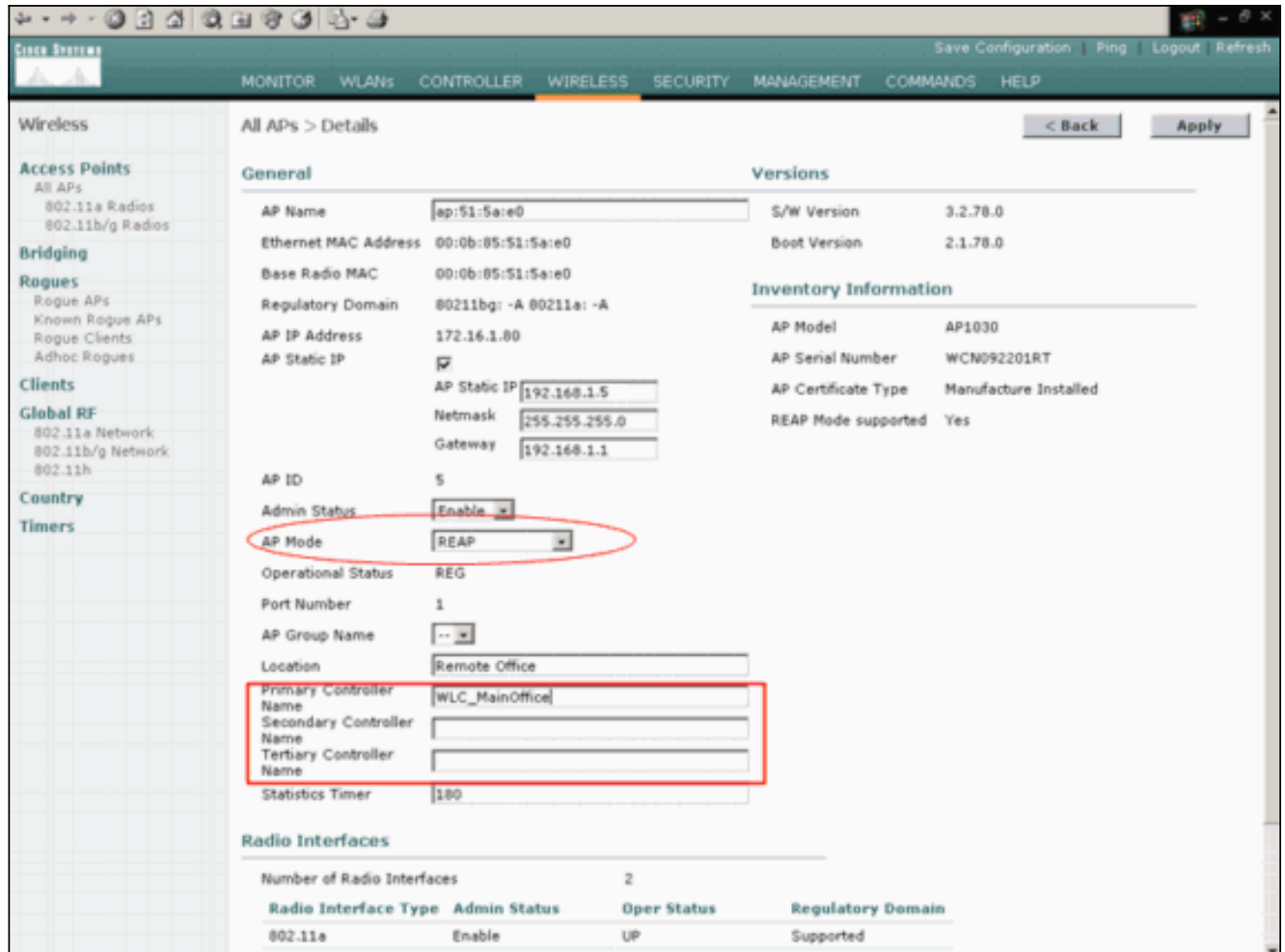
Nadat de LAP de controller heeft ontdekt, kunt u zien dat de AP is geregistreerd op de controller in het draadloze venster van de WLC. Hierna volgt een voorbeeld:

AP Name	AP ID	Ethernet MAC	Admin Status	Operational Status	Port	
ap:51:5a:e0	5	00:0b:05:51:5a:e0	Enable	REG	1	<a href="#">Detail</a>

Volg deze stappen om de LAP te configureren voor de normale REAP-modus:

1. Klik vanuit de WLC GUI op **Draadloos**. Het venster Alle APs verschijnt. Dit venster toont APs die aan WLC worden geregistreerd.
2. Selecteer AP dat u voor de modus REAP moet vormen en klik op **Detail**. Het venster Alle APs > Detail voor de specifieke AP verschijnt. In dit venster kunt u de verschillende parameters van AP configureren, waaronder: AP-naam IP-adres (dat u kunt wijzigen in statisch) Admin-status Beveiligingsparameters AP-modus Lijst van WLC's waarmee AP kan verbinden Overige parameters
3. Kies **REAP** uit het vervolgkeuzemenu AP-modus. Deze modus is alleen beschikbaar op AP-compatibele AP's.
4. Bepaal de controlenamen die de AP's zullen gebruiken om te registreren en klik op

**Toepassen.** U kunt maximaal drie controlerenamen definiëren (primaire, secundaire en tertiaire). De AP's zoeken naar de controller in de dezelfde volgorde die u in dit venster geeft. Omdat dit voorbeeld slechts één controller gebruikt, definieert het voorbeeld de controller als de primaire controller. Hierna volgt een voorbeeld:



U hebt AP voor de wijze van het REAP ingesteld en u kunt het op de verre plaats opstellen.

**Opmerking:** In dit voorbeeldvenster kunt u zien dat het IP-adres van de AP is gewijzigd in statische IP-adressen 192.168.1.5 is toegewezen. Deze opdracht komt voor omdat dit het subtype is dat gebruikt moet worden op het externe kantoor. U gebruikt het IP-adres vanaf de DHCP-server, 172.16.1.80, alleen tijdens het voorbereidingsstadium. Nadat het AP bij de controller is geregistreerd, wijzigt u het adres in een statisch IP-adres.

## [Configureer de 2800 routers om de WAN-link in te stellen](#)

Om de WAN-link te creëren, gebruikt dit voorbeeld twee 2800 Series routers met OSPF om informatie tussen de netwerken te verzenden. Hier is de configuratie van beide routers voor het voorbeeldscenario in dit document:

```

Hoofdkantoor

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-Templat1 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

```

## Vestigingskantoor

```

BranchOffice#show run
Building configuration...

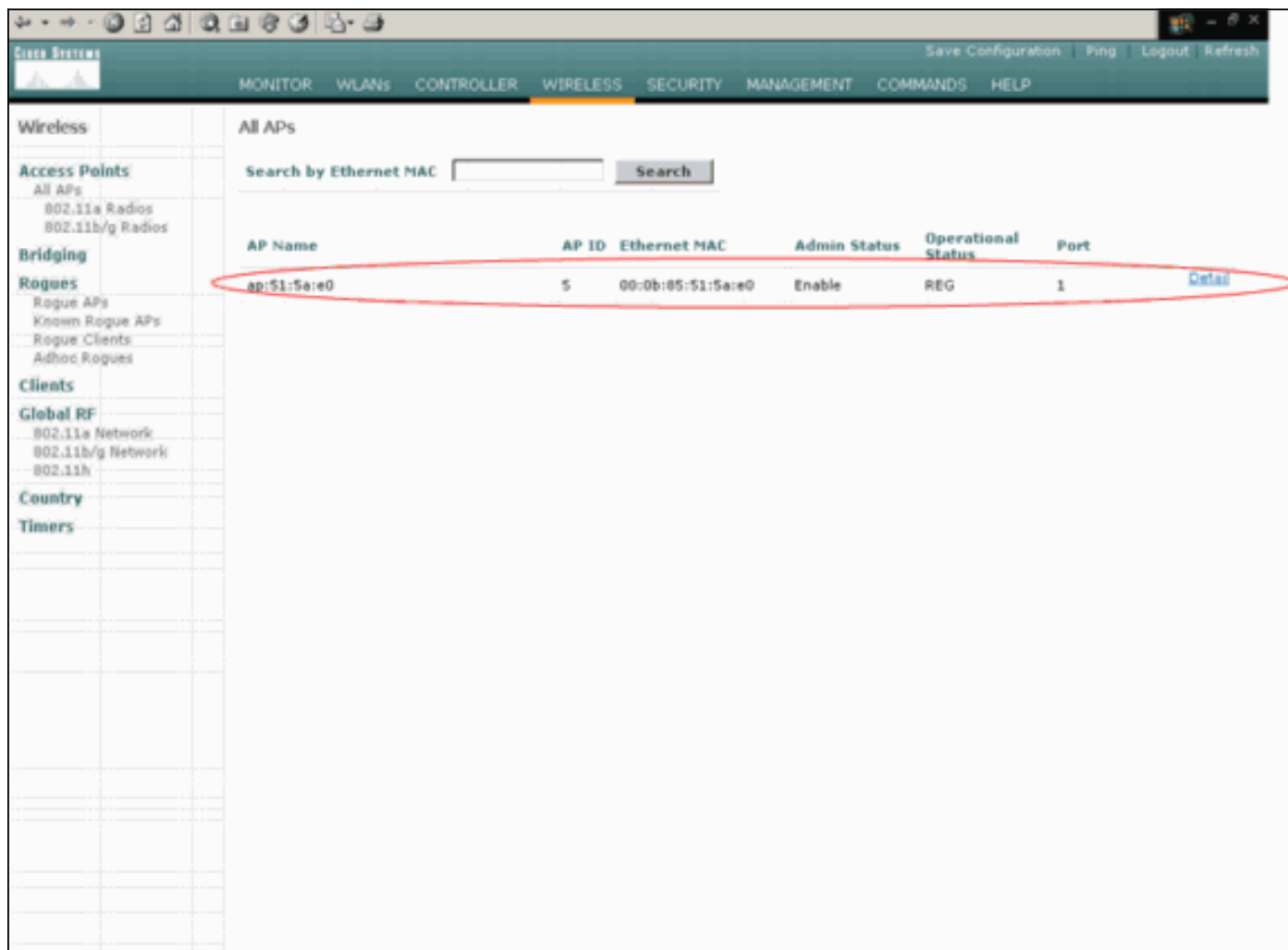
Current configuration : 596 bytes
!
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname BranchOffice
!
!
ip subnet-zero
!
!
!
!
interface Ethernet0
 ip address 192.168.1.1 255.255.255.0
 !--- This is the interface which acts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

```

## [AP op de Remote Site implementeren](#)

Nu u WLAN's op de WLC's hebt geconfigureerd, de LAP hebt voorbereid en de WAN-verbinding tussen het hoofdkantoor en het externe kantoor hebt ingesteld, bent u klaar om het AP op de externe site te implementeren.

Nadat u de AP op de verre plaats hebt opgestart, zoekt AP de controller in de volgorde die u in het voorbereidingsstadium hebt ingesteld. Nadat de AP de controller vindt, registreert de AP bij de controller. Hierna volgt een voorbeeld. Vanaf WLC kunt u zien dat AP zich bij de controller op poort 1 heeft aangesloten:



Clients die SSID **SSID1** hebben en waarvoor WAP-PSK is ingeschakeld, associëren met AP op WLAN 1. Clients die SSID **SSID2** hebben, en die 802.1x-verificatie hebben ingeschakeld, associëren met AP op WLAN 2. Hier is een voorbeeld dat twee clients toont. Eén client is verbonden met WLAN 1 en de andere client is verbonden met WLAN 2:

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:acidd:05	ap:51:5a:e0	00:0b:85:51:5a:e0	SSID1	802.11a	Associated	Yes	1	<a href="#">Detail</a> <a href="#">Link Test</a> <a href="#">Disable</a> <a href="#">Remove</a>
00:40:96:ac1e6:57	ap:51:5a:e0	00:0b:85:51:5a:e0	SSID2	802.11a	Associated	Yes	1	<a href="#">Detail</a> <a href="#">Link Test</a> <a href="#">Disable</a> <a href="#">Remove</a>

## Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie van uw REAP correct werkt.

**Opmerking:** Raadpleeg [Belangrijke informatie over debug Commands](#) voordat u debug-opdrachten gebruikt.

Breng de WAN-link naar beneden. Wanneer de WAN-link is ingedrukt, verliest AP connectiviteit met de WLC. De WLC dereguleert vervolgens de AP van zijn lijst. Hierna volgt een voorbeeld:

```
(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
```

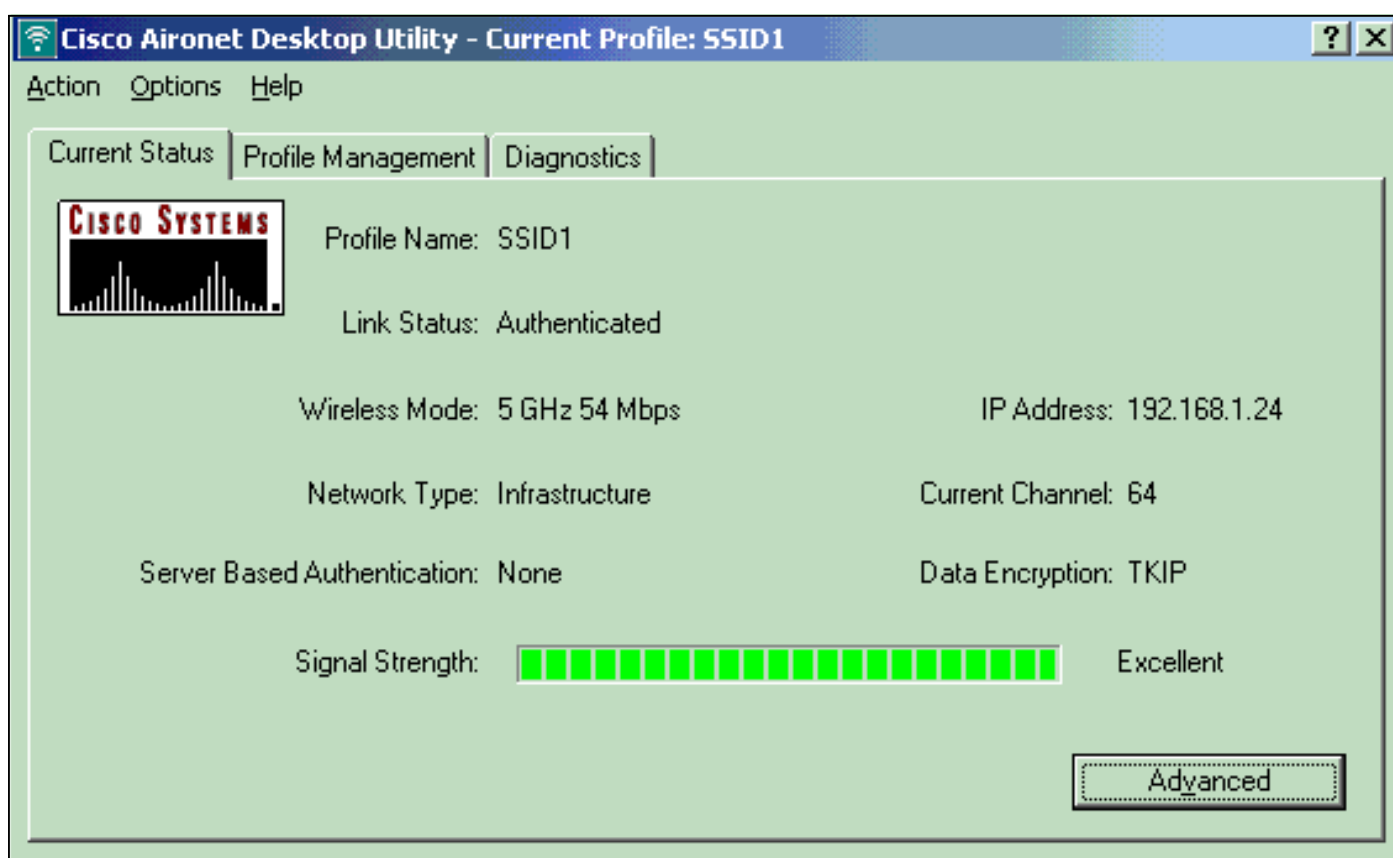
Wed May 17 15:04:22 2006: Received LWAPP Down event for AP 00:0b:85:51:5a:e0 slot 1!

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

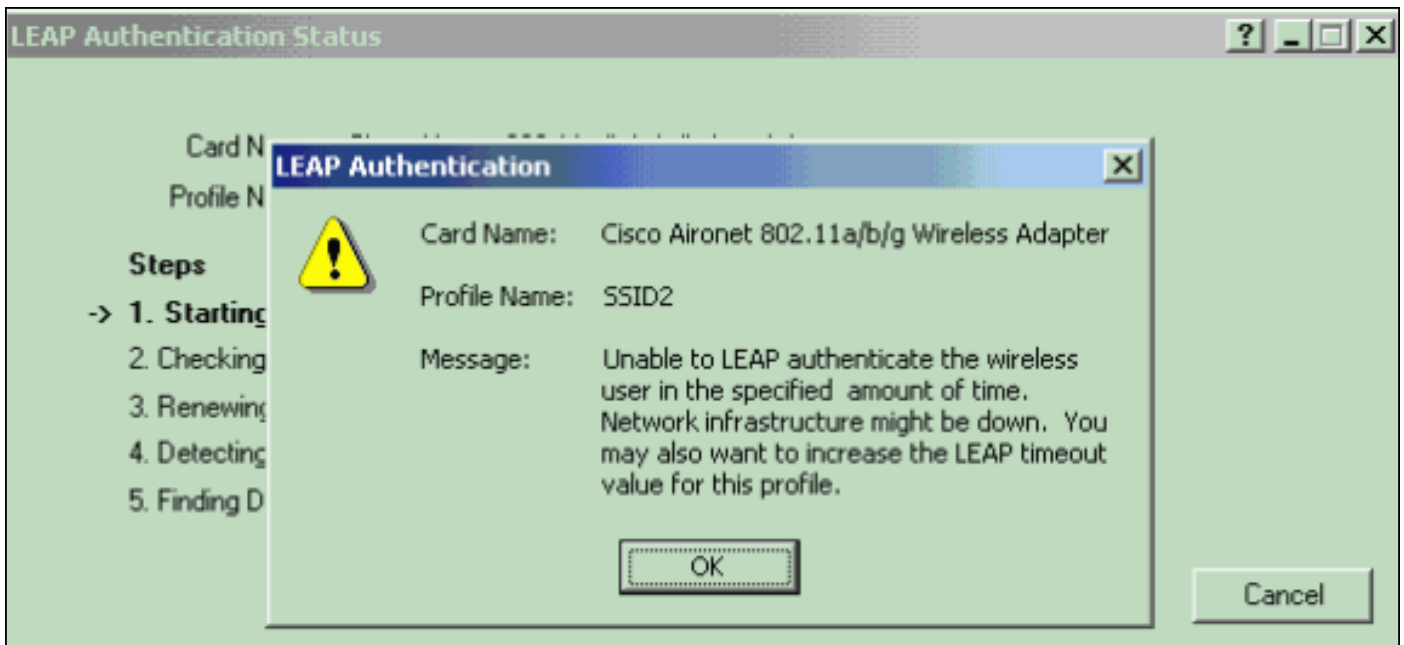
Van de **debug lwapp gebeurtenissen kunnen** commando output **maken**, je kunt zien dat de WLC de AP deregistert omdat de WLC geen hartstochtelijk antwoord van AP ontving. Een antwoord op de hartslag lijkt op boodschappen die levend blijven. De controller probeert vijf opeenvolgende hartslagen, één seconde uit elkaar. Als de WLC geen antwoord ontvangt, dereguleert de WLC het AP.

Wanneer het AP in standalone modus is, begint het AP-stroom LED te knipperen. De klanten die aan de eerste WLAN (WLAN 1) associëren worden nog steeds aan de AP gekoppeld omdat de clients in de eerste WLAN worden geconfigureerd voor alleen WAP-PSK-encryptie. De LAP verwerkt de encryptie zelf in de standalone modus. Dit is een voorbeeld dat de status (wanneer de WAN-link is ingedrukt) toont van een client die is verbonden met WLAN 1 met SSID1 en WAP-PSK:

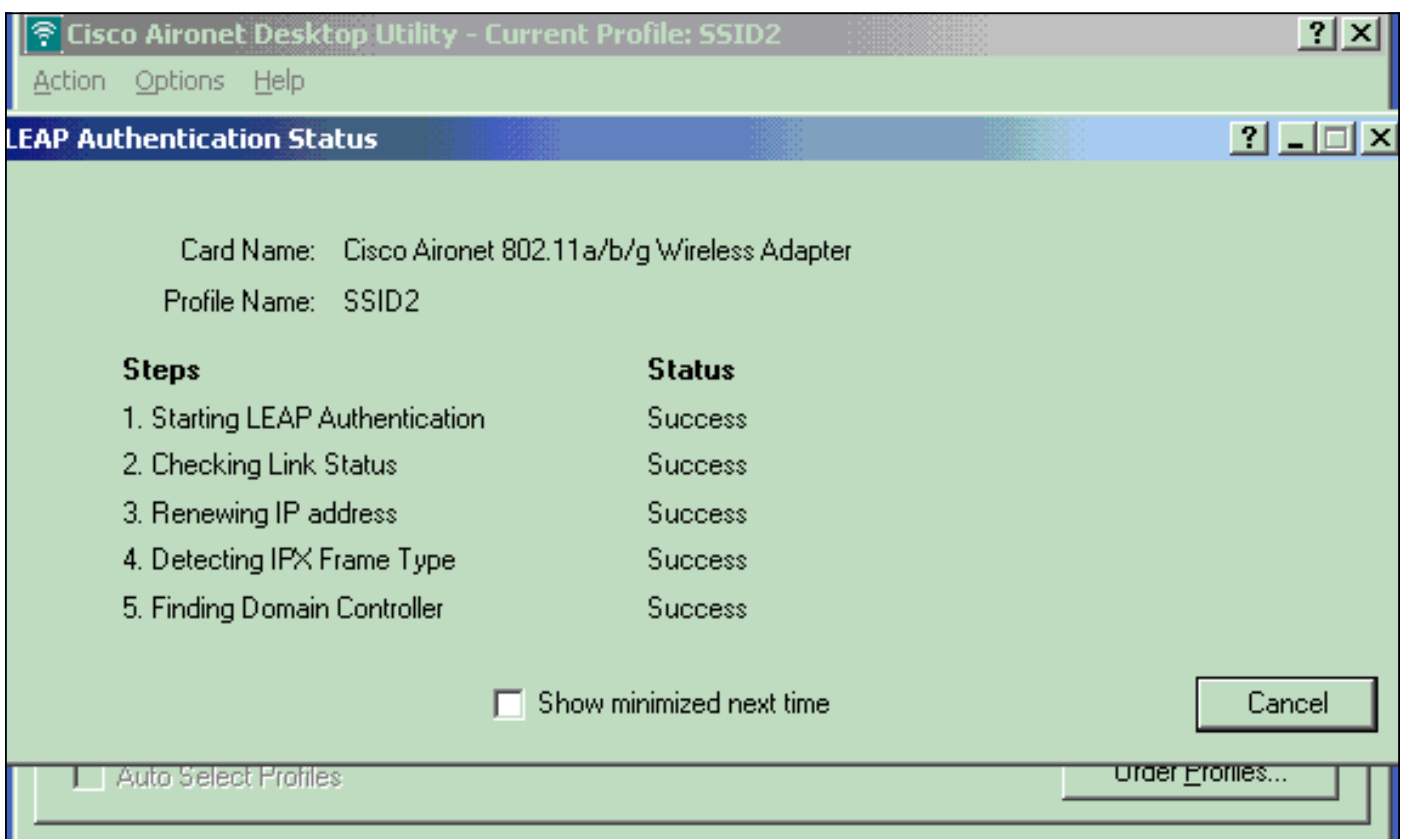
**Opmerking:** TKIP is de encryptie die met WAP-PSK gebruikt wordt.



De klanten die zijn verbonden met WLAN 2 worden losgekoppeld omdat WLAN 2 gebruik maakt van EAP-verificatie. Deze ontkoppeling gebeurt omdat klanten die MAP-authenticatie gebruiken, moeten communiceren met de WLC. Dit is een voorbeeldvenster dat aantoont dat de EAP-verificatie mislukt wanneer de WAN-link is weggevallen:



Nadat de WAN-link is geopend, herstellen de AP-switches de normale REAP-modus en registreren zij met de controller. Ook de cliënt die gebruikmaakt van MAP-authenticatie komt naar voren. Hierna volgt een voorbeeld:



Deze voorbeelduitvoer van de **debug-gebeurtenissen** maakt het mogelijk om opdracht te geven in de controller toont deze resultaten:

```
(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, gw 192.168.1.1
```

## Problemen oplossen

Gebruik dit gedeelte om de configuratie van het probleem op te lossen.

### Opdrachten voor troubleshooting

U kunt deze debug-opdrachten gebruiken om de configuratie problemen op te lossen.

**Opmerking:** Raadpleeg [Belangrijke informatie over debug Commands](#) voordat u **debug-**opdrachten gebruikt.

- **debug lwapp gebeurtenissen** maken het mogelijk—hiermee wordt de opeenvolging van gebeurtenissen weergegeven die tussen de LAP en de WLC plaatsvinden.
- **debug lwapp fouten activeren**—hiermee worden de fouten weergegeven die in de LWAPP-communicatie optreden.
- **debug-pakkettransport door middel van:** Geeft het debug van een LWAPP-pakkettransport weer.
- **debug mac addr**-schakelt MAC-debugging in voor de client die u specificeert.

## Gerelateerde informatie

- [REAP-implementatiegids bij de Vestigingsvestiging](#)
- [PPP-verificatie met WLAN-controllers \(WLC\) - configuratievoorbeeld](#)
- [Configuratievoorbeeld voor draadloos LAN-controller en lichtgewicht access point](#)
- [WLAN-controller-failover voor lichtgewicht access points - Configuratievoorbeeld](#)
- [Draadloze ondersteuningspagina](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)