Configurazione di Aironet serie 600 OfficeExtend Access Point

Sommario

Introduzione

In questo documento vengono fornite informazioni sui requisiti per configurare un controller Cisco Wireless LAN (WLAN) per l'utilizzo con Cisco Aironet® serie 600 OfficeExtend Access Point (OEAP). Cisco Aironet serie 600 OEAP supporta la modalità split e dispone di funzionalità che richiedono configurazione tramite il controller WLAN e funzionalità che possono essere configurate localmente dall'utente finale. Nel documento vengono fornite anche informazioni sulle configurazioni necessarie per una connessione corretta e sui set di funzionalità supportati.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Per la stesura del documento, è stato usato Cisco Aironet serie 600 OfficeExtend Access Point (OEAP).

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

Linee guida per l'installazione

- Cisco Aironet serie 600 OEAP è supportato su questi controller: Cisco 5508, WiSM-2 e Cisco 2504.
- La prima versione del controller che supporta Cisco Aironet serie 600 OEAP è 7.0.116.0
- Le interfacce di gestione del controller devono trovarsi su una rete IP instradabile.
- Ènecessario modificare la configurazione del firewall aziendale per consentire il traffico con i numeri di porta UDP **5246** e **5247**.

Cenni preliminari su Office Extend Solution

- A un utente viene fornito un punto di accesso (AP) con l'indirizzo IP del controller aziendale oppure l'utente può immettere l'indirizzo IP del controller dalla schermata di configurazione (pagine HTML di configurazione).
- L'utente collega l'access point al router di casa.
- L'access point riceve un indirizzo IP dal router di origine, si unisce al controller innescato e crea un tunnel protetto.
- Cisco Aironet serie 600 OEAP quindi annuncia l'SSID aziendale, che estende gli stessi metodi e servizi di sicurezza attraverso la WAN alla home dell'utente.
- Se è stata configurata la LAN remota, una porta cablata sull'access point viene ricollegata tramite tunneling al controller.
- L'utente può quindi abilitare un SSID locale aggiuntivo per uso personale.

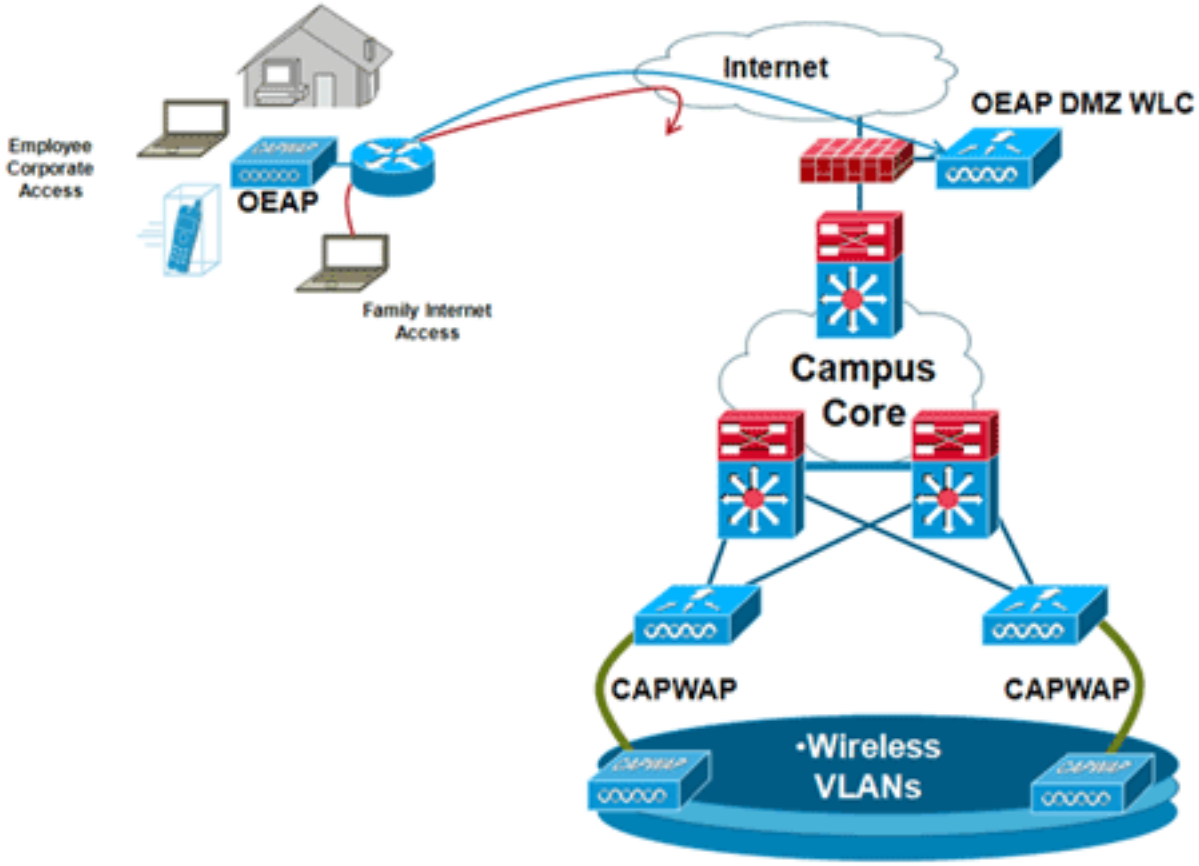
Linee guida per la configurazione del firewall

La configurazione generale sul firewall consente il controllo CAPWAP e i numeri delle porte di

gestione CAPWAP attraverso il firewall. Il controller Cisco Aironet serie 600 OEAP può essere posizionato nella zona DMZ.

Nota: è necessario aprire le porte UDP **5246** e **5247** sul firewall tra il controller WLAN e il Cisco Aironet serie 600 OEAP.

Il diagramma mostra un Cisco Aironet serie 600 OEAP controller sulla DMZ:



Di seguito è riportato un esempio di configurazione del firewall:

```
interface Ethernet0/0
 nameif outside
 security-level 0
 ip address X.X.X.X 255.255.255.224
!--- X.X.X.X represents a public IP address ! interface Ethernet0/2 nameif dmz security-level 50
ip address 172.16.1.2 255.255.255.0 ! access-list Outside extended permit udp any host X.X.X.Y
eq 5246 !--- Public reachable IP of corporate controller access-list Outside extended permit udp
any host X.X.X.Y eq 5247 !--- Public reachable IP of corporate controller access-list Outside
extended permit icmp any any ! global (outside) 1 interface nat (dmz) 1 172.16.1.0 255.255.255.0
static (dmz,outside) X.X.X.Y 172.16.1.25 netmask 255.255.255.255 access-group Outside in
interface outside
```

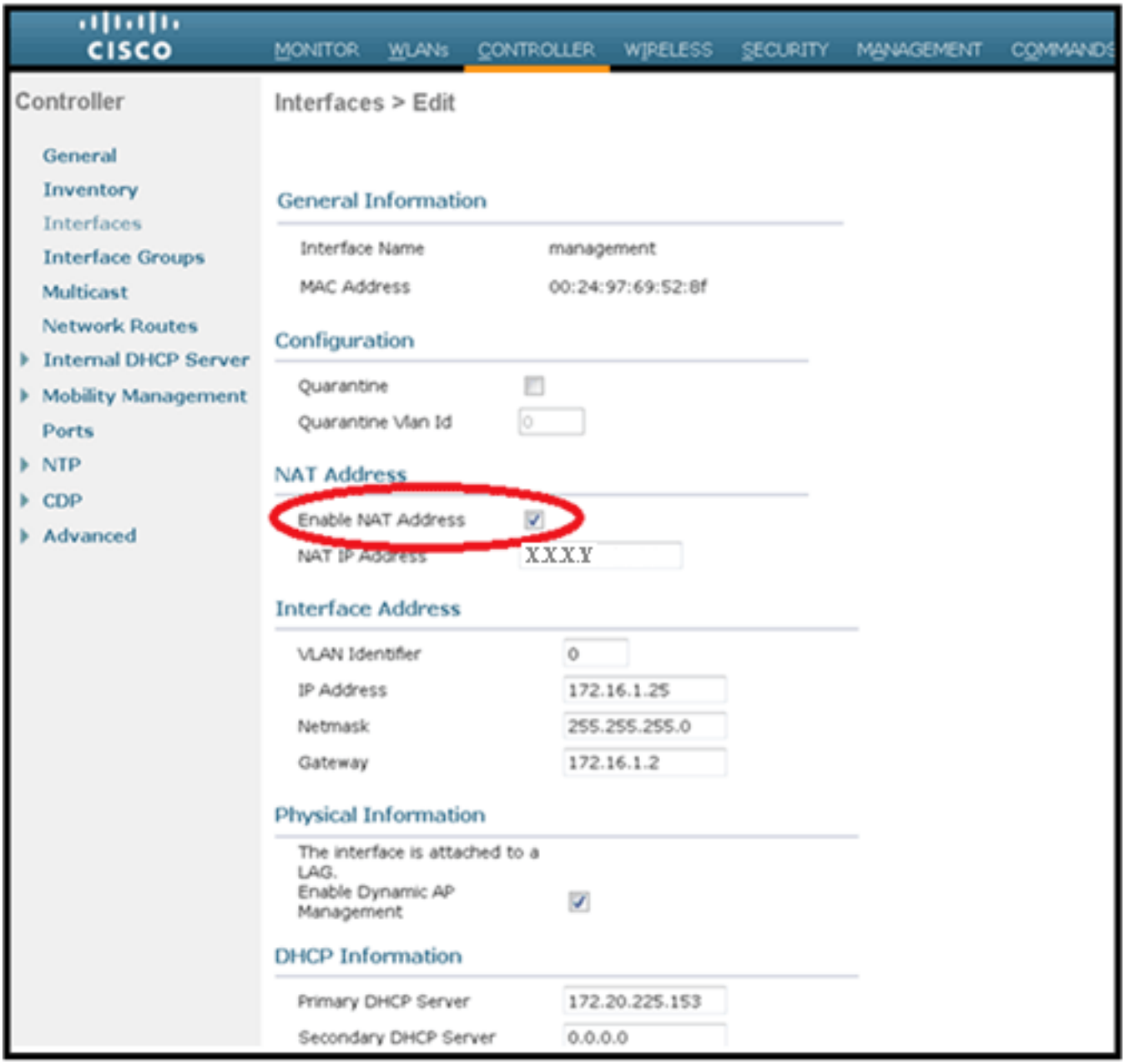
Per trasmettere l'indirizzo IP interno di AP-Manager all'access point OfficeExtend come parte del pacchetto CAPWAPP Discovery Response, l'amministratore del controller deve accertarsi che NAT sia abilitato nell'interfaccia di AP-Manager e che l'indirizzo IP NAT corretto sia inviato all'access point.

Nota: per impostazione predefinita, il WLC risponderà con l'indirizzo IP NAT solo durante il rilevamento dell'access point quando il protocollo NAT è abilitato. Se esistono access point all'interno e all'esterno del gateway NAT, usare questo comando per impostare il WLC in modo che risponda sia con l'indirizzo IP NAT che con l'indirizzo IP di gestione (interno) non NAT:

```
config network ap-discovery nat-ip-only disable
```

Nota: questo campo è obbligatorio solo se il WLC ha un indirizzo IP NAT.

Nel diagramma viene mostrato come il protocollo NAT sia abilitato, presupponendo che il WLC abbia un indirizzo IP NAT:



Nota: questa configurazione non è richiesta nel controller se è configurato con un indirizzo IP instradabile Internet e non dietro un firewall.

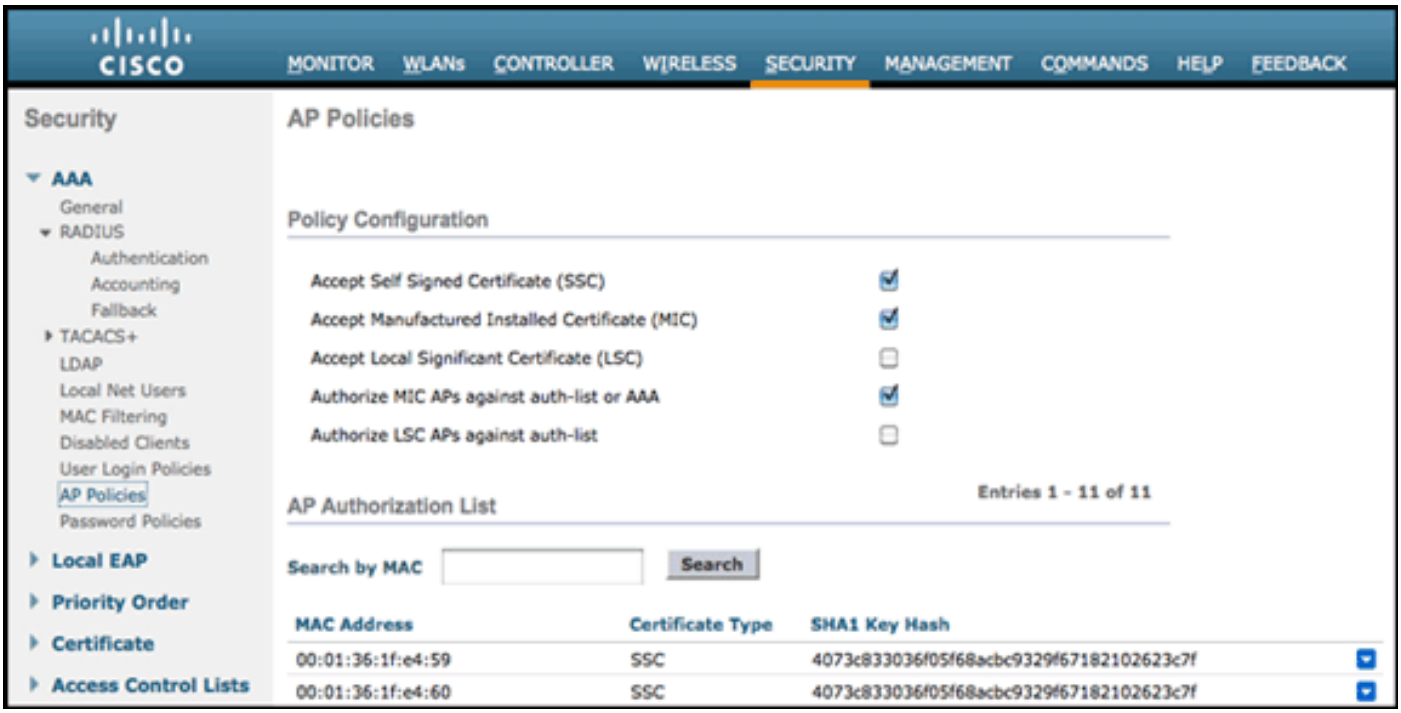
Passaggi di configurazione di Office Extend AP-600

Cisco Aironet serie 600 OEAP si collegherà al WLC come punto di accesso in modalità locale.

Nota: le modalità Monitor, H-REAP, Sniffer, Rogue Detection, Bridge e SE-Connect non sono supportate nella serie 600 e non sono configurabili.

Nota: la funzionalità OEAP di Cisco Aironet serie 600 nei punti di accesso serie 1040, 1130, 1140 e 3502i richiede la configurazione dei punti di accesso per il punto di accesso ibrido REAP (H-REAP) e l'impostazione della modalità secondaria per il punto di accesso su Cisco Aironet serie 600 OEAP. Questa operazione non viene effettuata con la serie 600 in quanto utilizza la modalità locale e non può essere modificata.

Il filtro MAC può essere usato nell'autenticazione dell'access point durante il processo di join iniziale per impedire che unità Cisco Aironet serie 600 OEAP non autorizzate si uniscano al controller. In questa immagine viene mostrato dove abilitare il filtro MAC e configurare i criteri di sicurezza AP:



L'indirizzo MAC Ethernet (non l'indirizzo MAC Radio) viene immesso qui. Inoltre, se si immette l'indirizzo MAC in un server Radius, è necessario utilizzare lettere minuscole. È possibile esaminare il registro eventi AP per informazioni su come individuare l'indirizzo MAC Ethernet (ulteriori informazioni al riguardo sono disponibili più avanti).

Impostazioni di configurazione WLAN e LAN remota

Esiste una porta LAN remota fisica (porta gialla n. 4) su Cisco Aironet serie 600 OEAP. La configurazione della WLAN è molto simile a quella della WLAN. Tuttavia, non essendo wireless e non essendo una porta LAN cablata sul pannello posteriore dell'access point, viene chiamata in uscita e gestita come porta LAN remota.

Sebbene sul dispositivo sia presente una sola porta fisica, è possibile connettere fino a quattro client cablati se si utilizza un hub o uno switch.

Nota: il limite del client LAN remoto supporta la connessione di uno switch o di un hub alla porta LAN remota per più dispositivi o la connessione diretta a un telefono IP Cisco collegato a tale porta.

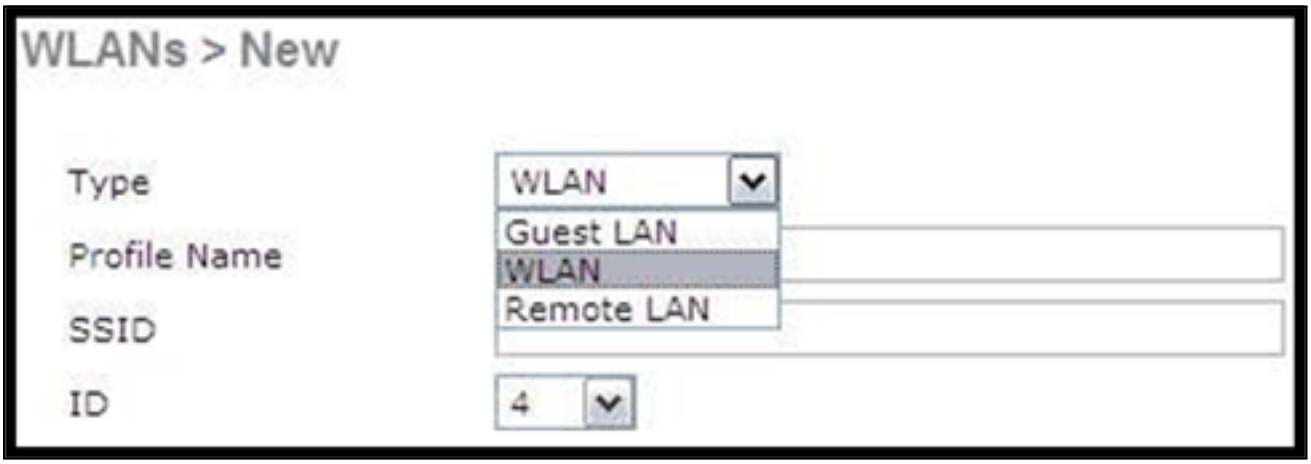
Nota: solo i primi quattro dispositivi possono connettersi finché uno di essi non rimane inattivo per più di un minuto. Se si utilizza l'autenticazione 802.1x, potrebbero verificarsi problemi durante il tentativo di utilizzare più client sulla porta cablata.

Nota: questo numero non influisce sul limite di 15 bit imposto per le WLAN del controller.

Una LAN remota è configurata in modo simile a una WLAN e a una LAN guest configurate sul controller.

Le WLAN sono profili di sicurezza wireless. Questi sono i profili utilizzati dalla rete aziendale. Cisco Aironet serie 600 OEAP supporta al massimo due WLAN e una LAN remota.

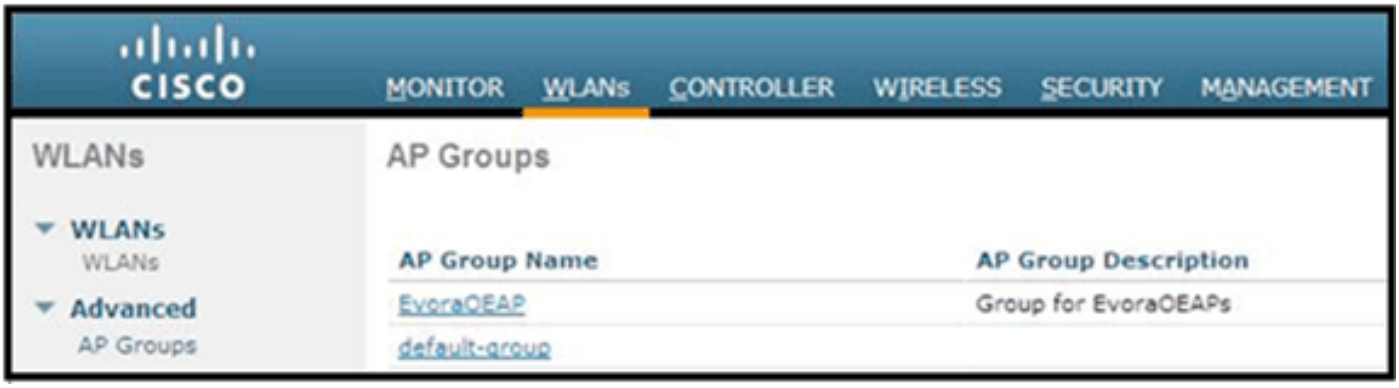
Una LAN remota è simile a una WLAN, con la differenza che è mappata alla porta cablata sul retro del punto di accesso (porta #4 in giallo), come mostrato nell'immagine:



Nota: se si hanno più di due WLAN o più di una LAN remota, è necessario posizionare tutte le WLAN in un gruppo AP.

L'immagine mostra dove vengono configurate le WLAN e la LAN remota:

Nell'immagine viene mostrato un esempio di nome di gruppo OEAP:



L'immagine mostra un SSID WLAN e una configurazione RLAN:

Se si immette il Cisco Aironet serie 600 OEAP in un gruppo AP, la configurazione del gruppo AP è soggetta agli stessi limiti di due WLAN e di una LAN remota. Inoltre, se il Cisco Aironet serie 600 OEAP è nel gruppo predefinito, ossia non è in un gruppo AP definito, gli ID della WLAN/LAN remota devono essere impostati su un valore inferiore all'ID 8 in quanto questo prodotto non supporta gli ID più alti.

Mantieni ID impostato su un valore inferiore a 8, come mostrato nell'immagine:

Nota: se si creano altre WLAN o LAN remote con l'intento di modificare le WLAN o le LAN remote usate dal Cisco Aironet serie 600 OEAP, disabilitare le WLAN o le LAN remote correnti che si stanno rimuovendo prima di abilitare le nuove WLAN o le LAN remote sulla serie 600. Se per un gruppo AP sono abilitate più LAN remote, disabilitarle tutte e quindi abilitarne solo una.

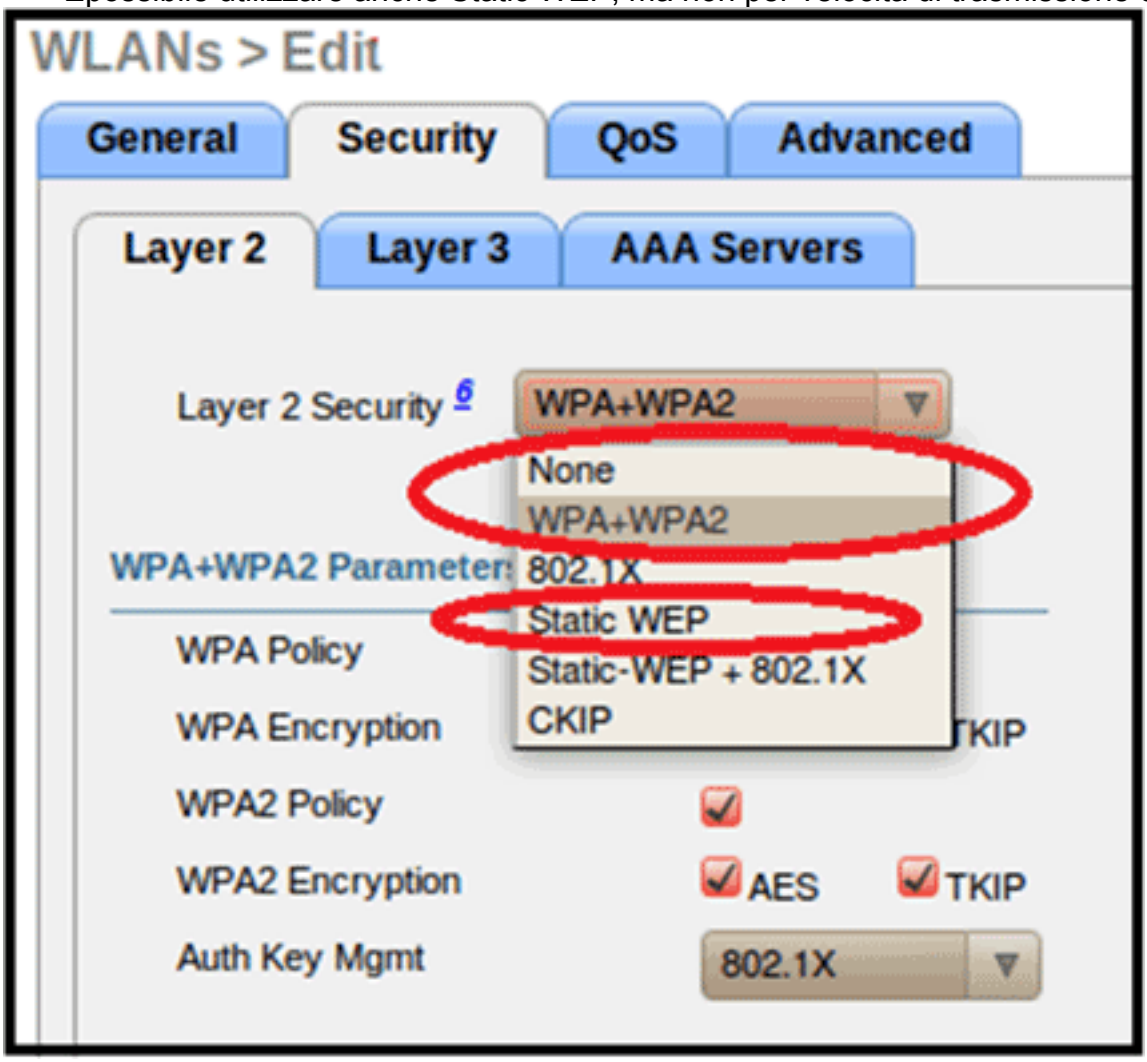
Se per un gruppo AP sono abilitate più di due WLAN, disabilitare tutte le WLAN e abilitarne solo due.

Impostazioni di sicurezza WLAN

Quando si imposta l'impostazione di sicurezza nella WLAN, sono presenti elementi specifici non supportati nella serie 600.

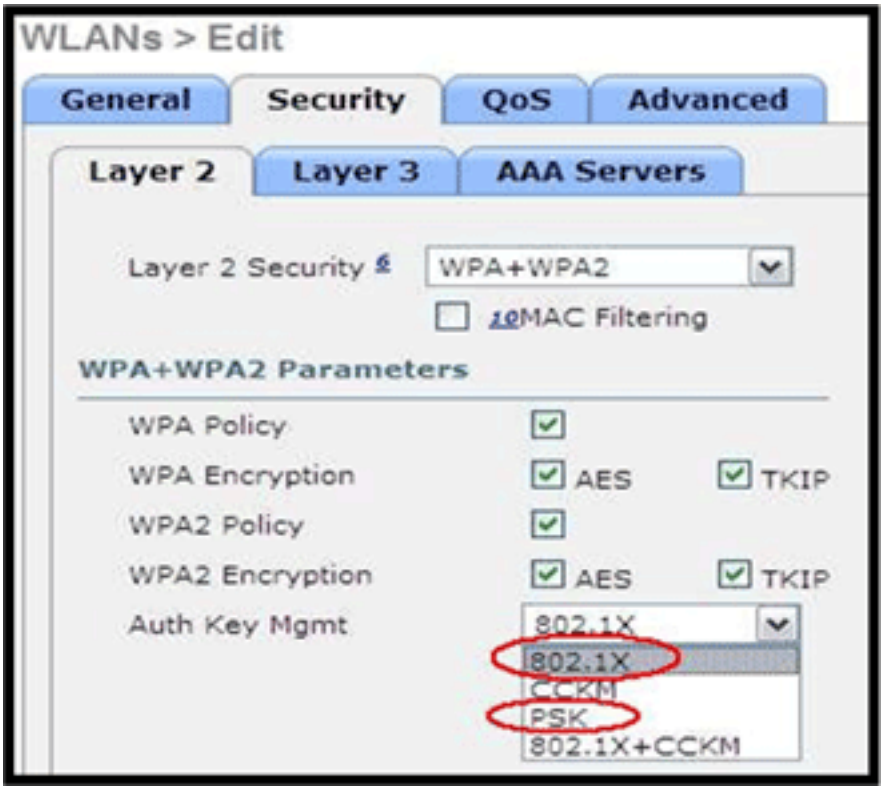
Per la sicurezza di layer 2, solo queste opzioni sono supportate per Cisco Aironet serie 600 OEAP:

- Nessuna
- WPA+WPA2
- Èpossibile utilizzare anche Static WEP, ma non per velocità di trasmissione dati .11n.

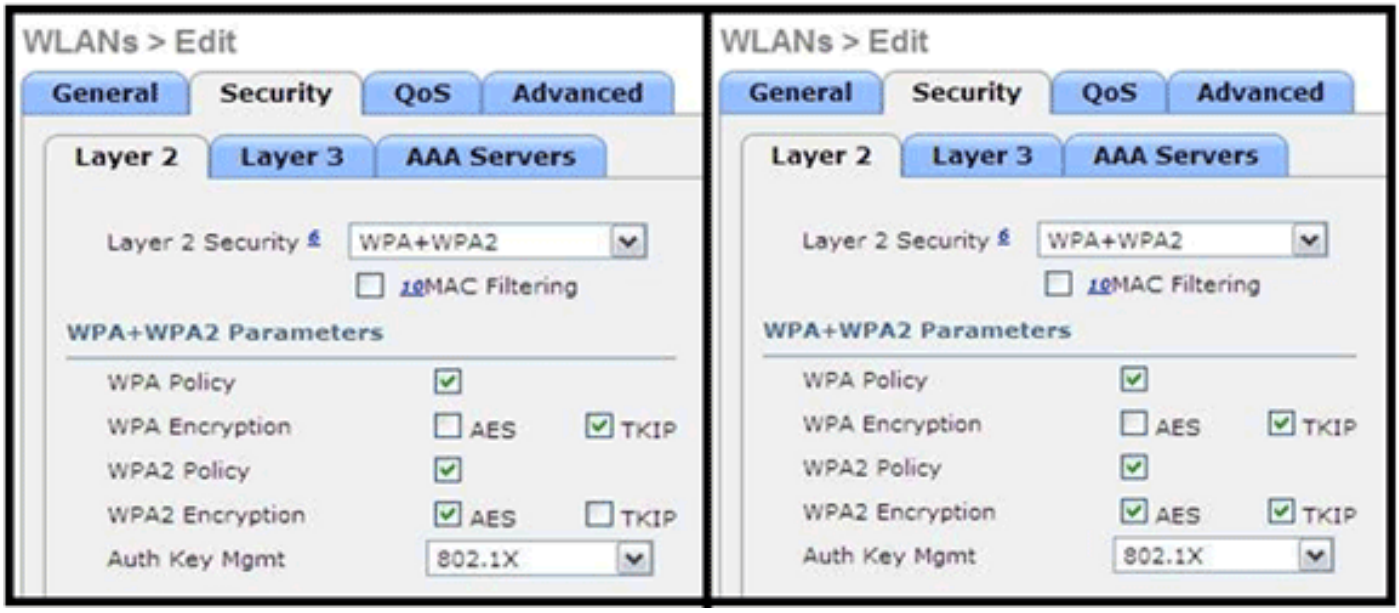


Nota: selezionare solo 802.1x o PSK.

Le impostazioni di crittografia di protezione devono essere identiche per WPA e WPA2 per TKIP e AES, come mostrato nella seguente immagine:

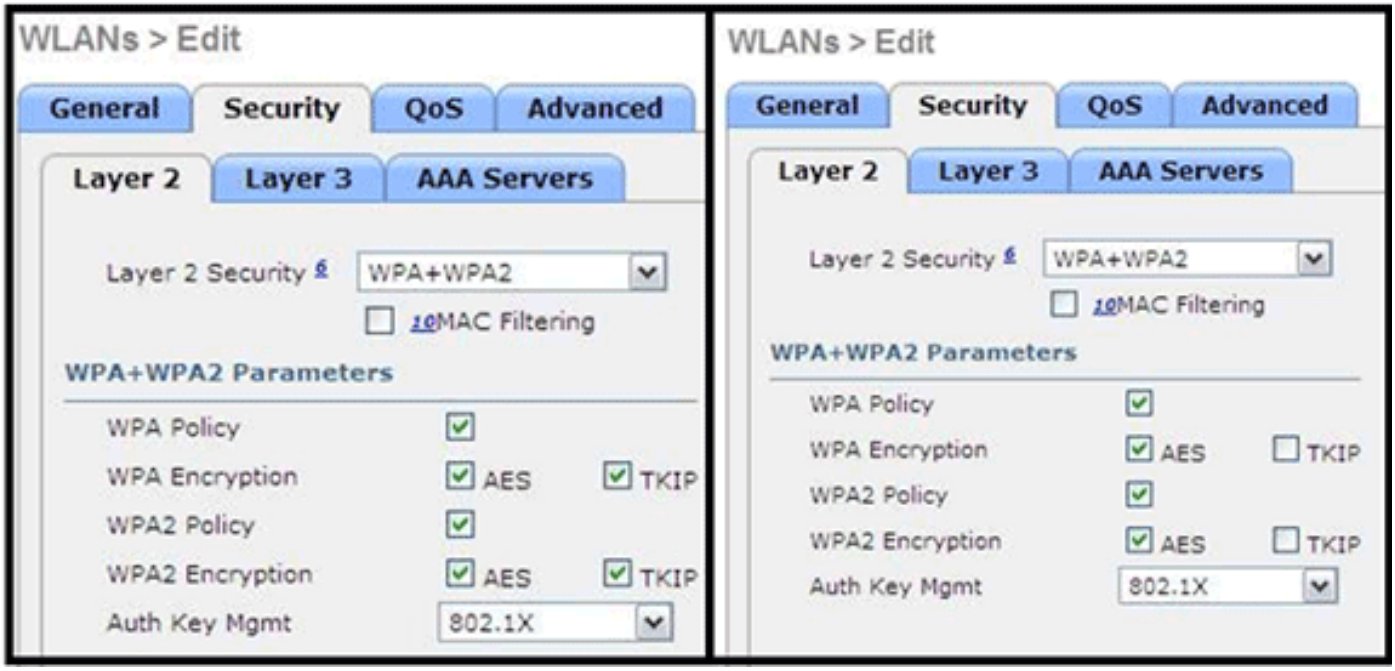


Queste immagini forniscono esempi di impostazioni incompatibili per TKIP e AES:



Nota: le impostazioni di protezione consentono funzionalità non supportate.

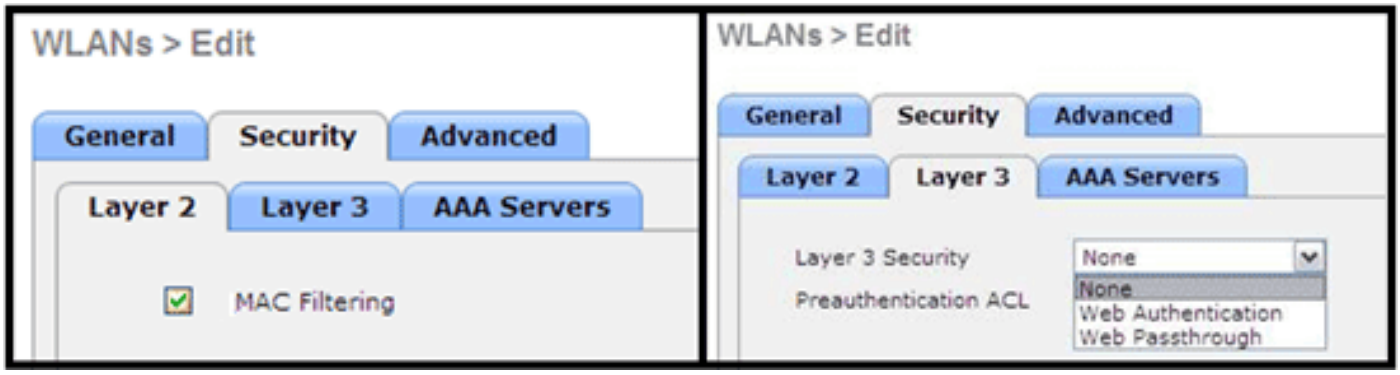
Queste immagini forniscono esempi di impostazioni compatibili:



Filtro MAC

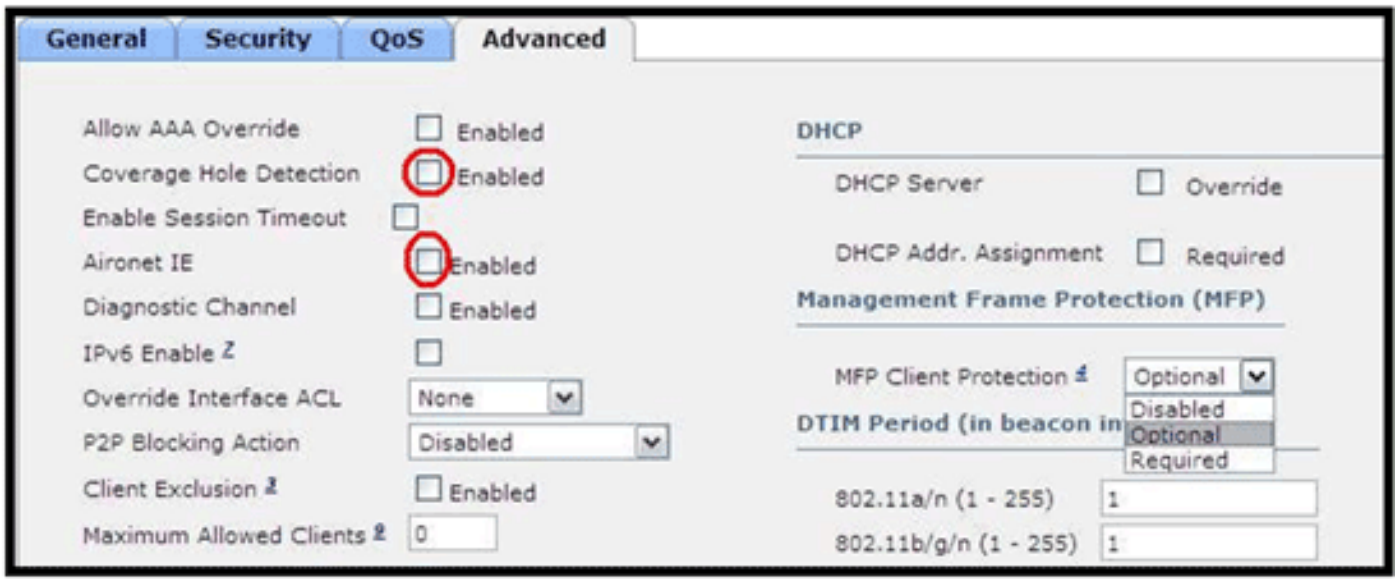
Le impostazioni di sicurezza possono essere lasciate aperte, impostate per il filtro MAC o impostate per l'autenticazione Web. Per impostazione predefinita viene utilizzato il filtro MAC.

Questa immagine mostra il filtro MAC di layer 2 e layer 3:



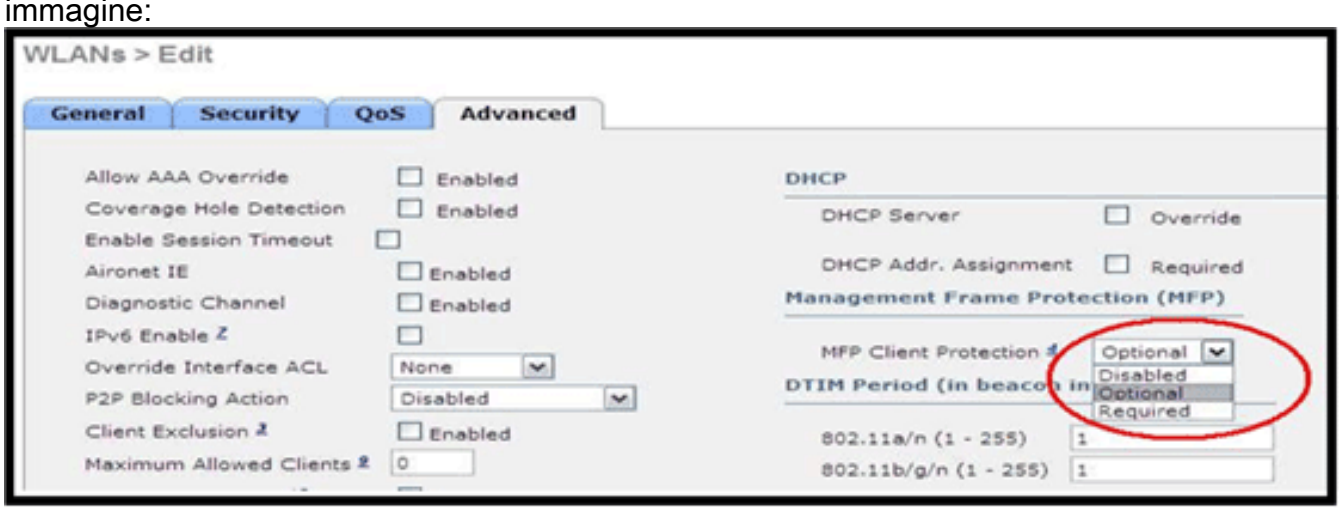
Le impostazioni QoS sono gestite:

Èinoltre necessario gestire le impostazioni avanzate:



Note:

- Il rilevamento dei fori di copertura non deve essere abilitato.
- Aironet IE (Information Elements) non deve essere abilitato perché non vengono utilizzati.
- Anche Management Frame Protection (MFP) non è supportato e deve essere disabilitato o configurato come facoltativo, come mostrato nella seguente immagine:



- Il bilanciamento del carico e la selezione della banda client non sono supportati e non devono essere abilitati:

Conteggio utenti supportati

Solo quindici utenti possono connettersi contemporaneamente alle WLAN Controller fornite sulla serie 600. Un sedicesimo utente non può eseguire l'autenticazione fino a quando uno dei primi client non esegue la deautenticazione o non si è verificato un timeout sul controller.

Nota: questo numero è cumulativo tra le WLAN dei controller sulla serie 600.

Ad esempio, se sono configurate due WLAN del controller e ci sono quindici utenti su una delle WLAN, nessun utente potrà unirsi all'altra WLAN sulla serie 600 in quel momento. Questo limite non si applica alle WLAN private locali che l'utente finale configura sulla serie 600 progettate per uso personale e i client connessi su queste WLAN private o sulle porte cablate non influiscono su questi limiti.

Gestione dei canali e impostazioni

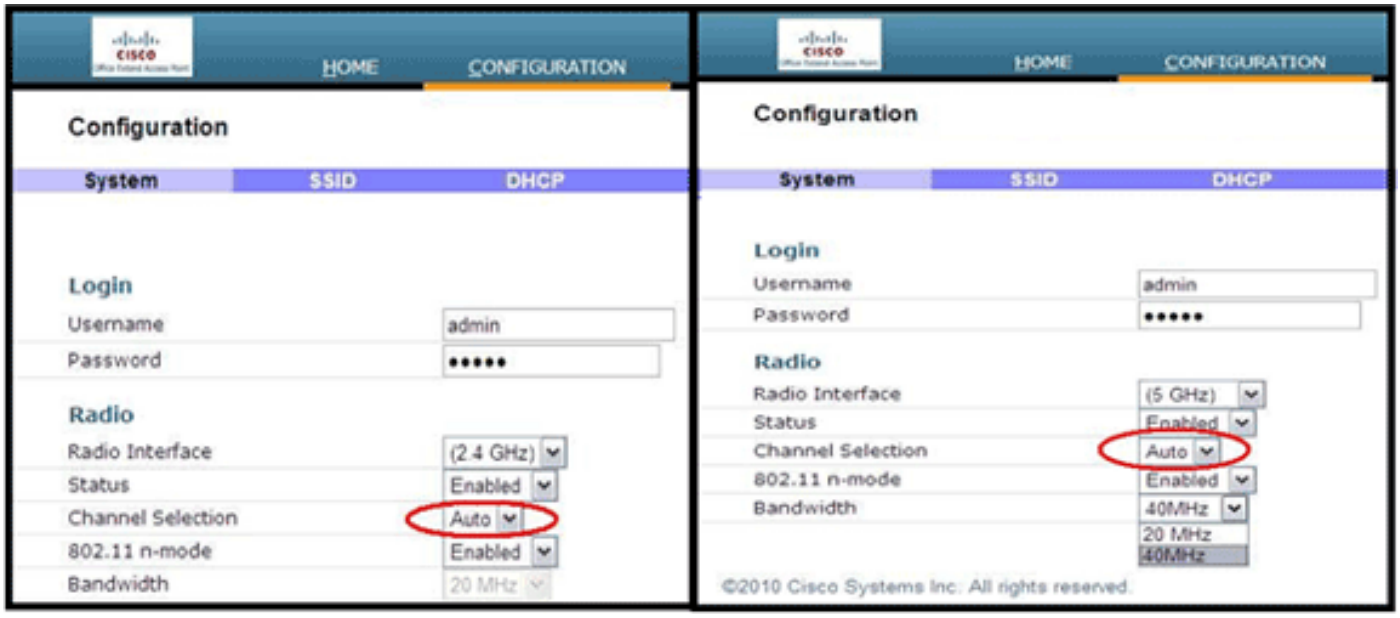
Le radio della serie 600 sono controllate tramite l'interfaccia GUI locale della serie 600 e non tramite il Wireless LAN Controller.

Il tentativo di controllare il canale dello spettro, accendere o disattivare le radio tramite il controller non avrà alcun effetto sulla serie 600.

La serie 600 eseguirà la scansione e sceglierà i canali per 2,4 GHz e 5,0 GHz durante l'avvio, a condizione che in entrambi gli spettri vengano mantenute le impostazioni predefinite sulla GUI locale.

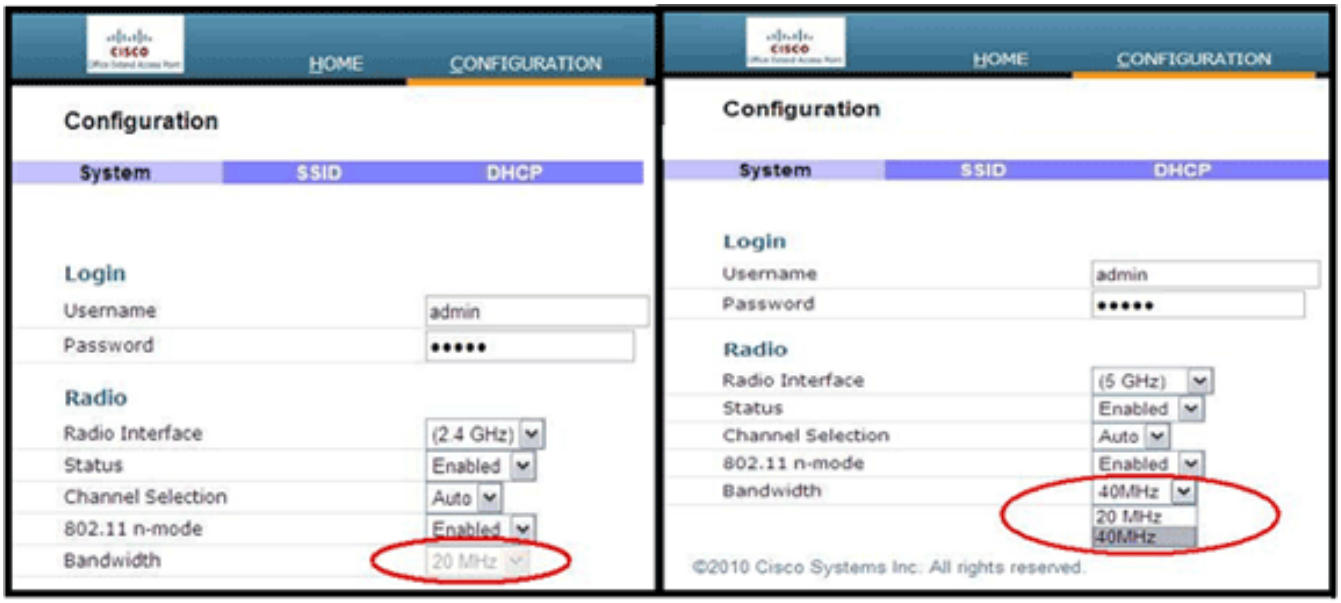
Nota: se l'utente disattiva una o entrambe le radio a livello locale (la radio è disabilitata anche per l'accesso aziendale), come accennato in precedenza, RRM e le funzionalità avanzate, come monitor, H-REAP, sniffer, vanno oltre le funzionalità di Cisco Aironet serie 600 OEAP posizionato per l'utilizzo domestico e da parte dei telelavoratori.

La selezione del canale e la larghezza di banda per 5,0 GHz sono configurate qui sull'interfaccia utente locale di Cisco Aironet serie 600 OEAP.



Note:

- Sono disponibili impostazioni di 20 e 40 MHz per 5 GHz.
- 2.4 GHz 40 MHz wide non è supportato e fisso a 20 MHz.
- L'ampiezza 40 MHz (channel bonding) non è supportata nei 2,4 GHz.



Avvertenze aggiuntive

Cisco Aironet serie 600 OEAP è progettato per implementazioni con un singolo access point. Pertanto, il roaming dei client tra la serie 600 non è supportato.

Nota: la disabilitazione dello spettro 802.11a/n o 802.11b/g/n sul controller potrebbe non disabilitare questi spettri su Cisco Aironet serie 600 OEAP perché il SSID locale potrebbe ancora funzionare.

L'utente finale ha abilitato/disabilitato il controllo delle radio in Cisco Aironet serie 600 OEAP.

Supporto 802.1x sulla porta cablata

In questa versione iniziale, 802.1x è supportato solo su Command Line Interface (CLI).

Nota: il supporto GUI non è stato ancora aggiunto.

Questa è la porta cablata (porta n. 4 in giallo) sul pannello posteriore della Cisco Aironet serie 600 OEAP ed è collegata alla LAN remota (vedere la sezione precedente sulla configurazione della LAN remota).

In qualsiasi momento, è possibile utilizzare il comando **show** per visualizzare la configurazione LAN remota corrente:

```
show remote-lan <remote-lan-id>
```

Per modificare la configurazione LAN remota, è necessario prima disabilitarla:

```
remote-lan disable <remote-lan-id>
```

Abilitare l'autenticazione 802.1X per la LAN remota:

```
config remote-lan security 802.1X enable <remote-lan-id>
```

Per annullarla, utilizzare il comando:

```
config remote-lan security 802.1X disable <remote-lan-id>
```

Per la LAN remota, "Encryption" è sempre "None" (come mostrato in **show remote-lan**) e non configurabile.

Se si desidera utilizzare il protocollo EAP locale (nel controller) come server di autenticazione:

```
config remote-lan local-auth enable <profile-name> <remote-lan-id>
```

In cui il `profilo` è definito tramite la GUI del controller (Security > Local EAP) o la CLI (**config local-auth**). Per ulteriori informazioni sul comando, consultare la guida al controller.

Per annullarla, usare questo comando:

```
config remote-lan local-auth disable <remote-lan-id>
```

Oppure, se si usa un server di autenticazione AAA esterno:

- **config remote-lan radius_server auth add/delete <*id-lan-remota*> <*id-server*>**
- **config remote-lan radius_server auth enable/disable <*id-lan-remota*>**

Dove il `server` è configurato tramite la GUI del controller (Security > RADIUS > Authentication) o la CLI (**config radius auth**). Per ulteriori informazioni sul comando, consultare la guida al controller.

Al termine della configurazione, abilitare la LAN remota:

```
config remote-lan enable <remote-lan-id>
```

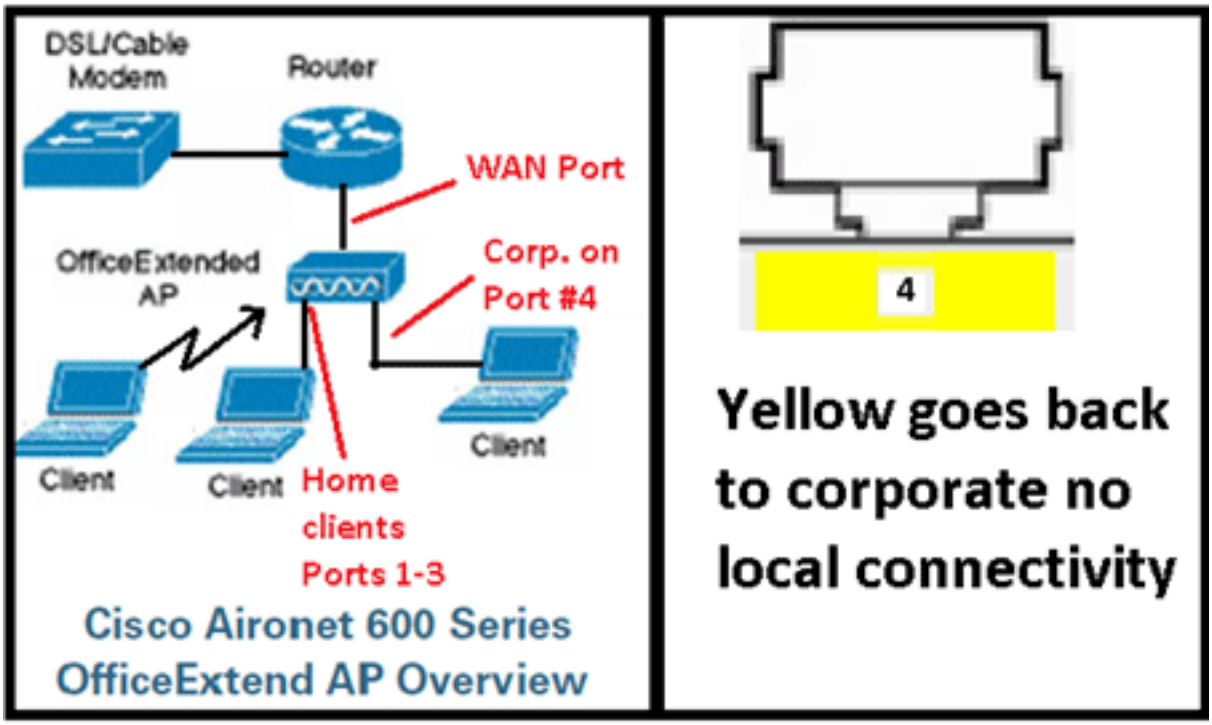
Per verificare l'impostazione, usare il comando **show remote-lan <*remote-id*>**.

Per il client LAN remoto, è necessario abilitare l'autenticazione 802.1X e configurarla di

conseguenza. Consultare il manuale dell'utente del dispositivo.

Configurazione access point OEAP-600

L'immagine mostra lo schema dei cavi di Cisco Aironet serie 600 OEAP:

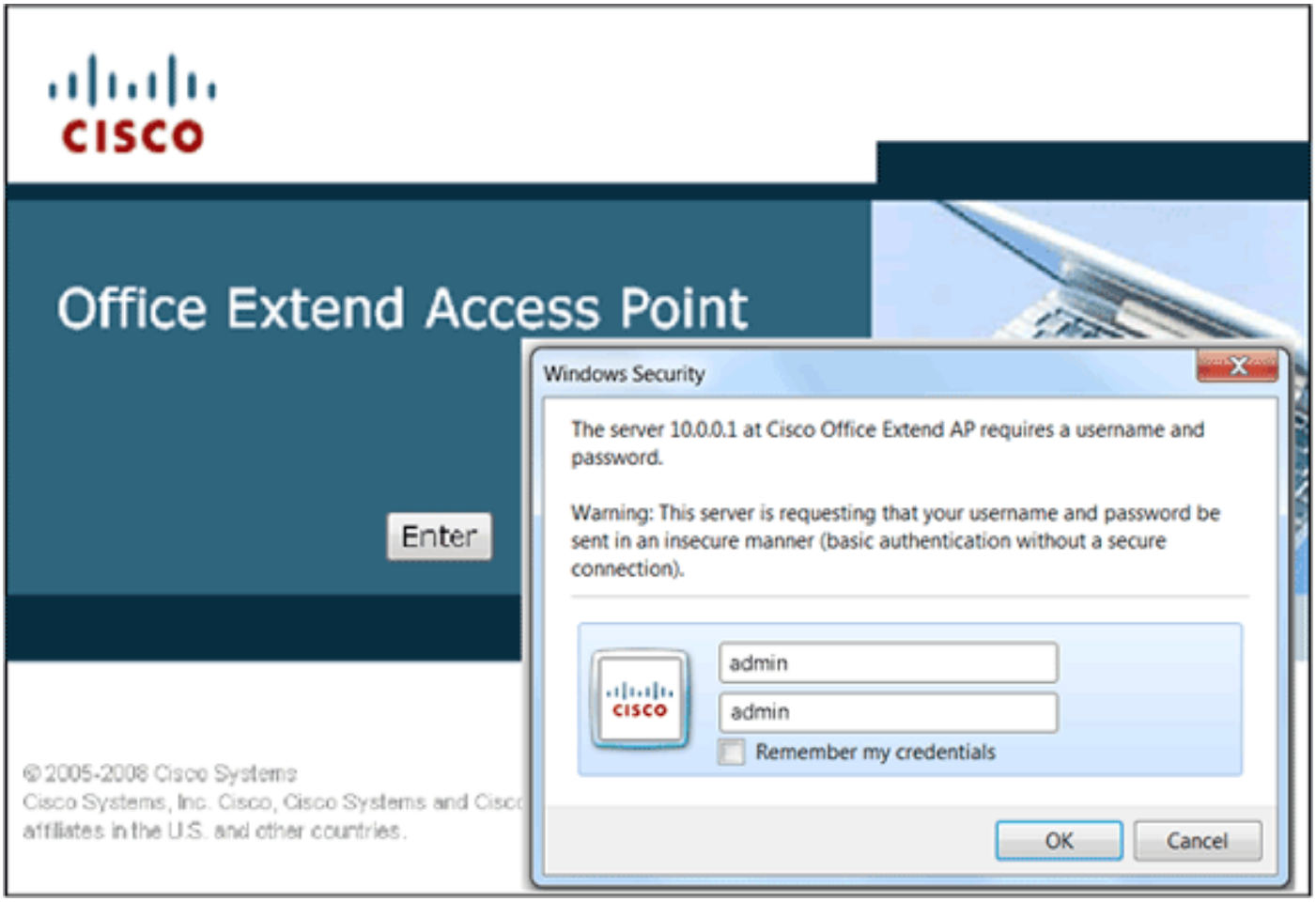


L'ambito DHCP predefinito del Cisco Aironet serie 600 OEAP è 10.0.0.x, quindi è possibile selezionare il punto di accesso sulle porte 1-3 usando l'indirizzo 10.0.0.1. Il nome utente e la password predefiniti sono admin.

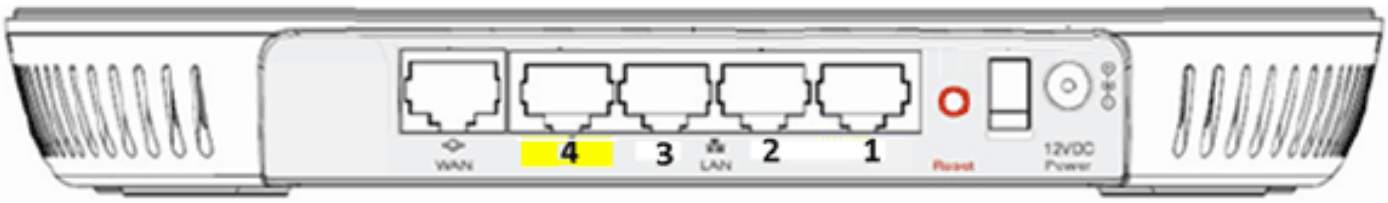
Nota: questa impostazione è diversa da AP1040, 1130, 1140 e 3502i, che hanno usato Cisco come nome utente e password.

Se le radio sono attive ed è già stato configurato un SSID personale, è possibile accedere alla schermata di configurazione in modalità wireless. In caso contrario, è necessario utilizzare le porte Ethernet locali da 1 a 3.

Per effettuare il login, il nome utente e la password predefiniti sono admin.



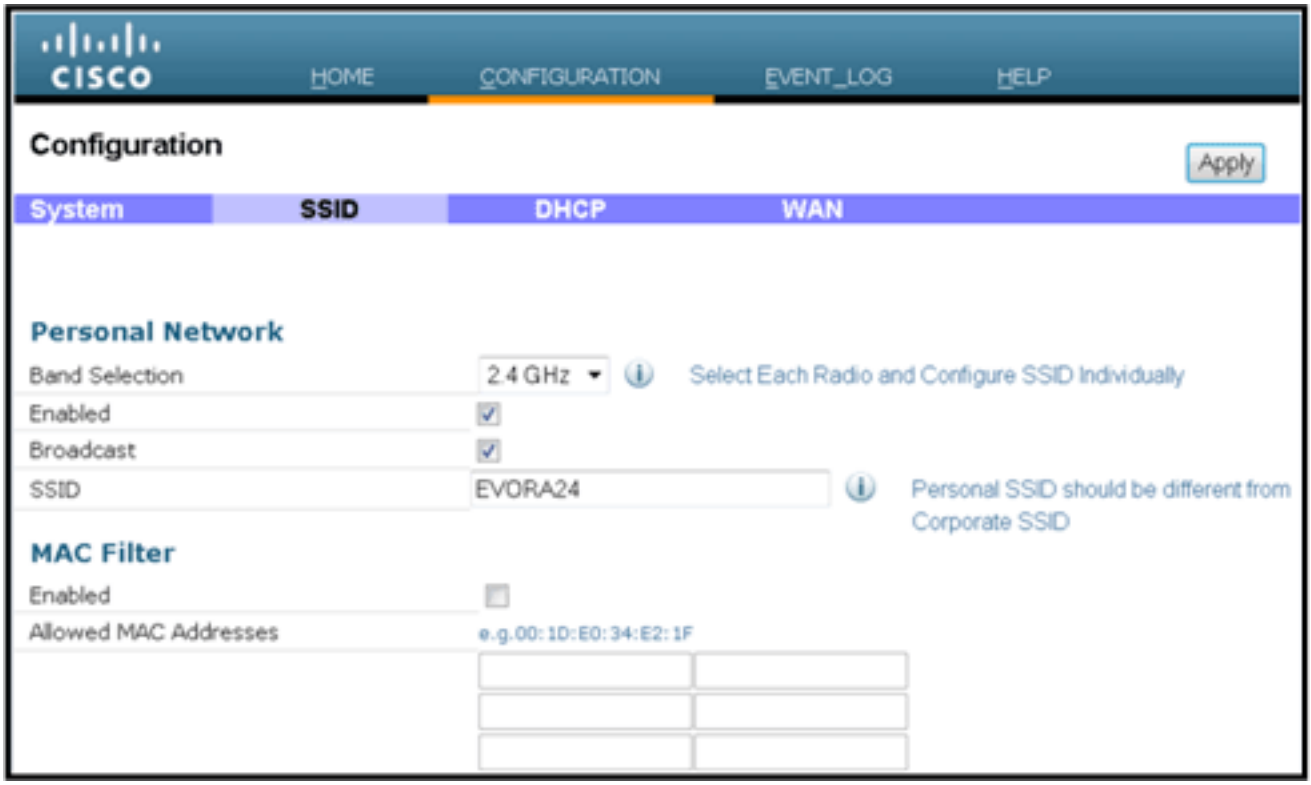
Nota: la porta gialla #4 non è attiva per l'uso locale. Se sul controller è configurata una LAN remota, questa porta eseguirà il tunneling indietro dopo che l'access point si è unito correttamente al controller. Per individuare il dispositivo, utilizzare localmente le porte 1-3:



Dopo aver individuato il dispositivo, viene visualizzata la schermata di stato home. Questa schermata fornisce le statistiche di radio e MAC. Se le radio non sono state configurate, la schermata di configurazione consente all'utente di abilitare le radio, impostare i canali e le modalità, configurare gli SSID locali e abilitare le impostazioni WLAN.

Dalla schermata SSID è possibile configurare la rete WLAN personale. Il SSID radio aziendale e i parametri di sicurezza vengono configurati ed eliminati dal controller (dopo aver configurato la WAN con l'IP del controller) e si è verificato un join riuscito.

L'immagine mostra una configurazione del filtro MAC locale SSID:



Dopo che l'utente ha configurato il SSID personale, la schermata seguente consente all'utente di impostare la protezione sul SSID privato dell'abitazione, abilitare le radio e configurare il filtro MAC, se desiderato. Se la rete personale utilizza velocità 802.11n, si consiglia di scegliere un tipo di autenticazione, un tipo di crittografia e una passphrase per abilitare WPA2-PSK e AES.

Nota: queste impostazioni SSID sono diverse da quelle aziendali se l'utente sceglie di disabilitare una o entrambe le radio (entrambe sono disabilitate anche per l'uso aziendale).

Gli utenti che dispongono dell'accesso locale alle impostazioni di controllo dell'amministratore hanno il controllo sulle funzioni principali, quali l'attivazione/disattivazione della radio, a meno che il dispositivo non sia protetto da password e configurato dall'amministratore. Pertanto, è necessario prestare attenzione a non disattivare entrambe le radio in quanto ciò può causare una perdita di connettività anche se il dispositivo si unisce correttamente al controller.

Nell'immagine sono illustrate le impostazioni di protezione del sistema:

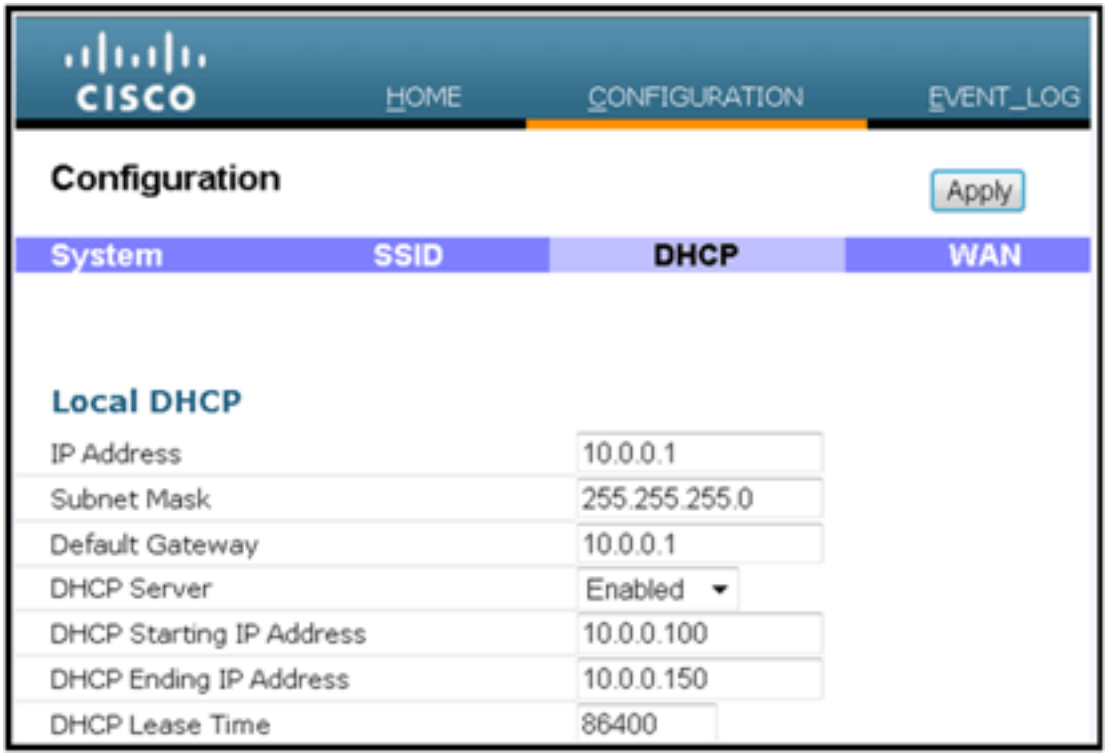
È previsto che il teleworker di casa installi Cisco Aironet serie 600 OEAP dietro un router di casa, in quanto questo prodotto non è progettato per sostituire la funzionalità di un router di casa. Ciò si verifica perché la versione corrente di questo prodotto non dispone del supporto firewall, del supporto PPPoE o dell'inoltro delle porte. Si tratta di funzionalità che i clienti si aspettano di trovare in un router di casa.

Sebbene questo prodotto possa funzionare senza un router di casa, si consiglia di non posizionarlo in questo modo per i motivi indicati. Possono inoltre verificarsi problemi di compatibilità che si connettono direttamente ad alcuni modem.

Poiché la maggior parte dei router domestici ha un ambito DHCP nell'intervallo 192.168.x.x, questo dispositivo ha un ambito DHCP predefinito di 10.0.0.x ed è configurabile.

Se il router di origine utilizza la versione 10.0.0.x, è necessario configurare Cisco Aironet serie 600 OEAP in modo che utilizzi una versione 192.168.1.x o un indirizzo IP compatibile per evitare conflitti di rete.

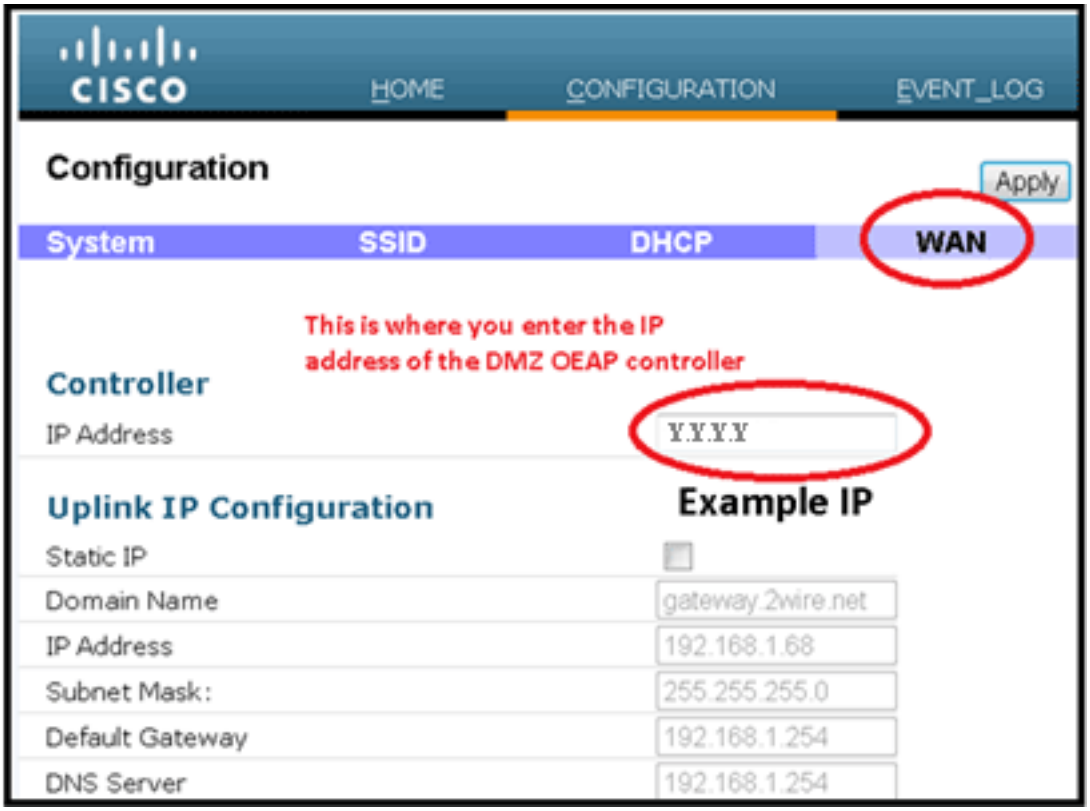
Nell'immagine viene mostrata una configurazione dell'ambito DHCP:



Attenzione: se Cisco Aironet serie 600 OEAP non è posizionato nell'area intermedia o non è configurato dall'amministratore IT, l'utente deve immettere l'indirizzo IP del controller aziendale (vedere di seguito) in modo che l'access point possa essere collegato correttamente al controller. Dopo aver completato il join, l'access point deve scaricare l'immagine più recente dal controller e i parametri di configurazione, ad esempio le impostazioni della WLAN aziendale. Inoltre, se configurata, la porta cablata n. 4 per le impostazioni LAN remote sul pannello posteriore del Cisco Aironet serie 600 OEAP.

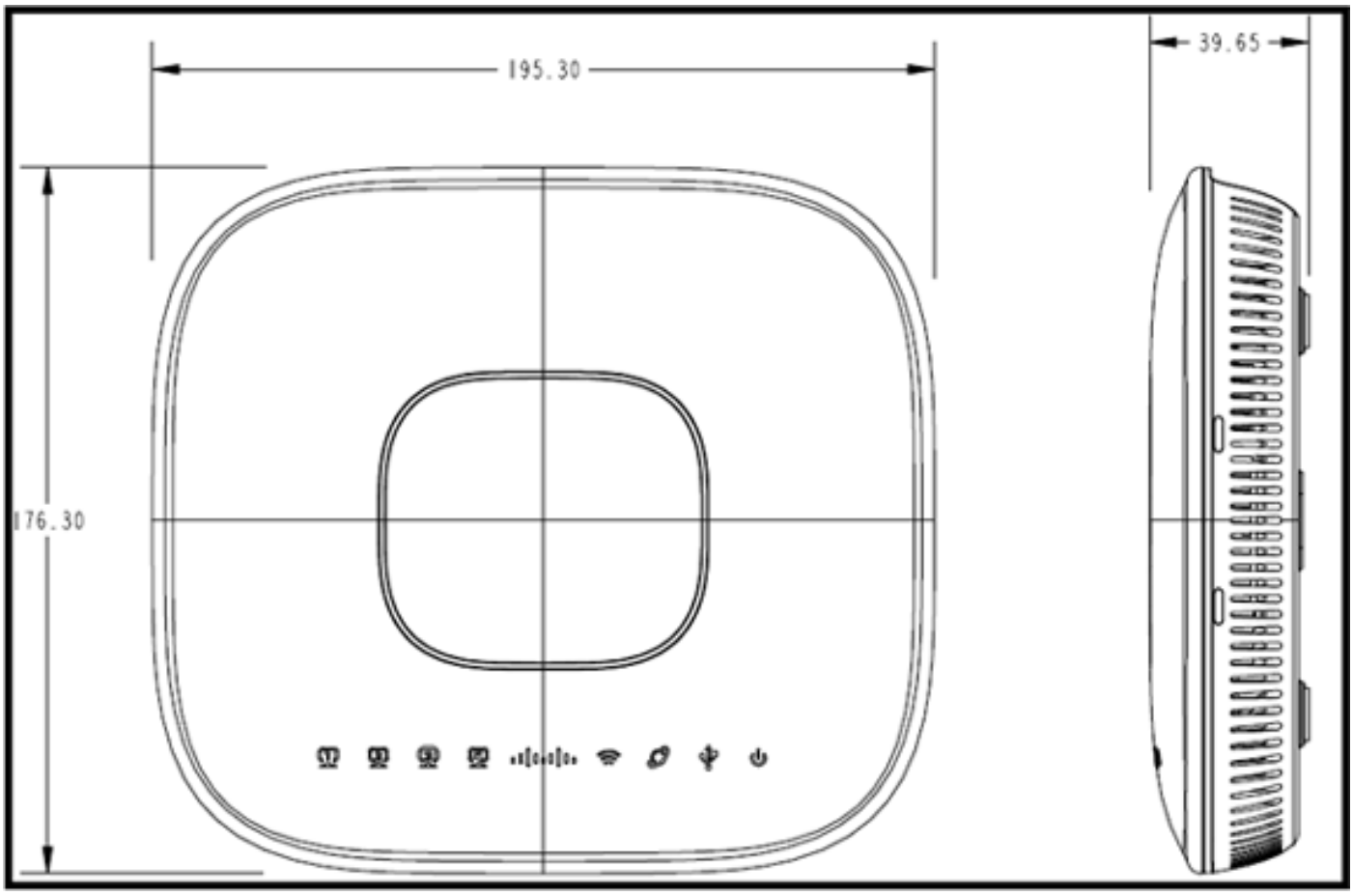
In caso contrario, verificare che l'indirizzo IP del controller sia raggiungibile tramite Internet. Se il filtro MAC è abilitato, verificare che l'indirizzo MAC sia stato immesso correttamente nel controller.

L'immagine mostra l'indirizzo IP del controller Cisco Aironet serie 600 OEAP:



Installazione hardware Access Point OEAP-600

L'immagine mostra gli aspetti fisici di Cisco Aironet serie 600 OEAP:

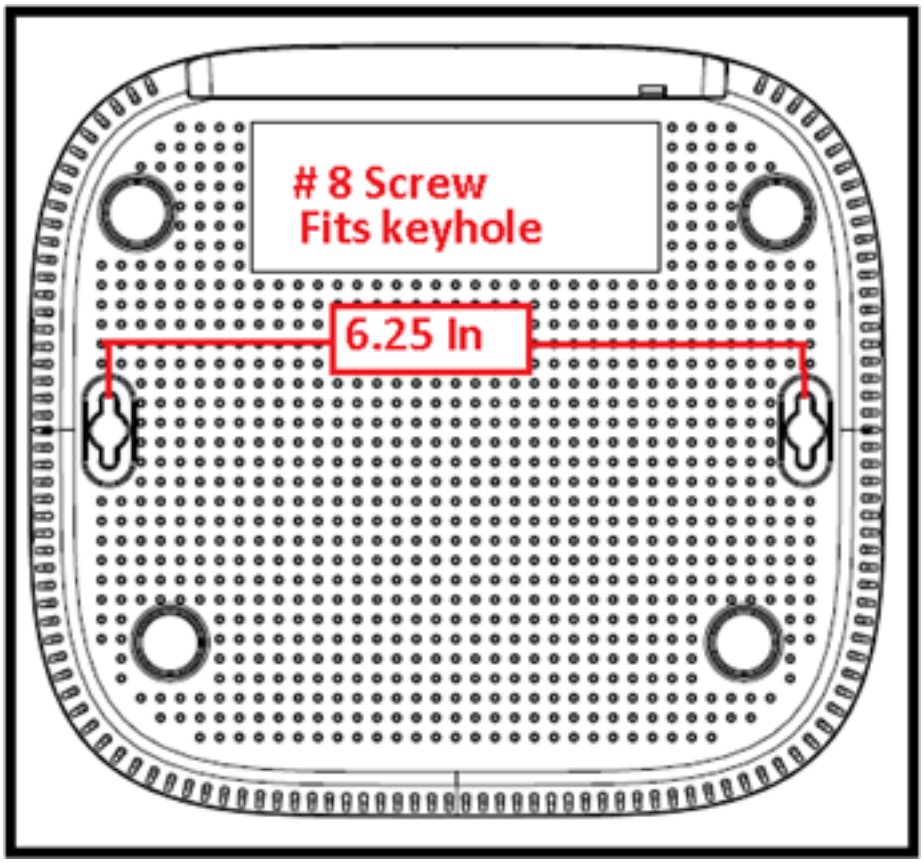


Questo access point è progettato per essere montato su un tavolo e ha piedi in gomma. Può anche essere montato a parete o posizionato verticalmente utilizzando la base in dotazione.

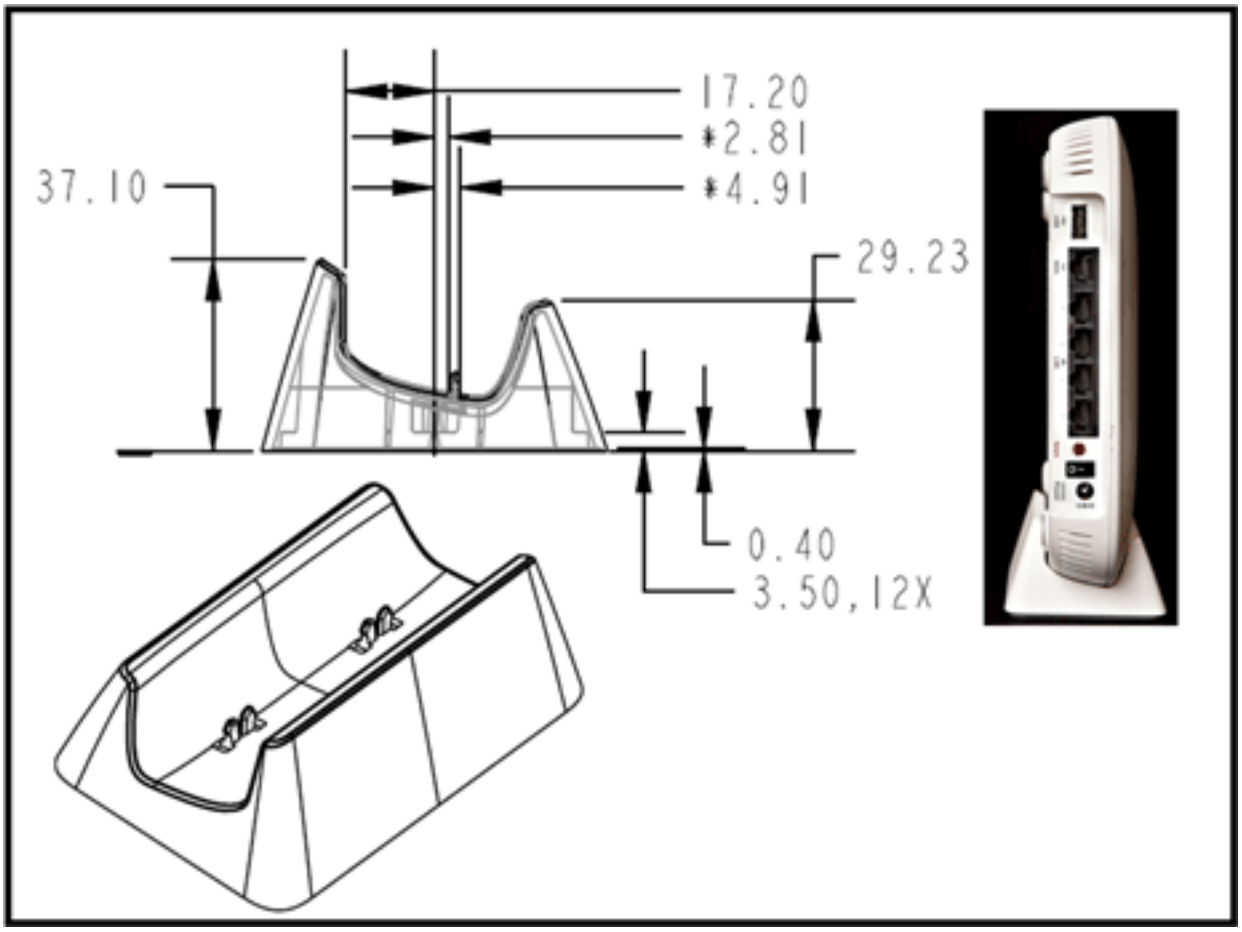
Cercare di individuare l'access point il più vicino possibile agli utenti desiderati. Evitare aree con grandi superfici metalliche, ad esempio posizionare il dispositivo su una scrivania di metallo o vicino a uno specchio di grandi dimensioni. Maggiore è il numero di muri e oggetti tra l'access point e l'utente, minore sarà la potenza del segnale e minori saranno le prestazioni.

Nota: questo access point utilizza un alimentatore a +12 Volt e non utilizza Power over Ethernet (PoE). Inoltre, il dispositivo non fornisce PoE. Accertarsi di utilizzare l'adattatore di alimentazione corretto con il punto di accesso. Inoltre, accertarsi di non utilizzare altre schede di rete di altri dispositivi, quali notebook e telefoni IP, in quanto potrebbero danneggiare il punto di accesso.

L'unità può essere montata sulla parete con ancoraggi in plastica o viti per legno.



L'unità può essere montata in posizione verticale utilizzando la base in dotazione.

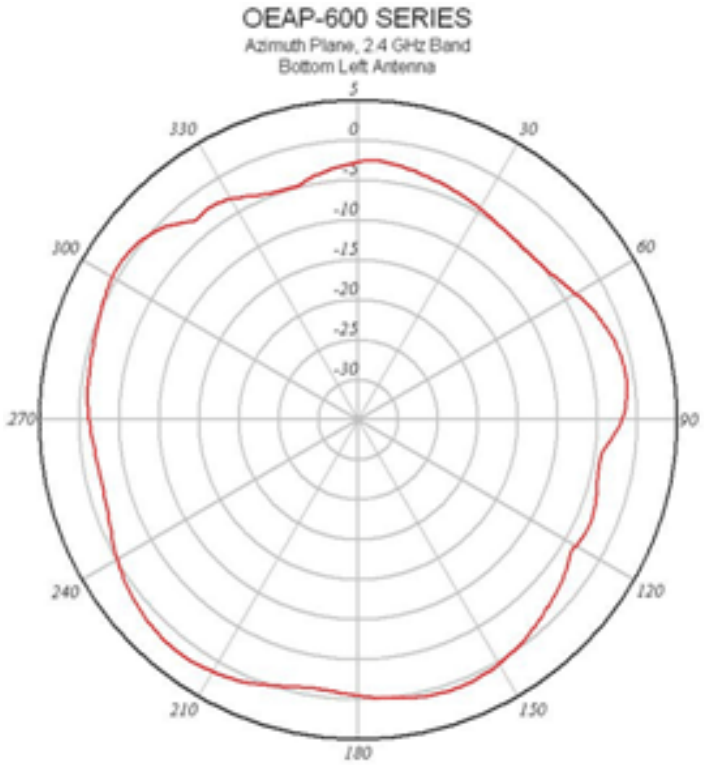


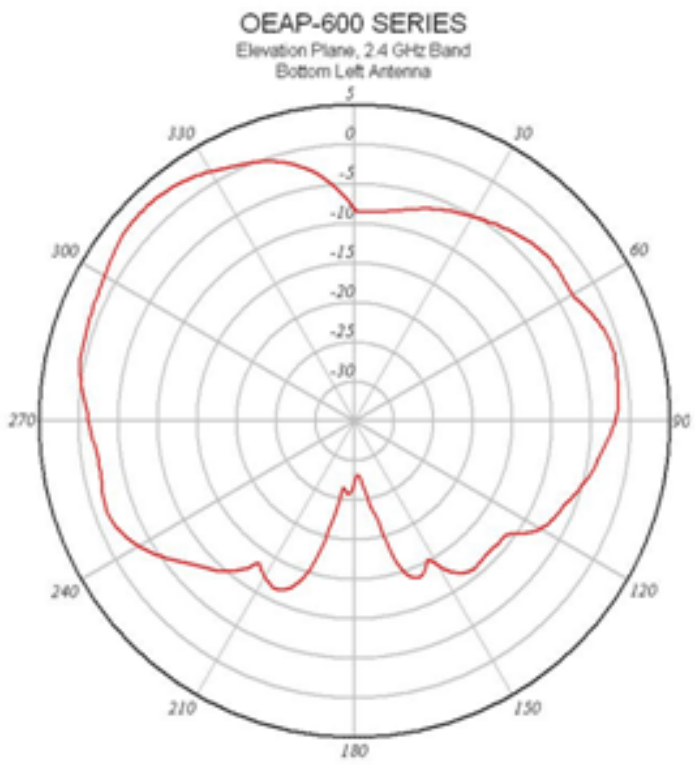
Cisco Aironet serie 600 OEAP ha antenne posizionate ai bordi dell'access point. L'utente deve fare attenzione a non posizionare l'access point in aree vicine a oggetti metallici o ostruzioni che possono causare la direzione o la diminuzione del segnale. Il guadagno dell'antenna è di circa 2 dBi in entrambe le bande e progettato per irradiare in un modello a 360 gradi. Simile a una lampadina (senza un paralume), l'obiettivo è irradiare in tutte le direzioni. Pensare al punto di accesso come a una lampada e provare a posizionarlo in prossimità degli utenti.

Gli oggetti metallici, come gli specchi, ostruiscono il segnale in modo molto simile all'analogia del paralume. È possibile che si verifichi una riduzione della velocità effettiva o dell'intervallo se il segnale deve penetrare o passare attraverso oggetti solidi. Se ci si aspetta una connettività, ad esempio in una casa a tre piani, evitare di posizionare l'access point nel seminterrato e provare a montarlo in una posizione centrale all'interno della casa.

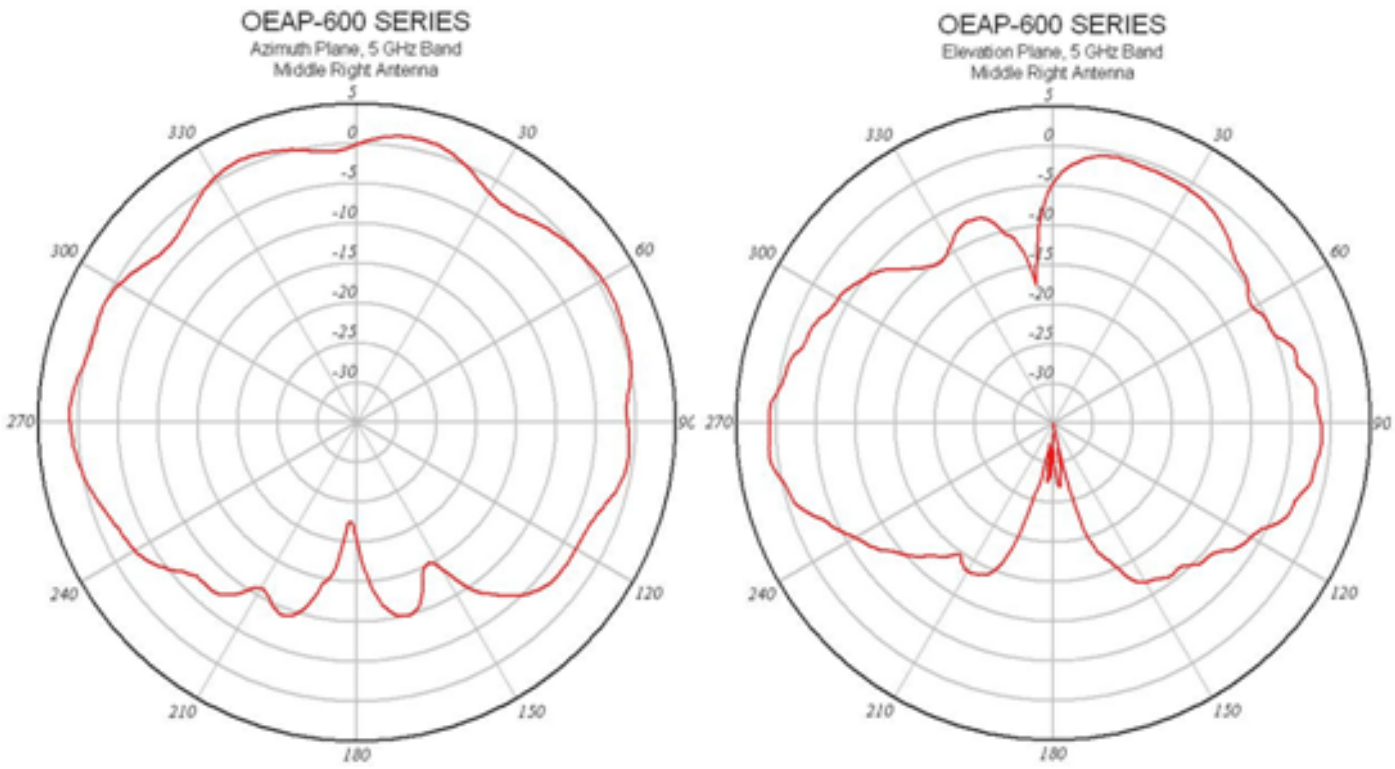
Il punto di accesso dispone di sei antenne (tre per banda).

L'immagine mostra un modello di radiazione dell'antenna a 2,4 GHz (ripreso dall'antenna in basso a sinistra).





L'immagine mostra un modello di radiazione dell'antenna a 5 GHz (tratto dall'antenna in mezzo a destra):



Risoluzione dei problemi di OEAP-600

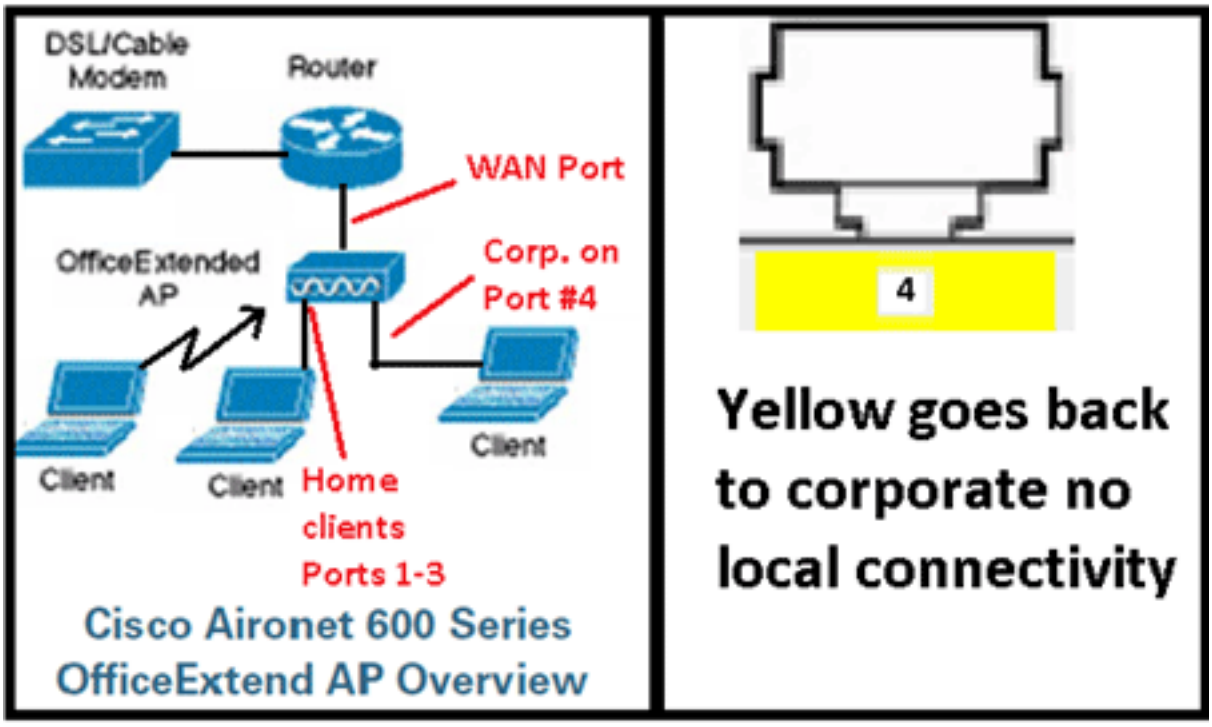
Verificare che il cablaggio iniziale sia corretto. Ciò conferma che la porta WAN su Cisco Aironet serie 600 OEAP è connessa al router e può ricevere correttamente un indirizzo IP. Se l'access point non sembra collegarsi al controller, collegare un PC alla porta 1-3 (porte del client di casa) e verificare se è possibile passare all'access point utilizzando l'indirizzo IP predefinito 10.0.0.1. Il nome utente e la password predefiniti sono admin.

Verificare che l'indirizzo IP per il controller aziendale sia impostato. In caso contrario, immettere l'indirizzo IP e riavviare Cisco Aironet serie 600 OEAP in modo che possa provare a stabilire un collegamento con il controller.

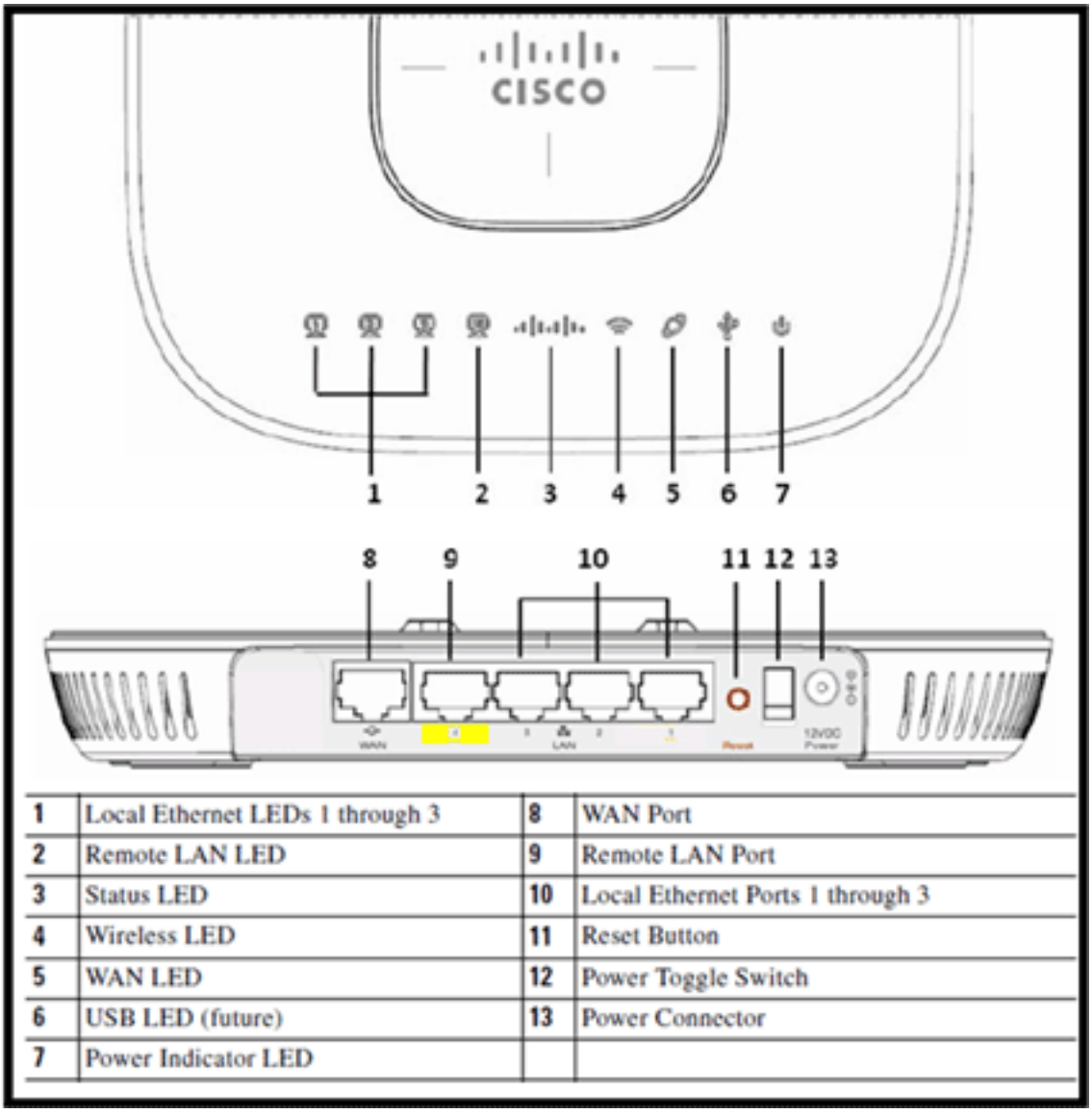
Nota: la porta aziendale n. 4 (in giallo) non può essere utilizzata per individuare il dispositivo a scopo di configurazione. Si tratta essenzialmente di una "porta inattiva", a meno che non sia configurata una LAN remota. Quindi, eseguirà il tunneling verso l'azienda (utilizzata per la connettività aziendale cablata)

Controllare il registro eventi per verificare lo stato dell'associazione (ulteriori informazioni su questo argomento in seguito).

L'immagine mostra lo schema dei cavi Cisco Aironet serie 600 OEAP:



L'immagine mostra le porte di connettività OEAP Cisco Aironet serie 600:



1	Local Ethernet LEDs 1 through 3	8	WAN Port
2	Remote LAN LED	9	Remote LAN Port
3	Status LED	10	Local Ethernet Ports 1 through 3
4	Wireless LED	11	Reset Button
5	WAN LED	12	Power Toggle Switch
6	USB LED (future)	13	Power Connector
7	Power Indicator LED		

Se Cisco Aironet serie 600 OEAP non riesce a collegarsi al controller, si consiglia di controllare i seguenti elementi:

1. Verificare che il router sia funzionante e collegato alla porta WAN del Cisco Aironet serie 600 OEAP.
2. Collegare un PC a una delle porte da 1 a 3 su Cisco Aironet serie 600 OEAP. Dovrebbe vedere Internet.
3. Verificare che l'indirizzo IP del controller aziendale sia presente nell'access point.
4. Verificare che il controller sia in DMZ e raggiungibile tramite Internet.
5. Verificare che il join e il LED del logo Cisco siano di colore blu o viola.
6. Attendere il tempo necessario nel caso in cui l'access point debba caricare una nuova immagine e riavviare.
7. Se è in uso un firewall, verificare che le porte UDP 5246 e 5247 non siano bloccate.

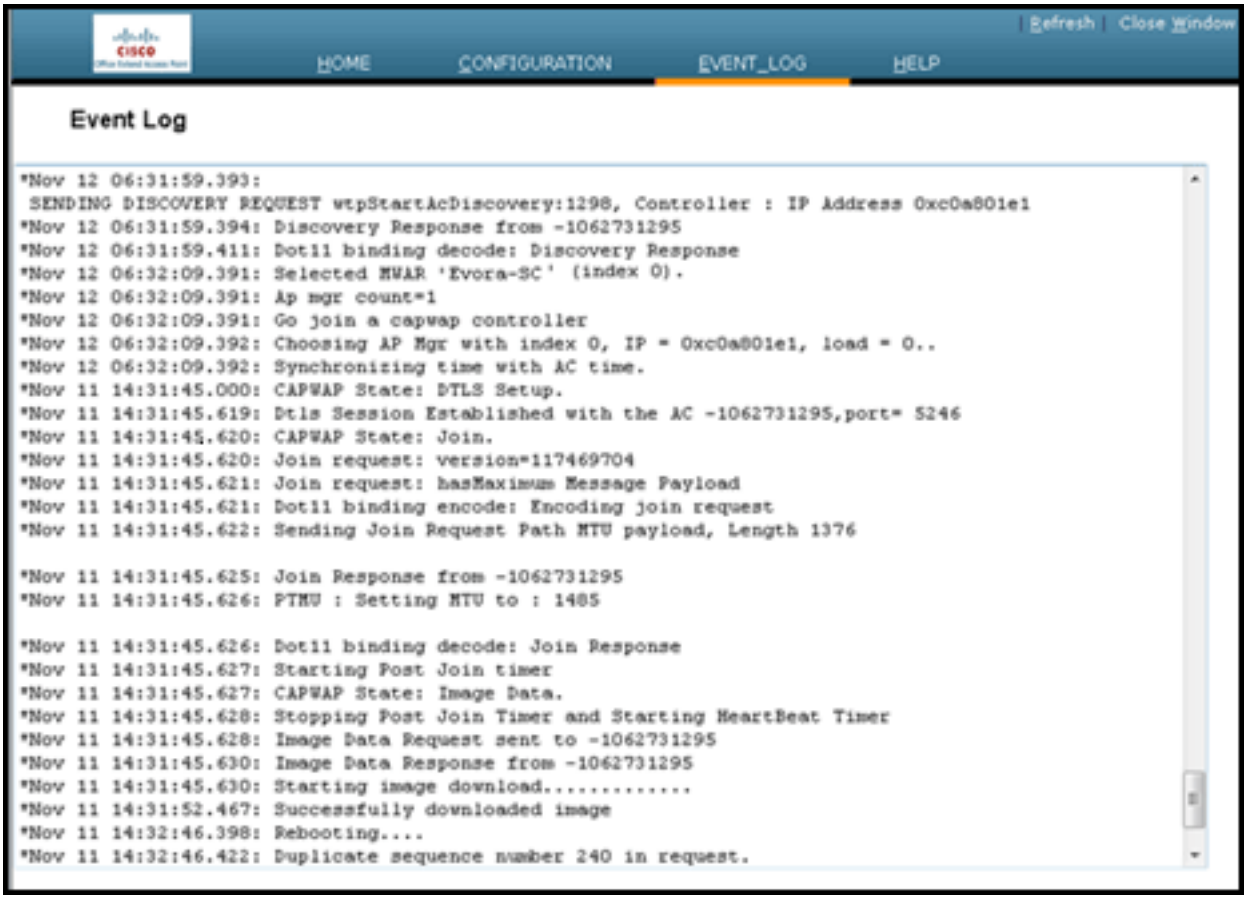
L'immagine mostra lo stato del LED del logo Cisco Aironet serie 600 OEAP:

Understanding Cisco Aironet 600 Series OfficeExtend AP LEDs

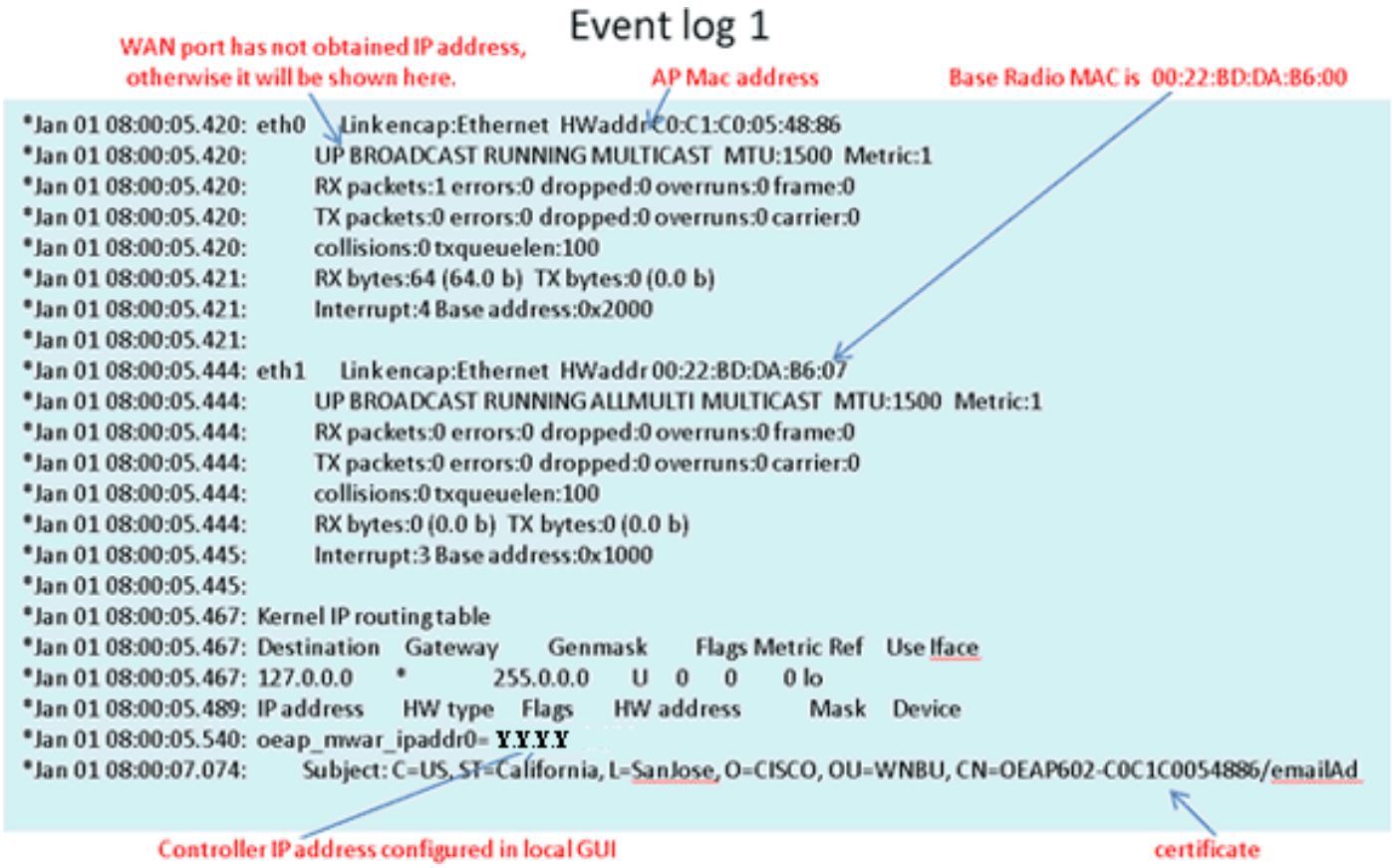
Status LED	Meaning
Purple	Association status, when CAPWAP is connected: Normal operating condition, but no wireless client associated.
Blue	Association status, when CAPWAP is connected: Normal operating condition, at least one wireless client association.
Flashing blue	Operating Status: Software upgrade in progress.
Flashing orange	Operating Status: No IP address, waiting for DHCP IP.
Cycling through purple, orange and blue	Operating Status: Discovery/join process in progress, no client associated.
Cycling through purple, orange	Operating Status: Discovery/join process in progress, with client associated.
Orange	Cisco IOS errors: Software failure; try disconnecting and reconnecting unit power.

Se il processo di unione non riesce, il LED passa attraverso i colori o magari lampeggia in arancione. In questo caso, controllare il registro eventi per ulteriori dettagli. Per accedere al registro eventi, individuare l'access point (utilizzando il SSID personale o le porte cablate 1-3) e acquisire i dati per la revisione da parte dell'amministratore IT.

L'immagine mostra il registro eventi OEAP di Cisco Aironet serie 600:



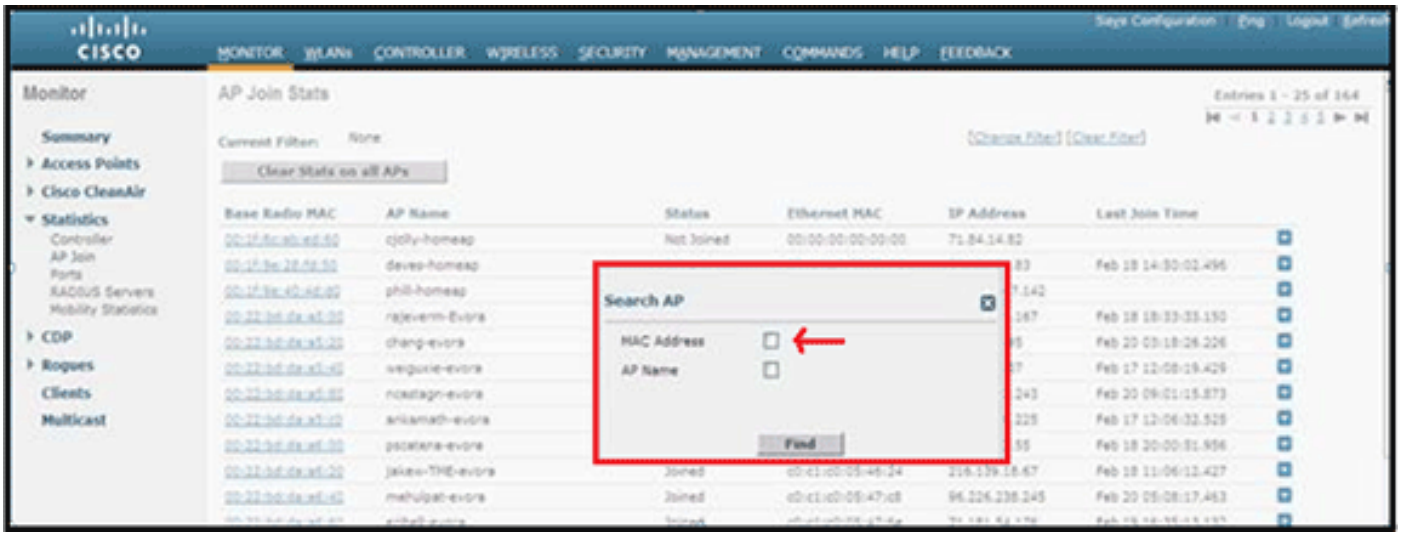
Se il processo di join non riesce e questa è la prima volta che Cisco Aironet serie 600 OEAP tenta di connettersi al controller, controllare le statistiche di join dell'access point per Cisco Aironet serie 600 OEAP. A tale scopo, è necessario disporre del MAC della radio base dell'access point. Questa informazione è disponibile nel registro eventi. Di seguito è riportato un esempio di registro eventi con commenti che consente di interpretare il problema:



Una volta appresa questa condizione, è possibile esaminare le statistiche del monitor del controller per determinare se Cisco Aironet serie 600 OEAP si è unito al controller o se si è mai unito al controller. Inoltre, questo dovrebbe fornire un'indicazione sul perché, o se, si è verificato un guasto.

Se è richiesta l'autenticazione AP, verificare che l'indirizzo MAC Ethernet OEAP Cisco Aironet serie 600 (non l'indirizzo MAC della radio) sia stato immesso nel server Radius in lettere minuscole. È possibile determinare l'indirizzo MAC Ethernet anche dal registro eventi.

Ricerca di Cisco Aironet serie 600 OEAP sul controller



Se si è determinato che è possibile accedere a Internet da un PC collegato alla porta Ethernet locale, ma l'access point non può ancora unirsi al controller, e si è verificato che l'indirizzo IP del controller è configurato nell'interfaccia utente grafica dell'access point locale ed è raggiungibile, quindi verificare se l'access point è stato unito correttamente. Probabilmente l'access point non è presente nel server AAA. Oppure, se l'handshake DTLS ha esito negativo, l'access point potrebbe avere un certificato errato o un errore di data/ora sul controller.

Se nessuna unità Cisco Aironet serie 600 OEAP può collegarsi al controller, verificare che il controller sia sulla DMZ raggiungibile e che le porte UDP 5246 e 5247 siano aperte.

Come eseguire il debug dei problemi di associazione dei client

L'access point si unisce correttamente al controller, ma il client wireless non può associarsi all'SSID aziendale. Controllare il registro eventi per verificare se un messaggio di associazione raggiunge l'access point.

Nella figura seguente vengono illustrati gli eventi normali per l'associazione del client a SSID aziendale con WPA o WPA2. Per SSID con autenticazione aperta o WEP statico, è presente un solo evento `ADD MOBILE`.

Registro eventi - Associazione client

Se l'evento (Re)Assoc-Req non è presente nel registro, verificare che le impostazioni di protezione del client siano corrette.

Se l'evento (Re)Assoc-Req viene visualizzato nel log ma il client non può associarsi correttamente, abilitare il comando **debug client <indirizzo MAC>** sul controller per il client e individuare il problema allo stesso modo di un client che lavora con altri punti di accesso Cisco non OEAP.

Interpretazione del registro eventi

I seguenti registri eventi con commenti possono essere utili per risolvere altri problemi di connessione OEAP di Cisco Aironet serie 600.

Di seguito vengono riportati alcuni esempi raccolti dai file di log degli eventi OEAP della serie Cisco Aironet 600 con i relativi commenti che semplificano l'interpretazione del log degli eventi:

Event log 2

*Jan 01 08:00:07.093: Build version 7.0.112.66 (compiled Feb 19 2011 at 16:29:58).
*Jan 01 08:00:08.975: CAPWAP State: Init.
*Jan 01 08:00:09.009: CAPWAP State: Discovery.
*Jan 01 08:00:09.042: Starting Discovery.
*Jan 01 08:00:09.044: CAPWAP State: Discovery.
*Jan 01 08:00:09.193: Discovery Request sent to **Y.Y.Y.Y** with discovery type set to 1
*Jan 01 08:00:09.194: Discovery Request sent to **Y.Y.Y.Y** with discovery type set to 1
*Jan 01 08:00:09.194:
SENDING DISCOVERY REQUEST wtpStartAcDiscovery:1338, Controller Cisco_7d:88:00: IP Address
*Jan 01 08:00:09.195: Discovery Request sent to **Y.Y.Y.Y** with discovery type set to 0
*Jan 01 08:00:09.256: Discovery Response from **Y.Y.Y.Y**
*Jan 01 08:00:09.272: Dot11 binding decode: Discovery Response
*Jan 01 08:00:09.272: wtpDecodeDiscoveryResponse Discovery Latency: 0, WLC: IP= **Y.Y.Y.Y** , name=Cisco_7d:88:00, index
*Jan 01 08:00:09.272: Discovery Response from **Y.Y.Y.Y**
*Jan 01 08:00:09.273: Dot11 binding decode: Discovery Response
*Jan 01 08:00:09.273: wtpDecodeDiscoveryResponse Discovery Latency: 0, WLC: IP= **Y.Y.Y.Y** , name=Cisco_7d:88:00, index
*Jan 01 08:00:09.273: Discovery Response from **Y.Y.Y.Y**
*Jan 01 08:00:09.274: Dot11 binding decode: Discovery Response
*Jan 01 08:00:09.274: wtpDecodeDiscoveryResponse Discovery Latency: 0, WLC: IP= **Y.Y.Y.Y** , name=Cisco_7d:88:00, index
*Jan 01 08:00:12.133: Dropping dtls packet since session is not established. ab462383, 147e, c0a80121, 147e, 0
*Jan 01 08:00:19.182: Selected MWAR 'Cisco_7d:88:00'(index 0).
*Jan 01 08:00:19.183: Selected MWAR 'Cisco_7d:88:00' (index 0).
*Jan 01 08:00:19.183: Ap mgr count=1
*Jan 01 08:00:19.183: Go join a capwap controller
*Jan 01 08:00:19.183: Choosing AP Mgr with index 0, IP = **Y.Y.Y.Y** , load = 151..
*Jan 01 08:00:19.183: Synchronizing time with AC time.
*Feb 19 23:33:56.000: CAPWAP State: DTLS Setup.
*Feb 19 23:34:16.813: Dtls Session Established with the AC **Y.Y.Y.Y** , port= 5246

Discovery Request sent
If AP can not get IP address, then Discovery Req. will not be sent

Discovery resp. received from controller. If no response from controller, then need to check whether controller is accessible

Selected controller to join, timestamp synced to the controller

DTLS handshaking with the controller completed. If certificate has problem, then the failure will happen here

Event log 3

*Feb 19 23:34:16.813: CAPWAP State: Join.
*Feb 19 23:34:16.814: Join request: version=7.0.114.76

*Feb 19 23:34:16.815: Join request: hasMaximum Message Payload
*Feb 19 23:34:16.815: Dot11 binding encode: Encoding join request
*Feb 19 23:34:16.815: Sending Join Request Path MTU payload, Length 1376

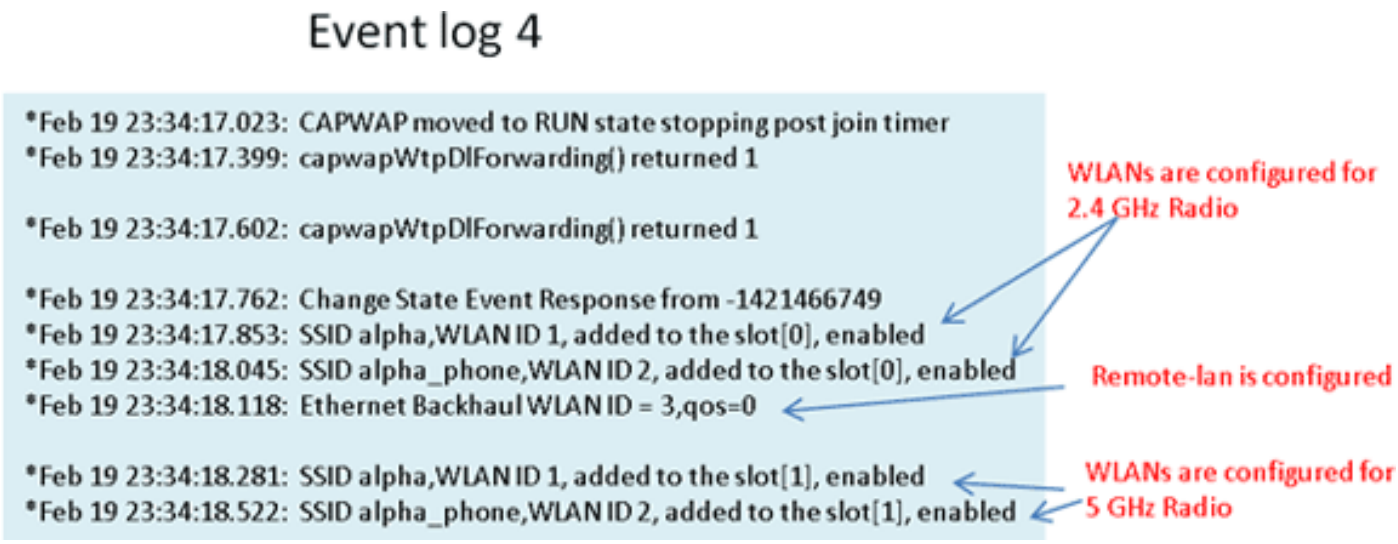
*Feb 19 23:34:16.887: Join Response from **Y.Y.Y.Y**
*Feb 19 23:34:16.888: PTMU : Setting MTU to : 1485

*Feb 19 23:34:16.888: Dot11 binding decode: Join Response
*Feb 19 23:34:16.889: Starting Post Join timer
*Feb 19 23:34:16.890: CAPWAP State: Image Data.
*Feb 19 23:34:16.890: Controller Version: 7.0.114.76
*Feb 19 23:34:16.890: AP Version: 7.0.114.76
*Feb 19 23:34:16.891: CAPWAP State: Configure.
*Feb 19 23:34:16.891: Dot11 binding encode: Encoding configuration status request.
*Feb 19 23:34:16.893: lwapp_encode_ap_reset_button_payload: reset button state off
*Feb 19 23:34:16.895: Configuration Status sent to **Y.Y.Y.Y**
*Feb 19 23:34:17.019: Configuration Status Response from **Y.Y.Y.Y**
*Feb 19 23:34:17.022: CAPWAP State: Run.
*Feb 19 23:34:17.022: Dot11 binding encode: Encoding change state event request.
*Feb 19 23:34:17.023: CAPWAP State: Run.

Join Resp. from controller
If AP is not added to AAA server, this step will fail.

Controller and AP have same version SW, no image download is need. When controller is upgraded to new version SW, image download will happen.

Capwap configuration completes



Quando la connessione a Internet non è affidabile

L'esempio del registro eventi riportato in questa sezione può verificarsi quando la connessione a Internet non riesce o risulta molto lenta o intermittente. Ciò può essere dovuto alla rete dell'ISP, al modem dell'ISP o al router di casa. A volte la connettività dall'ISP si interrompe o diventa inaffidabile. In questo caso, il collegamento CAPWAP (ritorno del tunnel alla rete aziendale) può non riuscire o avere difficoltà.

Di seguito è riportato un esempio di tale errore nel registro eventi:

```
*Feb 16 07:13:24.918: Re-Tx Count= 0, Max Re-Tx Value=5, NumofPendingMsgs=1
*Feb 16 07:13:36.919: Re-Tx Count= 4, Max Re-Tx Value=5, NumofPendingMsgs=2
*Feb 16 07:13:39.919: Max retransmission count exceeded going back to DISCOVER mode.
*Feb 16 07:13:39.919: Retransmission count for packet exceeded max(UNKNOWN_MESSAGE_TYPE (218103808)., 2)
*Feb 16 07:13:39.919: Retransmission count exceeded max, ignoring as the ethernet is overloaded
*Feb 16 07:13:42.918: Re-Tx Count= 6, Max Re-Tx Value=5, NumofPendingMsgs=2
Comment : This Retransmission continues on..... Multiple times..
*Feb 16 07:13:42.919: Max retransmission count exceeded going back to DISCOVER mode.
*Feb 16 07:13:42.919: Retransmission count for packet exceeded max(UNKNOWN_MESSAGE_TYPE (218103808)
*Feb 16 07:14:09.919: GOING BACK TO DISCOVER MODE
*Feb 16 07:14:09.920: CAPWAP State: DTLS Teardown.
*Feb 16 07:14:14.918: DTLS session cleanup completed. Restarting capwap state machine.
*Feb 16 07:14:14.919:
Lost connection to the controller, going to re-start evora...
```

Comandi aggiuntivi per il debug

Quando si utilizza Cisco Aironet serie 600 OEAP in un hotel o in un altro luogo a pagamento, prima che Cisco Aironet serie 600 OEAP possa eseguire il tunnel fino al controller, è necessario attraversare il giardino recintato. A tale scopo, collegare un notebook a una delle porte locali cablate (porta 1-3) o utilizzare un SSID personale per accedere all'hotel e visualizzare la schermata iniziale.

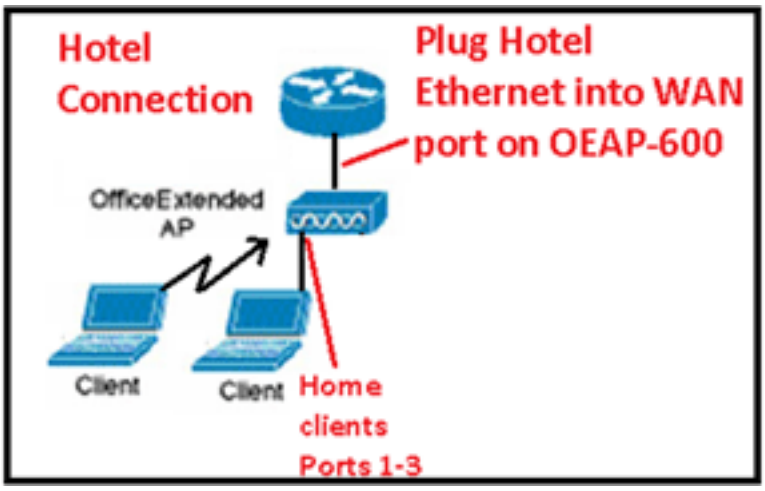
Una volta stabilita la connettività Internet dal lato domestico dell'access point, l'unità stabilisce un tunnel DTLS e gli SSID aziendali. Quindi, la porta cablata 4 (supponendo che sia configurata una LAN remota) diventa attiva.

Nota: l'operazione potrebbe richiedere alcuni minuti. Guarda il LED del logo Cisco in blu fisso o

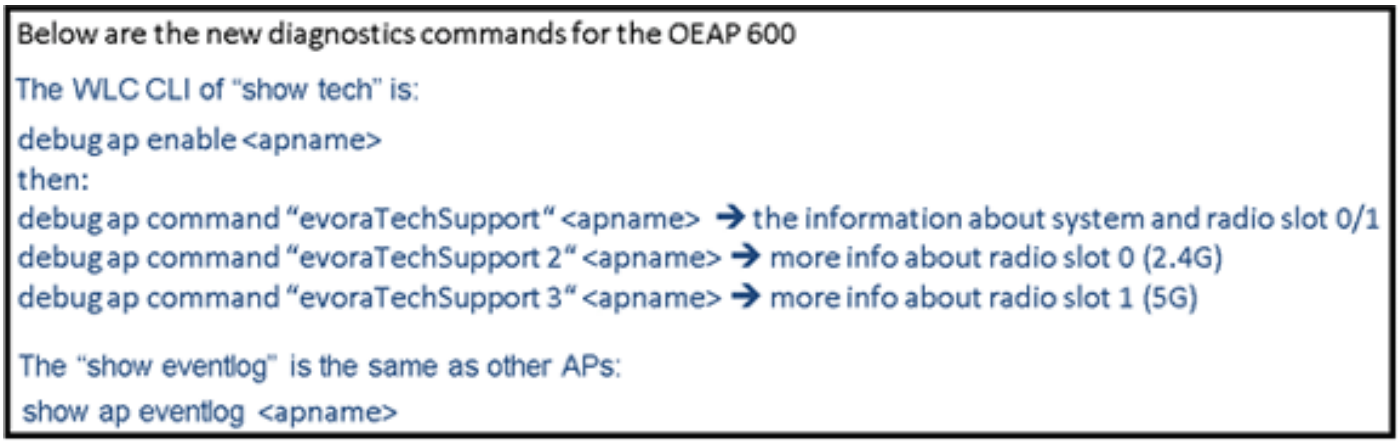
viola per segnalare che l'aggiunta è riuscita. A questo punto sono attive sia la connettività personale che quella aziendale.

Nota: il tunnel si interrompe quando un hotel o un altro ISP si disconnette (generalmente 24 ore). Poi, si deve ricominciare lo stesso processo. Si tratta di un comportamento normale e di progettazione.

In questa immagine viene illustrato Office Extend nella configurazione a pagamento:



Nell'immagine vengono mostrati i comandi di debug aggiuntivi (informazioni sull'interfaccia radio):



Problemi/avvertenze noti

Quando si carica il file di configurazione da un controller a un server TFTP/FTP, le configurazioni LAN remota vengono caricate come configurazioni WLAN. per ulteriori informazioni, fare riferimento alle note sulla versione per Cisco Wireless LAN Controller e Lightweight Access Point per la versione 7.0.116.0.

Su OEAP-600, se la connessione CAPWAP non riesce a causa di un errore di autenticazione sul controller, il LED del logo Cisco sull'OEAP-600 può spegnersi per un certo tempo prima che l'OEAP-600 tenti di riavviare il tentativo di connessione. Si tratta di un comportamento normale, quindi è necessario tenere presente che l'access point non è morto se il LED del logo si spegne momentaneamente.

Questo prodotto OEAP-600 ha un nome di accesso diverso da quello dei precedenti Access Point OEAP, per essere coerente con i prodotti di casa come Linksys, il nome utente predefinito è *admin* con una password di *admin* gli altri Cisco OEAP Access Point come AP-1130 e AP-1140

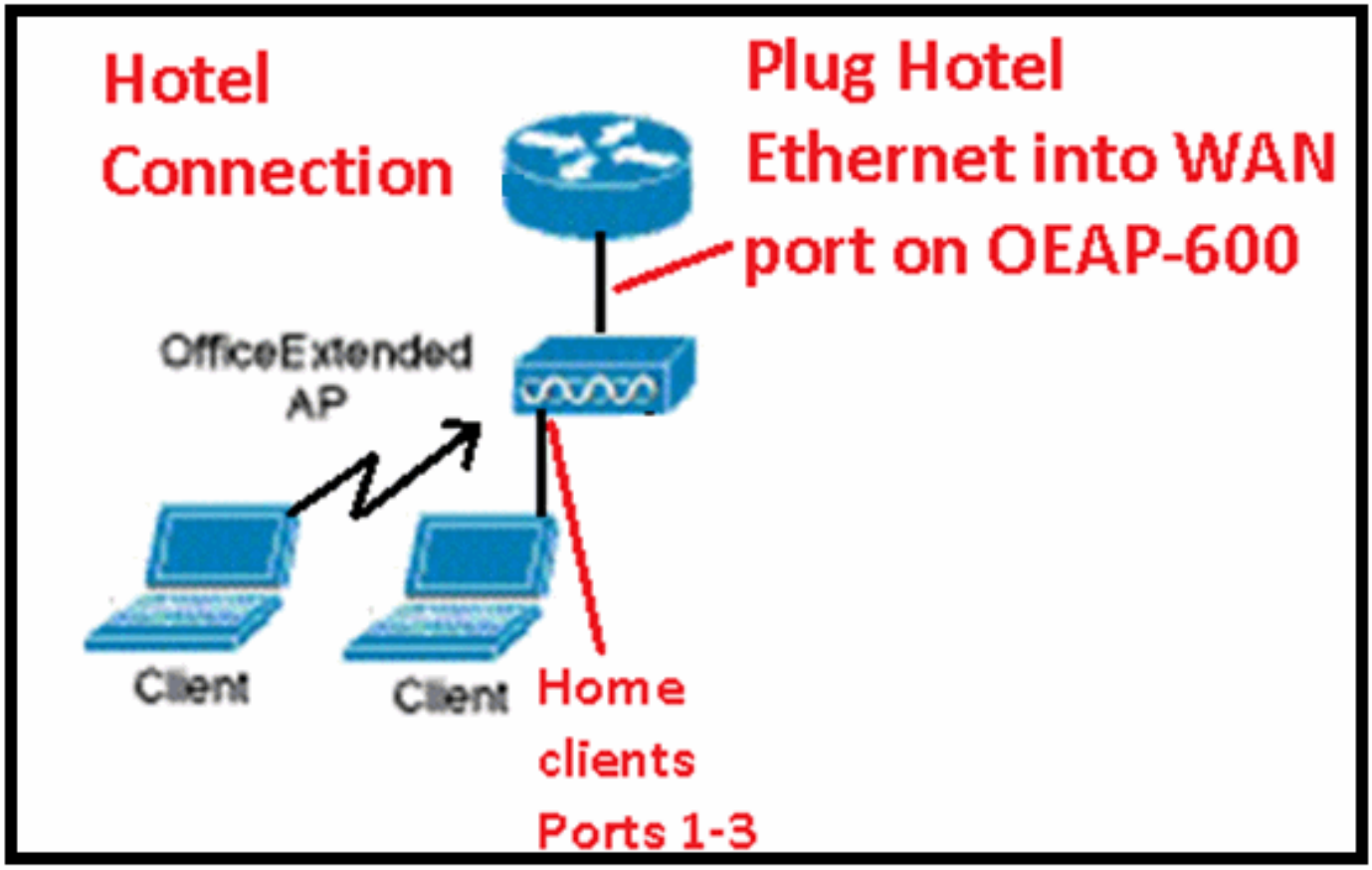
hanno un nome utente predefinito di *Cisco* con una password di *Cisco*.

questa prima versione di OEAP-600 ha supporto 802.1x, ma è supportata solo dalla CLI. Gli utenti che tentano di apportare modifiche alla GUI possono perdere le configurazioni.

Quando si utilizza l'OEAP-600 in un hotel o in un altro luogo a pagamento, prima che l'OEAP-600 possa tornare al controller, è necessario attraversare il giardino recintato. È sufficiente collegare un notebook a una delle porte locali cablate (porta 1-3) o utilizzare un SSID personale per accedere all'hotel e visualizzare la schermata iniziale. Una volta stabilita la connettività Internet dal lato domestico dell'access point, l'unità stabilisce un tunnel DTLS e gli SSID aziendali e la porta cablata #4, che si presume sia configurata la LAN remota, quindi diventa attiva. Notare che l'operazione potrebbe richiedere alcuni minuti, osservare il LED del logo Cisco per verificare se il colore è blu o viola a indicare che l'unione è riuscita. A questo punto sono attive sia la connettività personale che quella aziendale.

Nota: il tunnel può interrompersi quando un hotel o un altro ISP si disconnette (generalmente 24 ore) e sarà necessario riavviare lo stesso processo. Si tratta di un comportamento normale e di progettazione.

Office esteso in sede di pagamento per l'uso

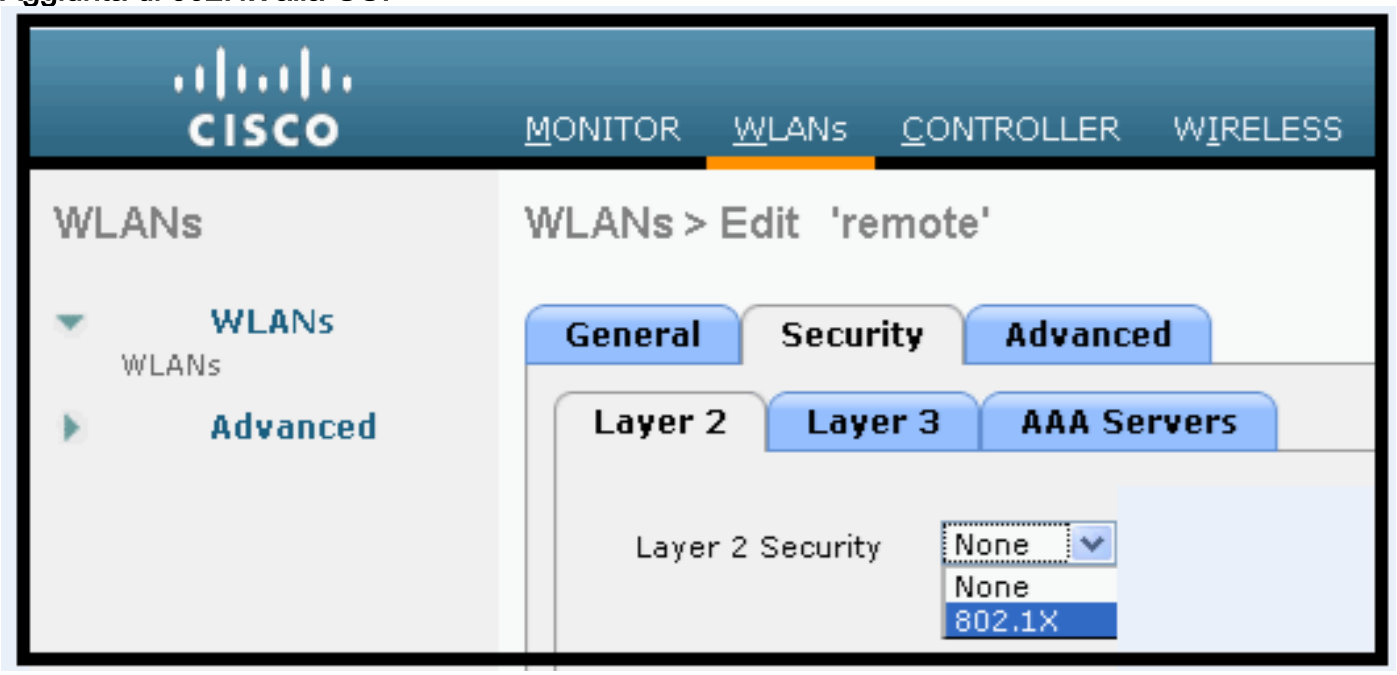


Di seguito sono riportati alcuni miglioramenti aggiuntivi introdotti nella release 7.2 di Cisco:

- Aggiunta della protezione 802.1x nella GUI
- Possibilità di disabilitare l'accesso WLAN locale sull'access point dal controller - disabilitazione del SSID personale che consente solo la configurazione aziendale
- Opzioni selezionabili per l'assegnazione dei canali
- Supporto modificato da 2 SSID aziendali a 3 SSID
- Supporto della funzione Dual RLAN Port

Aggiunta della protezione 802.1x nella GUI

Aggiunta di 802.1x alla GUI



Note relative all'autenticazione per la porta LAN remota.

802.1x authentication for remote-LAN port

WCS shall be provided to enable 802.1x Layer 2 Security and configure AAA server for remote-LAN. WEP encryption shall be always disabled.

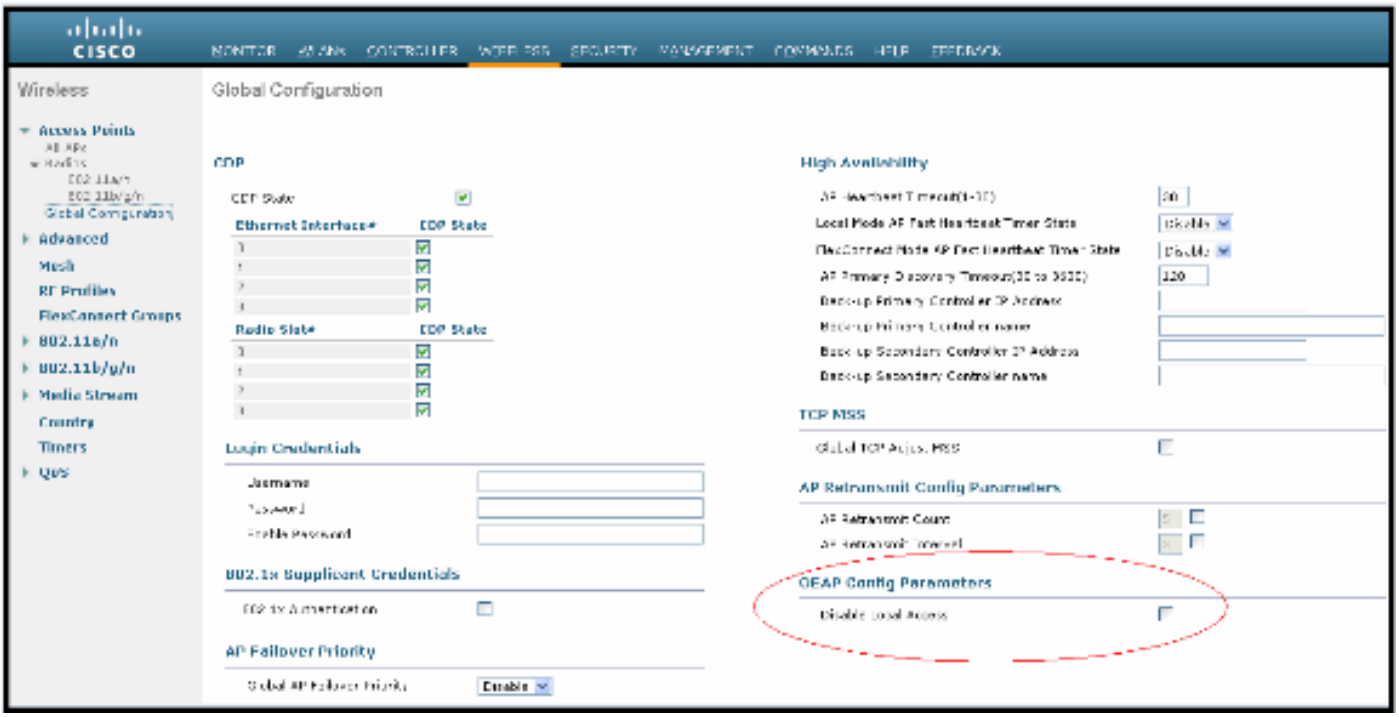
Same as 802.1x authentication for wireless clients, in 802.1x authentication for remote-LAN client, WLC acts as authenticator. Evora AP just forwards the EAPOL packets. AP converts EAPOL Ethernet packet to 802.11 data frame before sending it to WLC. The destination address in the 802.11 data frame shall be set to BSSID for remote-LAN. There is no data encryption for the Ethernet packets transferred on remote-LAN port. So there is no key exchange on EAPOL. The data security is provided by DTLS on CAPWAP data channel.

Following EAP methods are supported:

- EAP-TLS
- PEAP
- EAP-TTLS.

Possibilità di disabilitare l'accesso WLAN locale sull'access point dal controller - disabilitazione del SSID personale che consente solo la configurazione aziendale

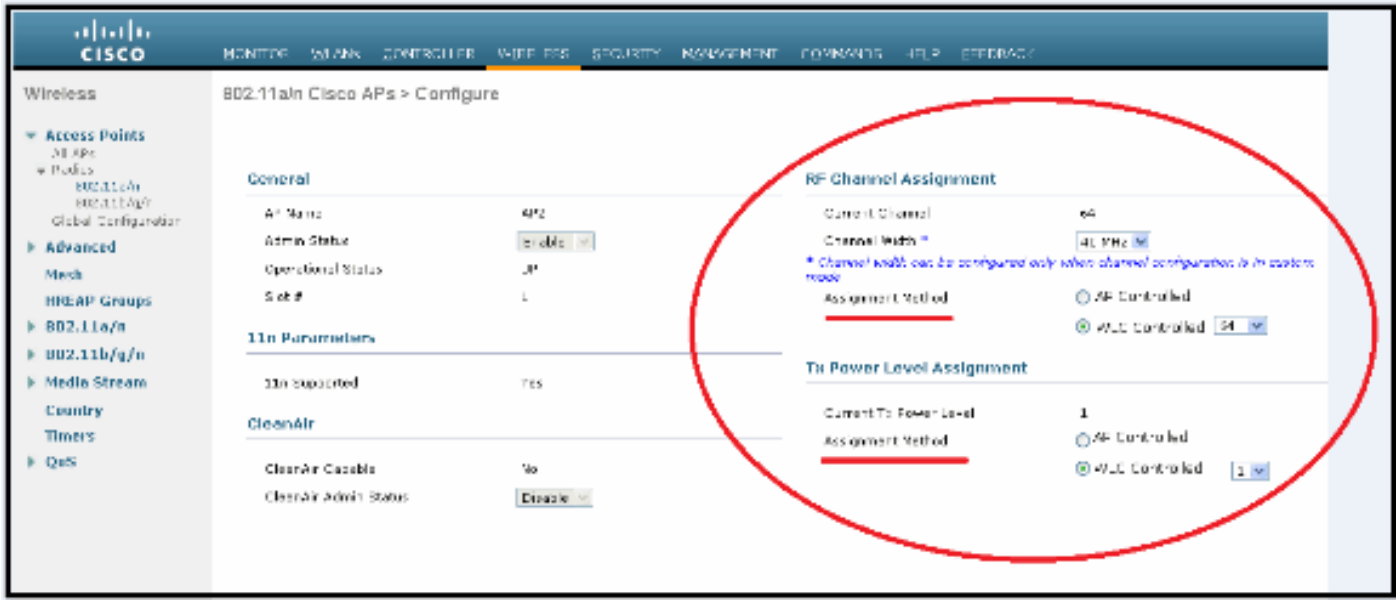
Disabilita accesso WLAN locale

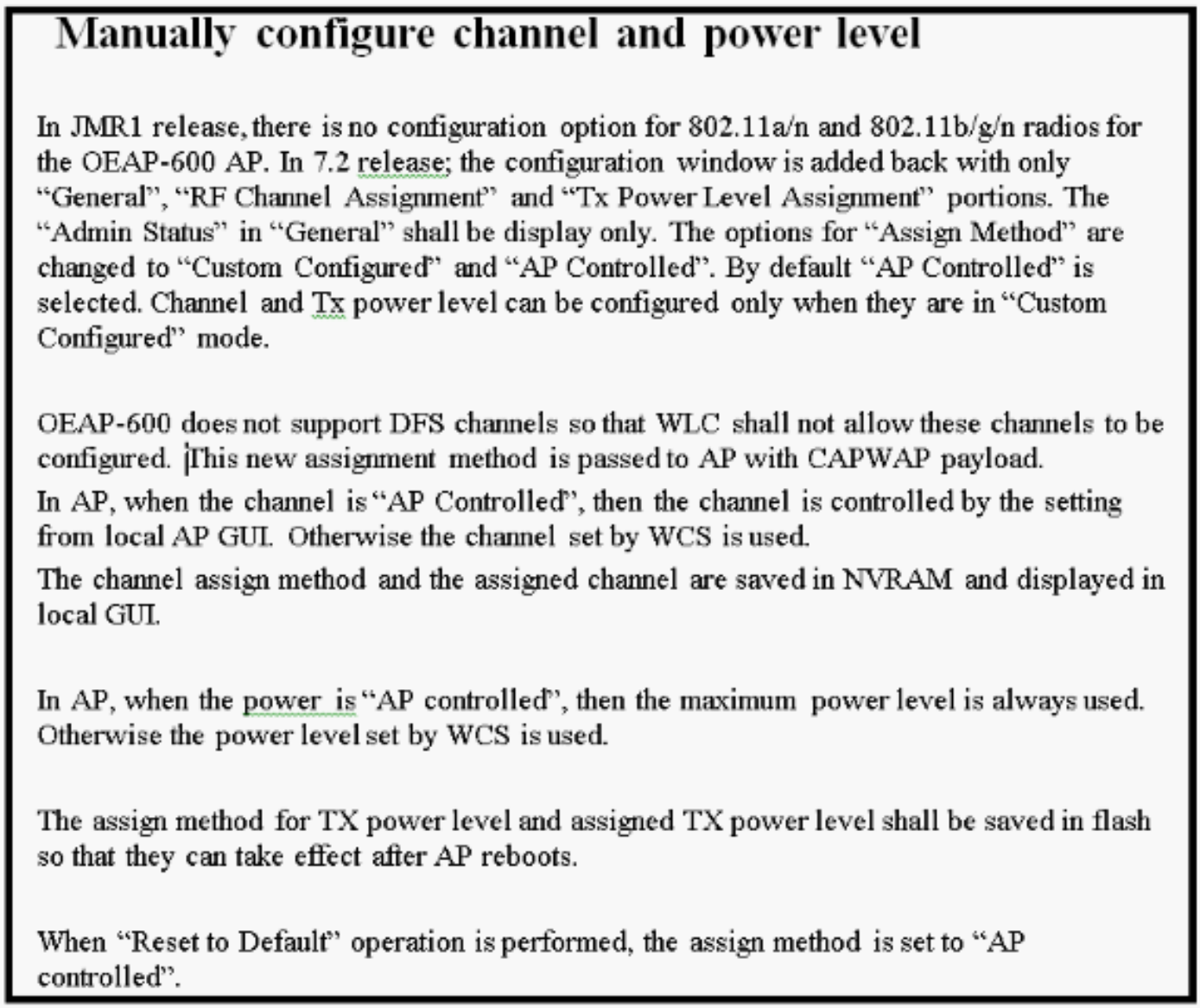


Le opzioni selezionabili per l'assegnazione dei canali sono:

- Controllo locale AP
- WLC controllato

Assegnazioni di alimentazione e canali RF ora locali o controllate da WLC





Supporto per la funzione Dual RLAN Port (solo CLI)

La presente nota si applica ai punti di accesso serie OEAP-600 che utilizzano la funzione Dual RLAN Ports, che consente alla porta Ethernet 3 OEAP-600 di funzionare come LAN remota. la configurazione è consentita solo dalla CLI e qui è riportato un esempio:

```
Config network oeap-600 dual-rlan-ports enable|disable
```

Nel caso in cui questa funzione non sia configurata, la LAN remota 4 a porta singola continuerà a funzionare. Ogni porta utilizza una lan remota univoca per ciascuna porta. Il mapping della rete LAN remota è diverso, a seconda che venga utilizzato il gruppo predefinito o i gruppi PA.

Gruppo predefinito

Se si utilizza il gruppo predefinito, alla porta 4 viene mappata una singola LAN remota con un ID di LAN remota pari. Ad esempio, la lan remota con id-lan-remota 2 è mappata alla porta 4 (sull'OEAP-600). La lan remota con un ID lan remoto dispari numerato viene mappata sulla porta 3 (sull'OEAP-600).

Ad esempio, prendiamo le due reti lan remote seguenti:

```
(Cisco Controller) >show remote-lan summary

Number of Remote LANS.......................... 2

RLAN ID  RLAN Profile Name    Status    Interface Name
-------  -----------------------------------  --------  --------------------
2        rlan2                                Enabled   management
3        rlan3                                Enabled   management
```

l'rlan2 ha un ID lan remota con numero pari, 2, e come tale viene mappata alla porta 4. l'ID 3 dell'rlan3 è dispari, quindi viene mappata alla porta 3.

Gruppi di AP

Se si utilizza un gruppo AP, la mappatura alle porte OEAP-600 è determinata dall'ordinamento del gruppo AP. Per utilizzare un gruppo AP, è necessario prima eliminare tutte le VLAN remote e le WLAN dal gruppo AP e lasciarlo vuoto. Quindi aggiungere le due reti lan remote al gruppo AP. Aggiungere prima la porta 3 AP LAN remota, quindi aggiungere il gruppo remoto della porta 4 e infine aggiungere le WLAN.

Una rete LAN remota nella prima posizione dell'elenco viene mappata alla porta 3, mentre la seconda posizione nell'elenco viene mappata alla porta 4, come nell'esempio seguente:

```
RLAN ID  RLAN Profile Name      Status    Interface Name
-------  -----------------------------------  --------  --------------------
2        rlan2                                Enabled   management
3        rlan3                                Enabled   management
```

Informazioni correlate

- Guida alla configurazione di Cisco Wireless LAN Controller, versione 7.0
- Documentazione e supporto tecnico – Cisco Systems

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).