

Esempio di configurazione di Remote-Edge AP (REAP) con Lightweight AP e Wireless LAN Controller (WLC)

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Convenzioni](#)

[Premesse](#)

[Configurazione](#)

[Esempio di rete](#)

[Configurazione del WLC per il funzionamento di base e configurazione delle WLAN](#)

[Prime the AP per l'installazione sul sito remoto](#)

[Configurazione dei router 2800 per stabilire il collegamento WAN](#)

[Distribuire il punto di accesso REAP sul sito remoto](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Comandi per la risoluzione dei problemi](#)

[Informazioni correlate](#)

[Introduzione](#)

Le funzionalità dei punti di accesso remoti (REAP) introdotte con Cisco Unified Wireless Network consentono l'implementazione remota dei Cisco Lightweight Access Point (LAP) dal controller WLAN (Wireless LAN). Ciò le rende ideali per filiali e punti vendita di piccole dimensioni. Questo documento spiega come implementare una rete WLAN basata su REAP con i Cisco serie 1030 LAP e 4400 WLC.

[Prerequisiti](#)

[Requisiti](#)

Prima di provare questa configurazione, accertarsi di soddisfare i seguenti requisiti:

- Conoscenza dei WLC e come configurare i parametri base del WLC
- Conoscenza della modalità di funzionamento REAP in un Cisco 1030 LAP
- Conoscenza della configurazione di un server DHCP esterno e/o di un server DNS (Domain

Name System)

- Conoscenza dei concetti di Wi-Fi Protected Access (WPA)

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco serie 4400 WLC con firmware versione 4.2
- Cisco 1030 LAP
- Due router Cisco serie 2800 con software Cisco IOS® versione 12.2(13)T13
- Cisco Aironet 802.11a/b/g Client Adapter con firmware versione 3.0
- Cisco Aironet Desktop Utility versione 3.0

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento [Cisco sulle convenzioni nei suggerimenti tecnici](#).

Premesse

La modalità REAP permette a un LAP di risiedere su un collegamento WAN e di comunicare con il WLC e fornire la funzionalità di un LAP normale. a questo punto, la modalità REAP è supportata solo sui 1030 LAP.

Per fornire questa funzionalità, il 1030 REAP separa il control plane Lightweight Access Point Protocol (LWAPP) dal data plane wireless. I WLC Cisco vengono ancora utilizzati per il controllo e la gestione centralizzati nello stesso modo in cui vengono utilizzati i punti di accesso basati su LWAPP normali, mentre tutti i dati utente vengono collegati localmente all'access point. L'accesso alle risorse di rete locali viene mantenuto durante le interruzioni della WAN.

I REAP AP supportano due modalità operative:

- Modalità REAP normale
- Modalità standalone

Il LAP è impostato in modalità REAP normale quando il collegamento WAN tra il REAP AP e il WLC è attivo. Quando i LAP funzionano in modalità REAP normale, possono supportare fino a 16 WLAN.

Quando il collegamento WAN tra il WLC e il LAP si interrompe, il LAP abilitato per il REAP passa alla modalità standalone. In modalità standalone, i REAP LAP possono supportare solo una WLAN in modo indipendente senza il WLC, se la WLAN è configurata con WEP (Wired Equivalent Privacy) o con un metodo di autenticazione locale. In questo caso, la WLAN supportata dal REAP AP è la prima WLAN configurata sull'access point, la WLAN 1. Ciò è dovuto al fatto che la maggior parte degli altri metodi di autenticazione devono passare informazioni al controller e dal controller e, quando il collegamento WAN non è attivo, questa operazione non è possibile. In modalità

standalone, i LAP supportano un numero minimo di funzionalità. Nella tabella seguente vengono mostrate le funzionalità supportate da un REAP LAP in modalità standalone rispetto a quelle supportate da un REAP LAP in modalità normale (quando il collegamento WAN è attivo e la comunicazione con il WLC è attiva):

Funzioni supportate da un REAP LAP in modalità REAP normale e in modalità standalone

		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

Nella tabella viene mostrato che più VLAN non sono supportate sui LAP REAP in entrambe le modalità. L'uso di più VLAN non è supportato perché i LAP REAP possono risiedere solo su una singola subnet perché non possono eseguire il tagging VLAN IEEE 802.1Q. Pertanto, il traffico su ciascuno degli identificatori dei set di servizi (SSID) termina sulla stessa subnet della rete cablata. Di conseguenza, il traffico di dati non viene separato sul lato cablato anche se il traffico wireless

può essere segmentato via etere tra SSID.

Per ulteriori informazioni sulla distribuzione di REAP e su come gestire REAP e le relative limitazioni, consultare la [guida alla distribuzione di REAP presso la filiale](#).

Configurazione

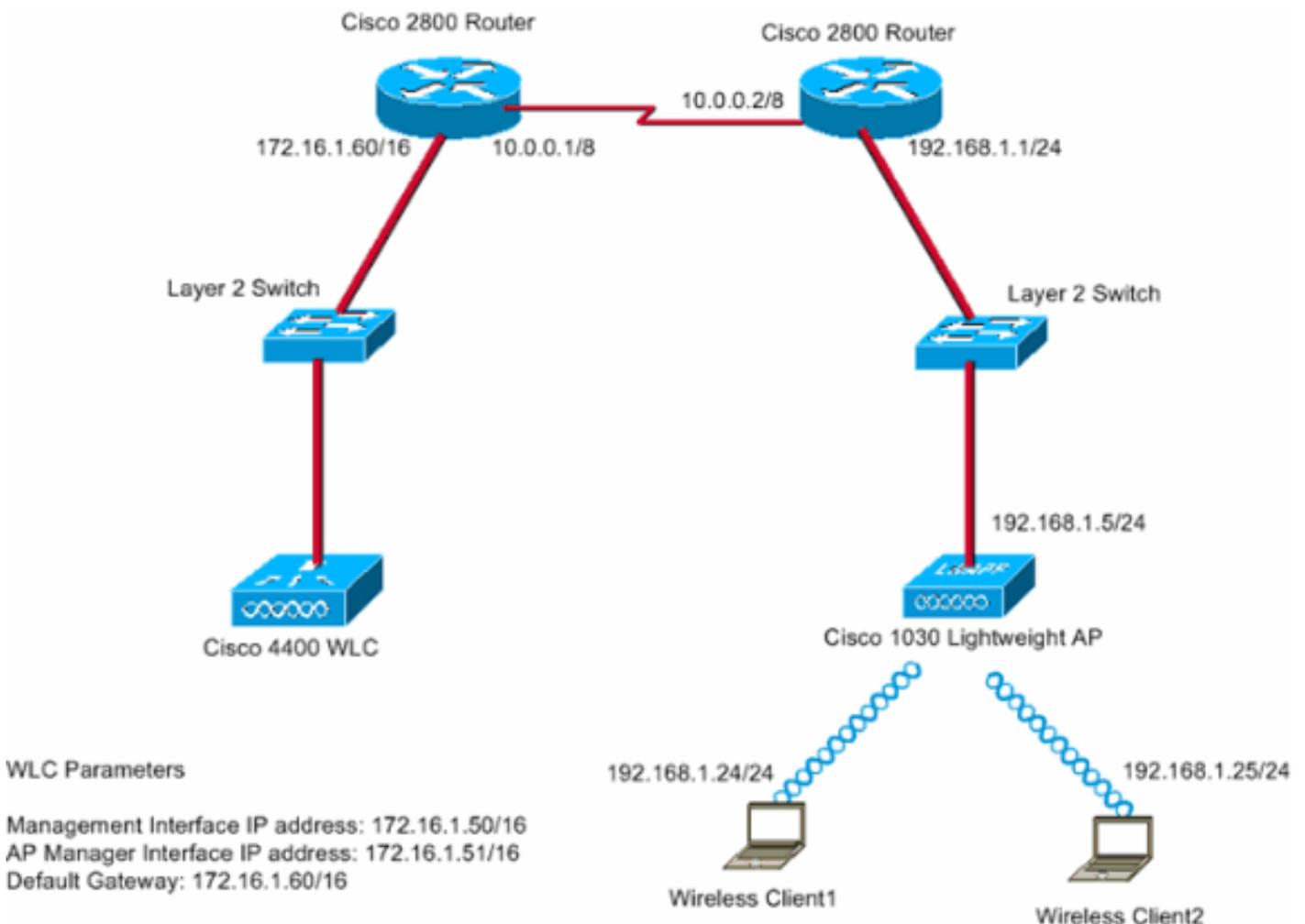
In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

Per configurare i dispositivi in modo da implementare l'impostazione della rete, attenersi alla seguente procedura:

1. [Configurare il WLC per il funzionamento di base e configurare le WLAN](#).
2. [Attivare il punto di accesso per l'installazione sul sito remoto](#).
3. [Configurare i router 2800 per stabilire il collegamento WAN](#).
4. [Distribuire il REAP LAP sul sito remoto](#).

Esempio di rete

Nel documento viene usata questa impostazione di rete:



La sede principale si collega alla succursale utilizzando una linea in leasing. La linea dedicata termina con i router serie 2800 a ciascuna estremità. In questo esempio viene usato il protocollo

Open Shortest Path First (OSPF) per instradare i dati sul collegamento WAN con incapsulamento PPP. Il modello 4400 WLC è installato nell'ufficio principale, mentre il modello 1030 LAP deve essere installato nell'ufficio remoto. Il 1030 LAP deve supportare due WLAN. Di seguito sono riportati i parametri per le WLAN:

- **WLAN 1**SSID: **SSID1**Autenticazione—**Aperta**Crittografia—**TKIP (Temporal Key Integrity Protocol) (chiave precondivisa WPA [WPA-PSK])**
- **WLAN 2**SSID—**SSID2**Autenticazione—**Extensible Authentication Protocol (EAP)**Crittografia—**TKIP****Nota:** per la WLAN 2, la configurazione indicata in questo documento utilizza l'autenticazione WPA (802.1x e TKIP per la crittografia).

È necessario configurare i dispositivi per questa installazione.

[Configurazione del WLC per il funzionamento di base e configurazione delle WLAN](#)

È possibile usare la configurazione guidata di avvio sull'interfaccia della riga di comando (CLI) per configurare il WLC per il funzionamento di base. In alternativa, è possibile usare la GUI per configurare il WLC. Questo documento spiega la configurazione sul WLC con l'uso della configurazione guidata di avvio dalla CLI.

Una volta avviato per la prima volta, il WLC entra direttamente nella configurazione guidata di avvio. La configurazione guidata consente di configurare le impostazioni di base. È possibile eseguire la procedura guidata dalla CLI o dalla GUI. Di seguito è riportato un esempio della configurazione guidata di avvio:

```
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
```

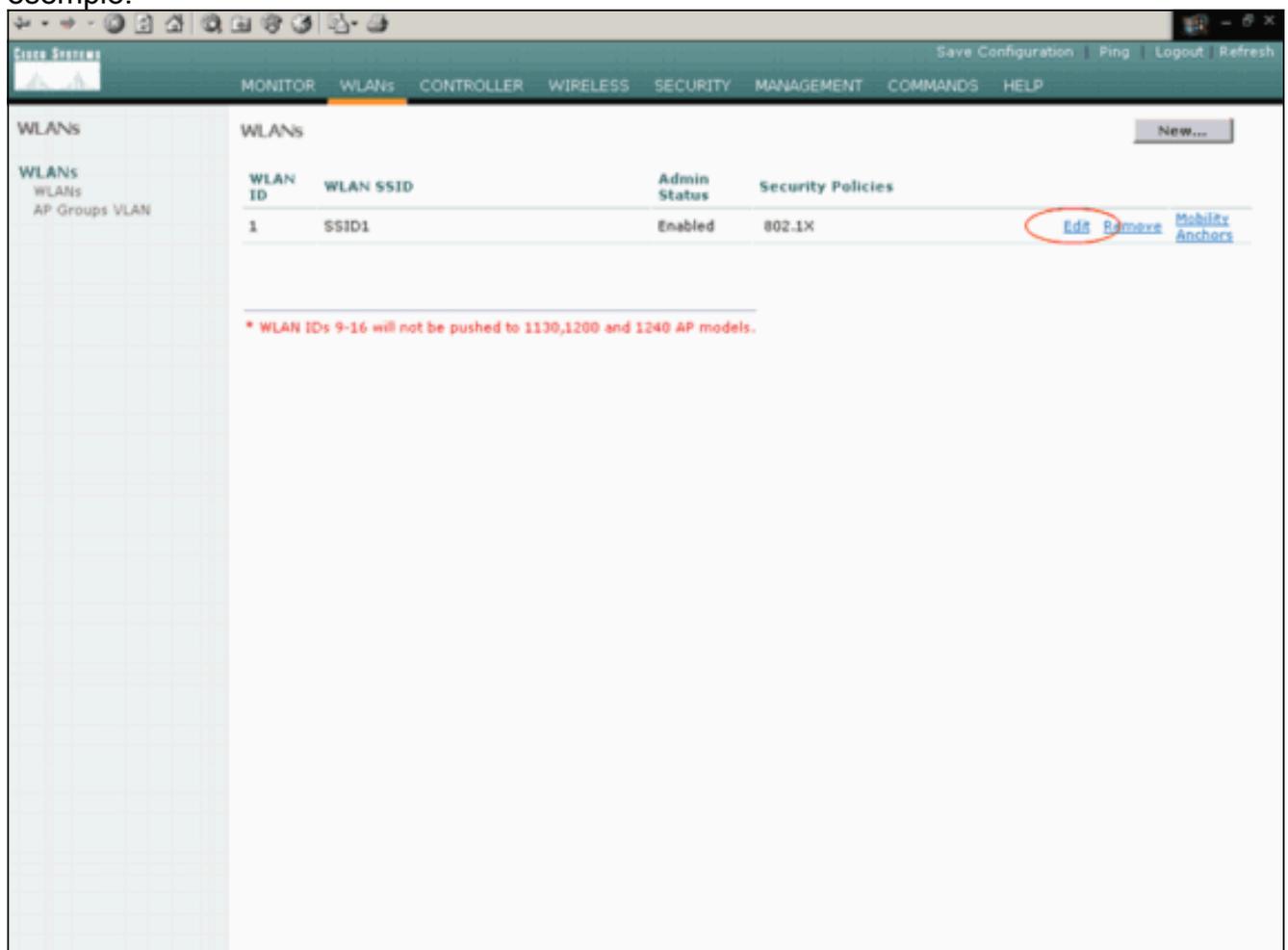
```
Configuration saved!
Resetting system with new configuration...
```

Nell'esempio vengono configurati questi parametri sul WLC:

- Nome sistema
- Indirizzo IP interfaccia di gestione
- Indirizzo IP interfaccia AP-manager
- Numero porta interfaccia di gestione
- Identificatore VLAN dell'interfaccia di gestione
- Nome gruppo di mobilità
- SSID
- Molti altri parametri

Questi parametri vengono utilizzati per impostare il WLC per il funzionamento di base. Come mostrato nell'output del WLC in questa sezione, il WLC usa 172.16.1.50 come indirizzo IP dell'interfaccia di gestione e 172.16.1.51 come indirizzo IP dell'interfaccia del gestore dell'access point. Per configurare le due WLAN per la rete, attenersi alla seguente procedura sul WLC:

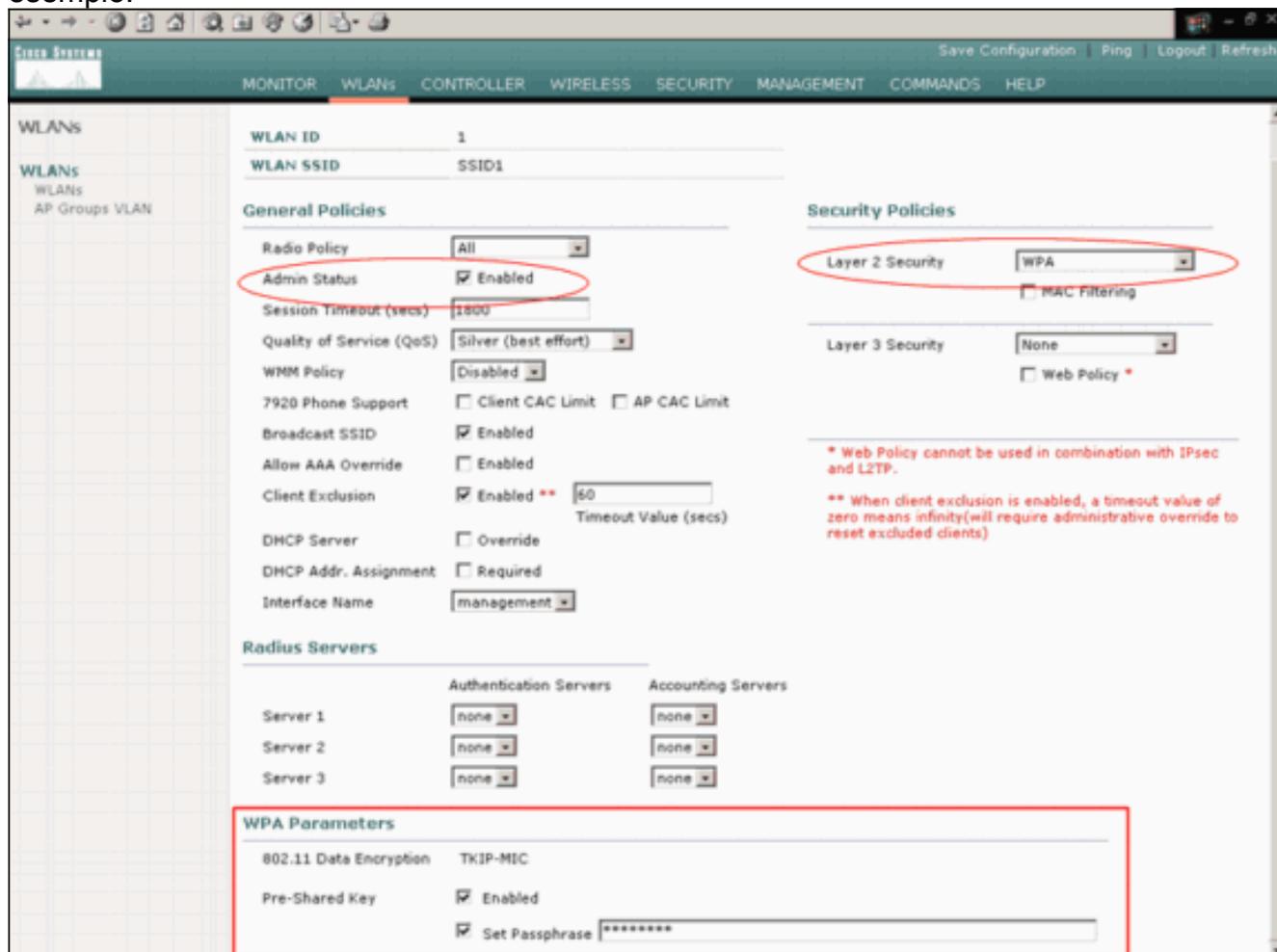
1. Dall'interfaccia utente del WLC, fare clic su **WLAN** nel menu nella parte superiore della finestra. Viene visualizzata la finestra WLAN. In questa finestra vengono elencate le WLAN configurate sul WLC. Poiché è stata configurata una WLAN con la configurazione guidata di avvio, è necessario configurare gli altri parametri per questa WLAN.
2. Fare clic su **Edit** (Modifica) per visualizzare l'SSID1 della WLAN. Di seguito è riportato un esempio:



Viene visualizzata la finestra WLAN > Modifica. In questa finestra è possibile configurare i parametri specifici della WLAN, che includono Criteri generali, Criteri di sicurezza, server RADIUS e altri.

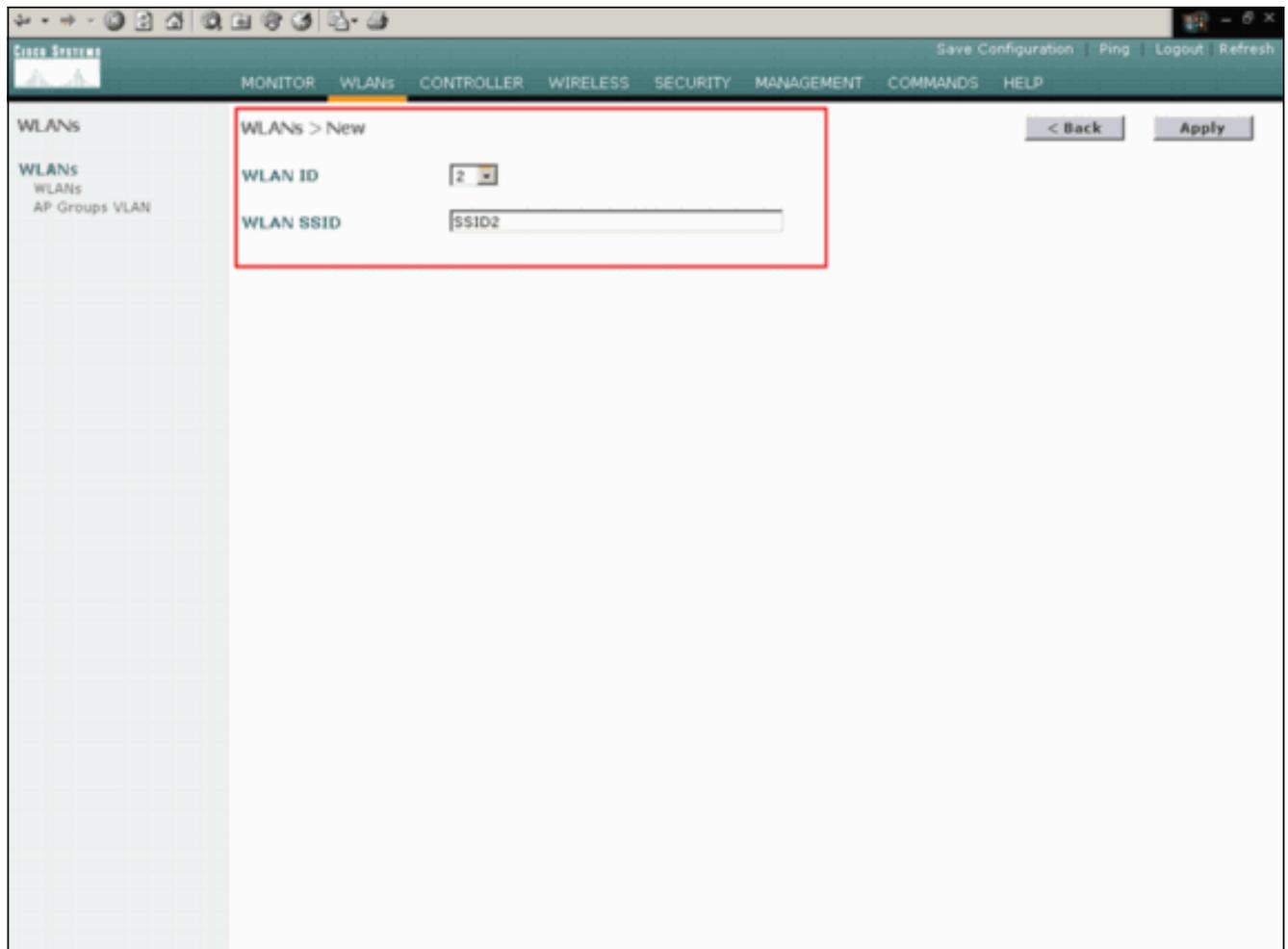
3. Selezionare quanto segue nella finestra WLAN > Modifica: Per abilitare la WLAN, nell'area Criteri generali selezionare la casella di controllo **Abilitato** accanto a Stato amministratore. Per utilizzare WPA per WLAN 1, selezionare **WPA** dal menu a discesa Sicurezza di layer

2. Definire i parametri WPA nella parte inferiore della finestra. Per utilizzare WPA-PSK sulla WLAN 1, selezionare la casella di controllo **Abilitato** accanto a Chiave già condivisa nell'area Parametri WPA e immettere la passphrase per WPA-PSK. WPA-PSK utilizzerà TKIP per la crittografia. **Nota:** affinché WPA-PSK funzioni, la passphrase WPA-PSK deve corrispondere a quella configurata sull'adattatore client. Fare clic su **Apply** (Applica). Di seguito è riportato un esempio:



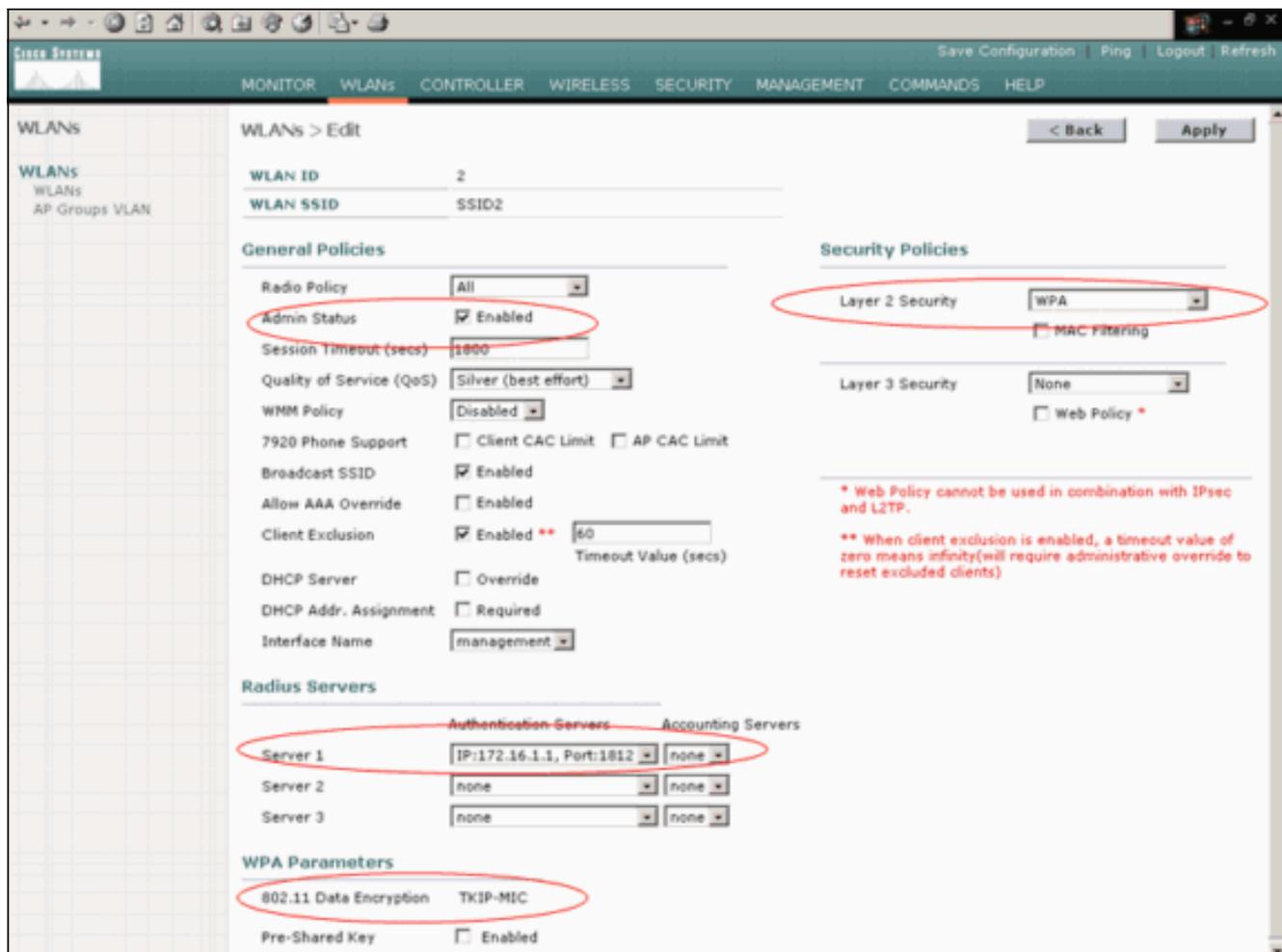
La WLAN 1 è stata configurata per la crittografia WPA-PSK.

4. Per definire la WLAN 2, fare clic su **New** (Nuovo) nella finestra WLAN. Viene visualizzata la finestra WLAN > Nuovo.
5. Nella finestra WLAN > Nuovo, definire l'ID WLAN e l'SSID della WLAN, quindi fare clic su **Applica**. Di seguito è riportato un esempio:



Viene visualizzata la finestra WLAN > Modifica per la seconda WLAN.

6. Selezionare quanto segue nella finestra WLAN > Modifica: Per abilitare la WLAN, nell'area Criteri generali selezionare la casella di controllo **Abilitato** accanto a Stato amministratore. Per configurare WPA per questa WLAN, scegliere **WPA** dal menu a discesa Sicurezza di layer 2. Nell'area Server Radius scegliere il server RADIUS appropriato da utilizzare per l'autenticazione dei client. Fare clic su **Apply** (Applica). Di seguito è riportato un esempio:



Nota: in questo documento non viene spiegato come configurare i server RADIUS e l'autenticazione EAP. Per informazioni su come configurare l'autenticazione EAP con i WLC, fare riferimento all'[esempio di configurazione dell'autenticazione EAP con i controller WLAN \(WLC\)](#).

[Prime the AP per l'installazione sul sito remoto](#)

Il priming è un processo tramite il quale i LAP ottengono un elenco di controller a cui possono connettersi. I LAP vengono informati di tutti i controller del gruppo di mobilità non appena si collegano a un unico controller. In questo modo, i LAP imparano tutte le informazioni di cui hanno bisogno per unirsi a qualsiasi controller del gruppo.

Per configurare un access point compatibile con il protocollo REAP, collegarlo alla rete cablata dell'ufficio principale. Questa connessione consente all'access point di rilevare un singolo controller. Quando il LAP si unisce al controller dell'ufficio principale, il punto di accesso scarica la versione del sistema operativo (OS) del punto di accesso che corrisponde all'infrastruttura WLAN e alla configurazione. Gli indirizzi IP di tutti i controller nel gruppo di mobilità vengono trasferiti nell'access point. Quando l'access point ha tutte le informazioni di cui ha bisogno, può essere connesso alla postazione remota. L'access point può quindi rilevare e unirsi al controller meno utilizzato dell'elenco, se è disponibile la connettività IP.

Nota: accertarsi di impostare i punti di accesso in modalità "REAP" prima di disattivarli per spedirli ai siti remoti. È possibile impostare la modalità a livello AP dalla CLI o dalla GUI del controller oppure utilizzando i modelli Wireless Control System (WCS). Per impostazione predefinita, gli access point sono impostati in modo da eseguire le normali funzionalità "locali".

I LAP possono usare uno qualsiasi di questi metodi per rilevare il controller:

- Individuazione di livello 2
- Individuazione di livello 3 Con l'utilizzo di una subnet broadcast locale Con l'opzione DHCP 43 Con l'utilizzo di un server DNS Con l'utilizzo del provisioning over-the-air (OTAP) Con l'uso di un server DHCP interno **Nota:** per utilizzare un server DHCP interno, il LAP deve connettersi direttamente al WLC.

in questo documento si presume che il LAP si registri sul WLC usando il meccanismo di rilevamento dell'opzione DHCP 43. Per ulteriori informazioni sull'uso dell'opzione DHCP 43 per registrare il LAP sul controller e altri meccanismi di rilevamento, consultare il documento sulla [registrazione di un Lightweight AP \(LAP\) su un Wireless LAN Controller \(WLC\)](#).

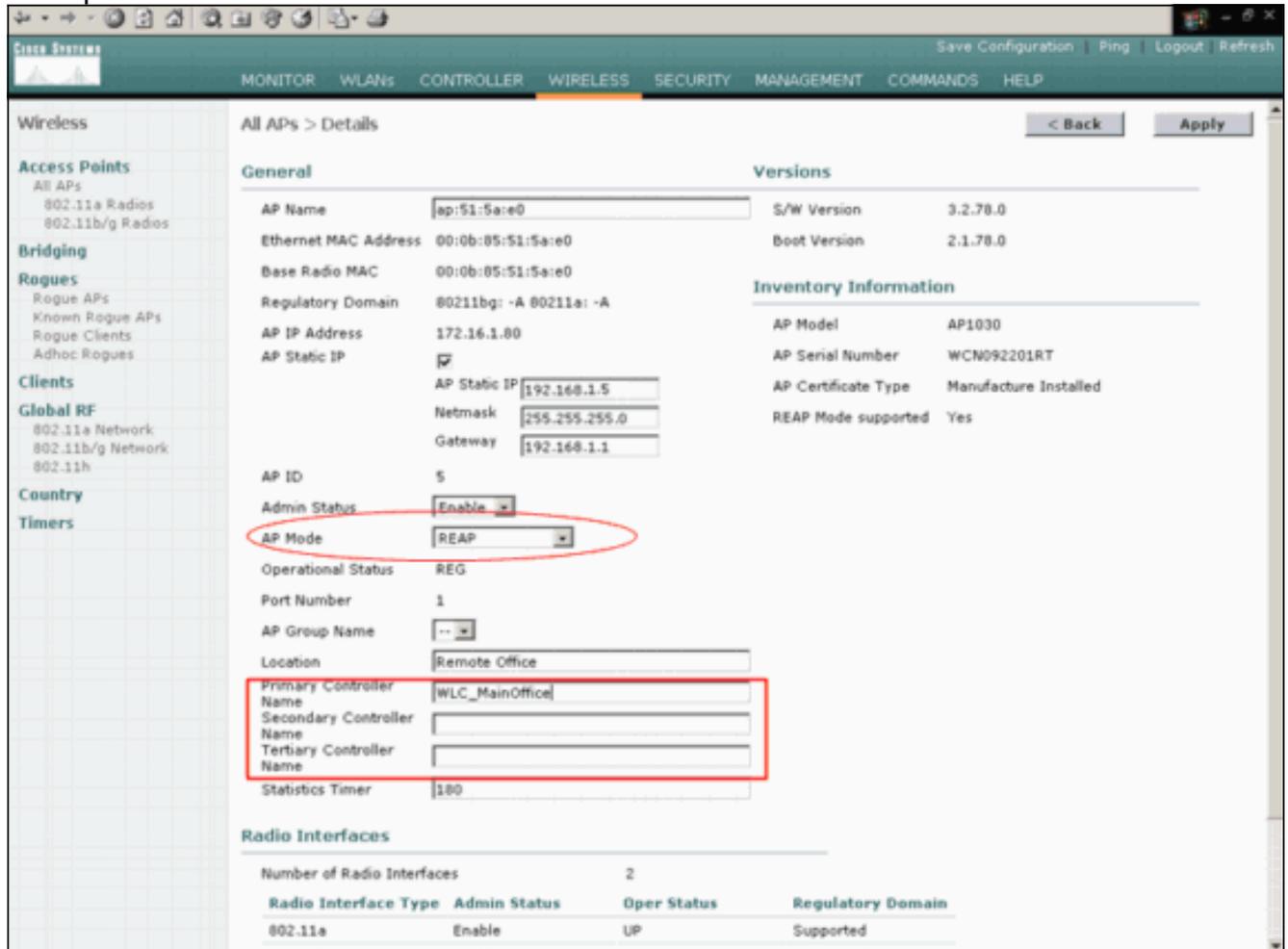
Quando il LAP rileva il controller, si osserverà che l'AP è registrato sul controller nella finestra Wireless del WLC. Di seguito è riportato un esempio:

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	Detail

Completare questa procedura per configurare il LAP per la modalità REAP normale:

1. Dall'interfaccia utente del WLC, fare clic su **Wireless**. Viene visualizzata la finestra Tutti gli access point. In questa finestra vengono elencati gli AP registrati sul WLC.
2. Selezionare l'access point da configurare per la modalità REAP e fare clic su **Detail**. Viene visualizzata la finestra Tutti gli access point > Dettagli per l'access point specifico. In questa finestra è possibile configurare i vari parametri dell'access point, tra cui: Nome punto di accesso Indirizzo IP (che può essere modificato in statico) Stato amministratore Parametri di protezione Modalità AP Elenco dei WLC a cui l'access point può connettersi Altri parametri
3. Scegliere **REAP** dal menu a discesa Modalità AP. Questa modalità è disponibile solo sui punti di accesso compatibili con il protocollo REAP.

4. Definire i nomi dei controller che gli access point utilizzeranno per registrare e fare clic su **Apply** (Applica). È possibile definire fino a tre nomi di controller (primario, secondario e terziario). Gli access point ricercano il controller nell'ordine specificato in questa finestra. Poiché in questo esempio viene utilizzato un solo controller, il controller viene definito come controller primario. Di seguito è riportato un esempio:



Il punto di accesso è stato configurato per la modalità REAP e può essere distribuito nel sito remoto.

Nota: nell'esempio, è possibile notare che l'indirizzo IP dell'access point è stato modificato in statico e che è stato assegnato un indirizzo IP statico 192.168.1.5. Questa assegnazione viene eseguita perché si tratta della subnet da utilizzare nell'ufficio remoto. L'indirizzo IP del server DHCP, 172.16.1.80, viene quindi utilizzato solo durante la fase di priming. Dopo aver registrato l'access point sul controller, è possibile modificare l'indirizzo in un indirizzo IP statico.

[Configurazione dei router 2800 per stabilire il collegamento WAN](#)

Per stabilire il collegamento WAN, nell'esempio vengono utilizzati due router serie 2800 con OSPF per indirizzare le informazioni tra le reti. Di seguito è riportata la configurazione di entrambi i router per lo scenario di esempio:

```

UfficioPrincipale
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

```

Filiale

```

BranchOffice#show run
Building configuration...

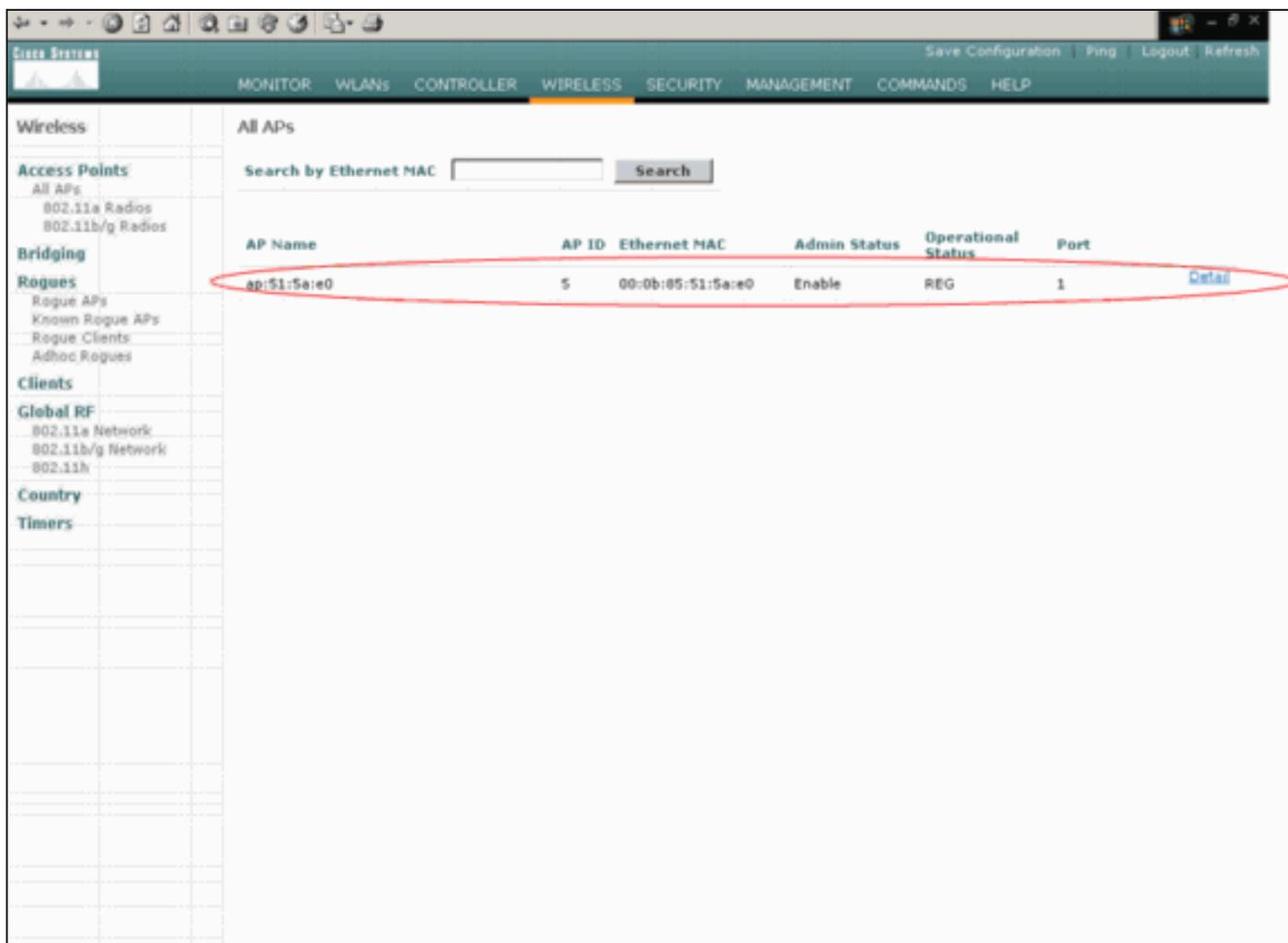
Current configuration : 596 bytes
!
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname BranchOffice
!
!
ip subnet-zero
!
!
!
!
interface Ethernet0
 ip address 192.168.1.1 255.255.255.0
 !--- This is the interface which acts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

```

Distribuire il punto di accesso REAP sul sito remoto

Dopo aver configurato le WLAN sui WLC, avviato il LAP e stabilito il collegamento WAN tra l'ufficio principale e l'ufficio remoto, è possibile installare l'AP sul sito remoto.

Dopo aver acceso l'access point sul sito remoto, l'access point cerca il controller nell'ordine configurato nella fase di attivazione. Una volta individuato il controller, l'access point si registra presso il controller. Ecco un esempio. Dal WLC, è possibile vedere che l'AP è stato collegato al controller sulla porta 1:



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	Detail

I client con SSID **SSID1** e per i quali è abilitata WPA-PSK, vengono associati all'access point sulla WLAN 1. I client con SSID **SSID2** e con l'autenticazione 802.1x abilitata, vengono associati all'access point sulla WLAN 2. Di seguito è riportato un esempio che mostra due client. Un client è connesso alla WLAN 1 e l'altro alla WLAN 2:

The screenshot shows the Cisco WLC GUI with the 'Clients' page selected. The table below is a representation of the data shown in the GUI.

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

Verifica

Per verificare che la configurazione REAP funzioni correttamente, consultare questa sezione.

Nota: consultare le [informazioni importanti sui comandi di debug](#) prima di usare i comandi di debug.

Abbassare il collegamento WAN. Quando il collegamento WAN non è attivo, l'access point perde la connettività con il WLC. Il WLC quindi annulla la registrazione dell'AP dall'elenco. Di seguito è riportato un esempio:

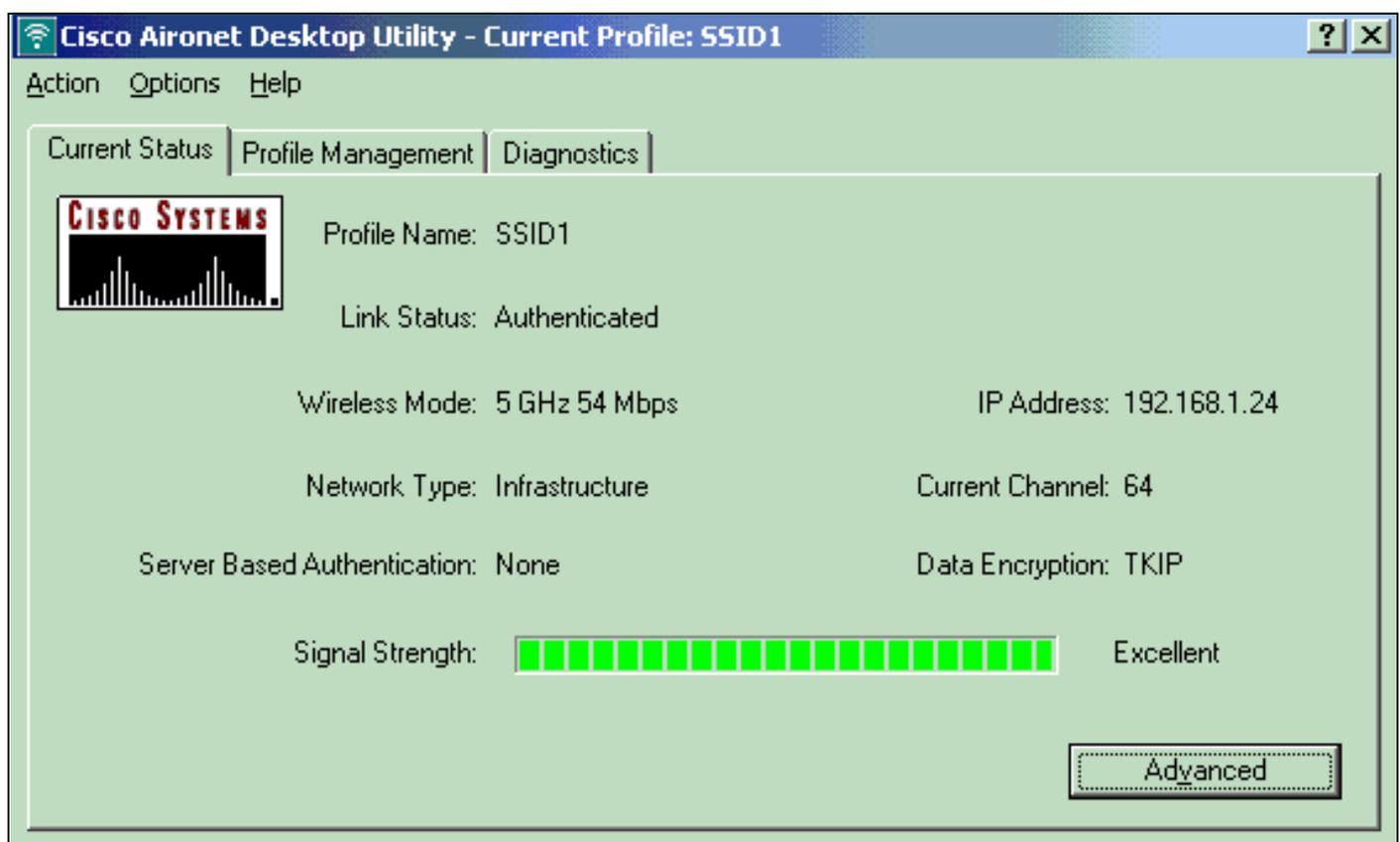
```
(Cisco Controller) >debug lwapp events enable
Wed May 17 15:04:22 2006: Did not receive heartbeat reply from AP 00:0B:85:51:5A:E0
Wed May 17 15:04:22 2006: Max retransmissions reached on AP 00:0B:85:51:5A:E0
(CONFIGURE_COMMAND, 1)
Wed May 17 15:04:22 2006: apfSpamProcessStateChangeInSpamContext: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

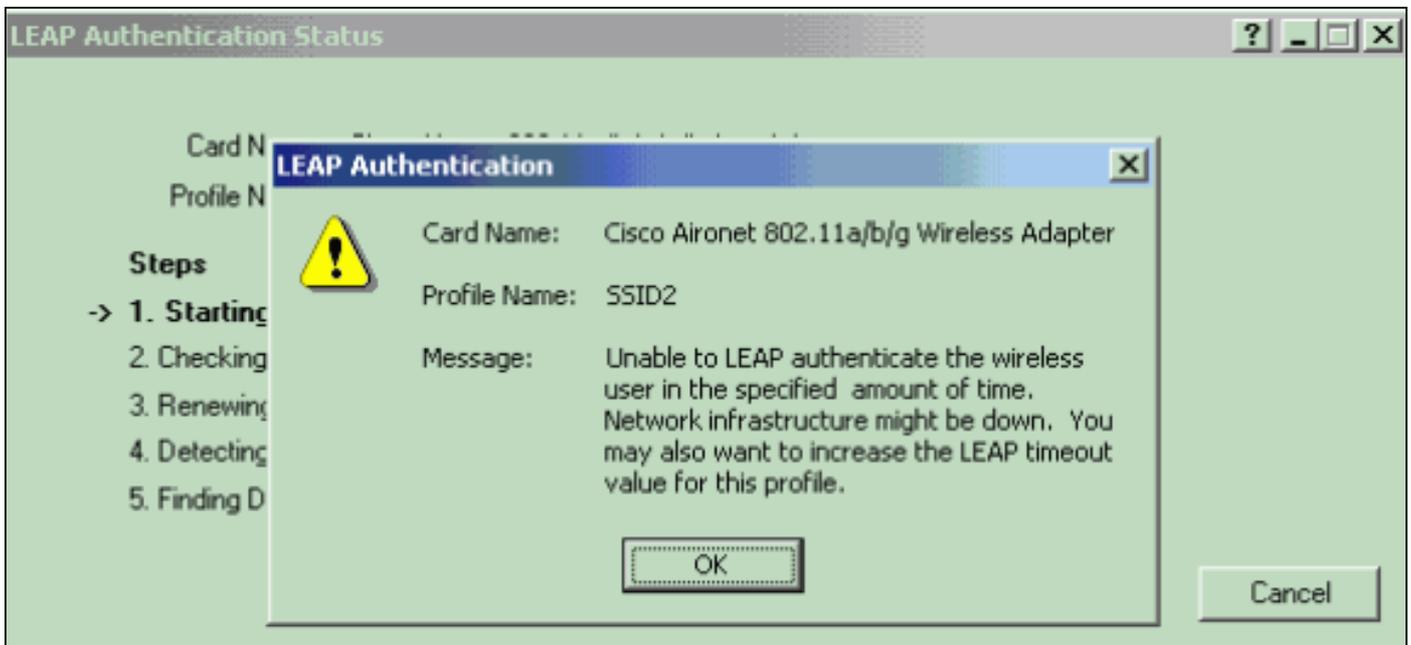
Come si evince dall'output del comando **debug lwapp events enable**, il WLC annulla la registrazione dell'access point in quanto non ha ricevuto una risposta heartbeat dall'access point. Una risposta heartbeat è simile ai messaggi keepalive. Il controller prova cinque heartbeat consecutivi, a un secondo l'uno dall'altro. Se il WLC non riceve una risposta, annulla la registrazione dell'AP.

Quando l'access point è in modalità standalone, il LED di alimentazione dell'access point lampeggia. I client associati alla prima WLAN (WLAN 1) sono ancora associati all'access point perché i client della prima WLAN sono configurati solo per la crittografia WPA-PSK. Il LAP gestisce la crittografia in modalità standalone. Di seguito è riportato un esempio che mostra lo stato (quando il collegamento WAN non è attivo) di un client connesso alla WLAN 1 con SSID1 e WPA-PSK:

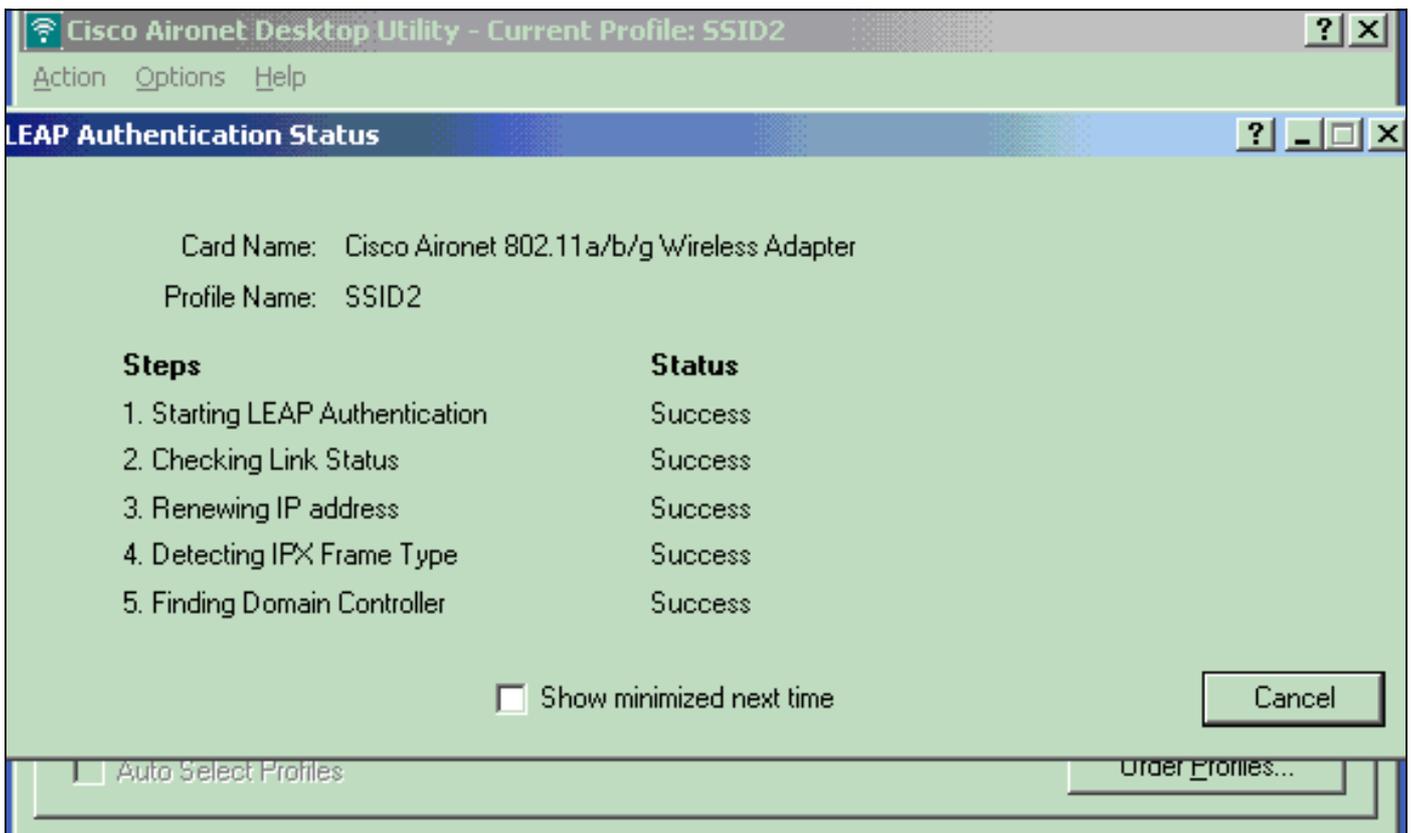
Nota: TKIP è la crittografia utilizzata con WPA-PSK.



I client connessi alla WLAN 2 vengono disconnessi perché la WLAN 2 utilizza l'autenticazione EAP. Questa disconnessione si verifica perché i client che utilizzano l'autenticazione EAP devono comunicare con il WLC. Di seguito è riportata una finestra di esempio che mostra che l'autenticazione EAP non riesce quando il collegamento WAN è inattivo:



Quando il collegamento WAN è attivo, il punto di accesso torna alla modalità REAP normale e si registra con il controller. Viene visualizzato anche il client che utilizza l'autenticazione EAP. Di seguito è riportato un esempio:



In questo output di esempio del comando **debug lwapp events enable** sul controller vengono visualizzati i seguenti risultati:

```
(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
```

[Risoluzione dei problemi](#)

Utilizzare questa sezione per risolvere i problemi relativi alla configurazione.

[Comandi per la risoluzione dei problemi](#)

È possibile utilizzare questi comandi di **debug** per risolvere i problemi relativi alla configurazione.

Nota: consultare le [informazioni importanti sui comandi di debug](#) prima di usare i comandi di debug.

- **debug lwapp events enable:** visualizza la sequenza di eventi verificatisi tra il LAP e il WLC.
- **debug lwapp errors enable:** visualizza gli errori che si verificano nella comunicazione LWAPP.
- **debug lwapp packet enable:** visualizza il debug di una traccia di pacchetto LWAPP.
- **debug mac addr:** abilita il debug MAC per il client specificato.

[Informazioni correlate](#)

- [Guida alla distribuzione di REAP presso le filiali](#)
- [Esempio di configurazione dell'autenticazione EAP con i controller WLAN \(WLC\)](#)
- [Esempio di configurazione base di Wireless LAN Controller e Lightweight Access Point](#)
- [Esempio di configurazione del failover del controller WLAN per i Lightweight Access Point](#)
- [Pagina di supporto wireless](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)