Domande frequenti su Lightweight Access Point

Sommario

Introduzione

Questo documento offre informazioni sulle domande più frequenti (FAQ) sui Cisco Lightweight Access Point (LAP).

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

DOMANDE FREQUENTI SUI LAP

D. Che cos'è un Cisco Lightweight Access Point (LAP)?

R. Cisco LAP fa parte dell'architettura Cisco Unified Wireless Network. Un LAP è un access point progettato per essere collegato a un controller WLAN (Wireless LAN). Il LAP fornisce supporto dual band per IEEE 802.11a, 802.11b e 802.11g e monitoraggio simultaneo dell'aria per una gestione dinamica della radiofrequenza (RF) in tempo reale. I Cisco LAP gestiscono inoltre funzioni sensibili al tempo, ad esempio la crittografia di layer 2, che consentono alle WLAN di Cisco di supportare in modo sicuro applicazioni voce, video e dati.

Gli access point sono "leggeri", ossia non possono agire in modo indipendente da un controller WLC. Il WLC gestisce le configurazioni AP e il firmware. I punti di accesso sono "zero touch" implementati e la configurazione individuale dei punti di accesso non è necessaria. I punti di accesso sono leggeri anche in quanto gestiscono solo funzionalità MAC in tempo reale. Gli AP lasciano tutte le funzionalità MAC non in tempo reale che devono essere elaborate dal WLC. Questa architettura è nota come architettura "split MAC".

D. È possibile configurare il LAP in modo che funzioni indipendentemente da un controller WLC?

R. No, i LAP non possono funzionare in modo indipendente dai WLC. i LAP funzionano solo in combinazione con un WLC. Il motivo è che il WLC fornisce tutti i parametri di configurazione e il firmware necessari al LAP nel processo di registrazione.

D. Che cos'è il protocollo LWAPP (Lightweight AP Protocol)?

R. LWAPP è un protocollo bozza IETF (Internet Engineering Task Force) che definisce la

messaggistica di controllo per la configurazione e l'autenticazione dei percorsi e le operazioni di runtime. LWAPP definisce anche il meccanismo di tunneling per il traffico di dati.

Un LAP rileva un controller utilizzando i meccanismi di rilevamento LWAPP. Il LAP invia una richiesta di join LWAPP al controller. Il controller invia al LAP una risposta di join LWAPP che consente all'AP di unirsi al controller. Quando il LAP si unisce al controller, il LAP scarica il software del controller se le revisioni sul LAP e sul controller non corrispondono. Successivamente, il LAP è completamente sotto il controllo del controllore. LWAPP protegge la comunicazione di controllo tra il LAP e il controller tramite una distribuzione sicura delle chiavi. Per la distribuzione della chiave protetta sono necessari certificati digitali X.509 con provisioning già eseguito sia sul LAP che sul controller. Ai certificati preinstallati viene fatto riferimento con il termine "MIC", acronimo di Manufacturing Installed Certificate (Certificato di produzione installato). I Cisco Aironet AP forniti prima del 18 luglio 2005 non dispongono di un MIC. In questo modo, quando gli access point vengono aggiornati per funzionare in modalità lightweight, viene creato un certificato autofirmato (SSC). I controller sono programmati per accettare SSC per l'autenticazione di access point specifici.

D. Cos'è il protocollo CAPWAP?

R. Nella versione 5.2 del software del controller, i Lightweight Access Point Cisco usano il protocollo standard IETF CAPWAP (Control and Provisioning of Wireless Access Point) per comunicare con il controller e gli altri LAP della rete. Nelle versioni precedenti alla 5.2, per tali comunicazioni viene usato il protocollo LWAPP (Lightweight Access Point Protocol).

CAPWAP, basato su LWAPP, è un protocollo standard interoperabile che consente a un controller di gestire una serie di access point wireless. Il protocollo CAPWAP è stato implementato nella versione 5.2 per:

- Fornire uno strumento di aggiornamento dai prodotti Cisco con protocollo LWAPP ai prodotti Cisco di nuova generazione con protocollo CAPWAP
- Gestire i lettori RFID e dispositivi simili
- Consentire ai controller di interagire con access point di terze parti in futuro

Gli access point che usano il protocollo LWAPP possono rilevare e collegarsi a un controller con protocollo CAPWAP, senza che la conversione a tale controller richieda ulteriori interventi. Ad esempio, il processo di rilevamento del controller e il processo di download del firmware rimangono invariati sia con il protocollo CAPWAP sia con il protocollo LWAPP. L'unica eccezione riguarda le implementazioni di Layer 2, che non sono supportate dal protocollo CAPWAP.

Èpossibile implementare controller CAPWAP e controller LWAPP sulla stessa rete. Il software basato su CAPWAP permette agli access point di collegarsi a un controller con protocollo CAPWAP o con protocollo LWAPP. L'unica eccezione riguarda gli access point Cisco Aironet serie 1140, che supportano solo il protocollo CAPWAP e pertanto possono collegarsi solo ai controller che usano tale protocollo. Ad esempio, un access point serie 1130 può collegarsi a un controller che usa il protocollo CAPWAP o LWAPP, mentre un access point serie 1140 può collegarsi solo a un controller che usa il protocollo CAPWAP.

Per ulteriori informazioni, fare riferimento alla sezione Protocolli di comunicazione degli access point nella guida alla configurazione.

D. Come fare per distinguere un punto di accesso (autonomo) normale da un punto di accesso LAP?

R. Il modo più semplice per distinguere un access point normale da un LAP è quello di esaminare il numero di parte dell'access point.

- LAP (Lightweight AP Protocol [LWAPP]) - I numeri di parte iniziano *sempre* con **AIR-LAPXXXX**.
- Access point autonomo (software Cisco IOS®) - I numeri di parte iniziano *sempre* con **AIR-APXXXX**.

I Cisco Aironet serie 1000 LAP sono un'eccezione a questo criterio. I codici dei LAP serie 1000 sono:

- AIR-AP1010-A-K9 per 1010 LAP
- AIR-AP1020-A-K9 per 1020 LAP
- AIR-AP1030-A-K9 per 1030 LAP

Nota: i numeri di parte possono variare a seconda del paese e del dominio normativo. I numeri di parte forniti in questo elenco sono solo esempi.

Accertarsi di ordinare l'access point appropriato per la LAN wireless (WLAN) in uso.

D. Quali modelli AP possono eseguire il protocollo LWAPP (Lightweight AP Protocol)?

R. Queste piattaforme Cisco Aironet AP sono in grado di eseguire LWAPP:

- Aironet serie 1500
- Cisco Aironet serie 1250
- Aironet serie 1240 AG
- Aironet serie 1230 AG
- Aironet serie 1200
- Aironet serie 1130 AG
- Aironet serie 1000
- Aironet serie 1140 AP**Nota:** l'access point serie 1140 è supportato solo con WLC con versione 5.2 o successive.

Nota: è possibile ordinare questi access point Aironet con software Cisco IOS in modo che funzionino come access point autonomi o in modo che funzionino con LWAPP. Il numero di parte determina se un access point è un access point basato su software Cisco IOS o un access point basato su LWAPP. Ecco alcuni esempi:

- AIR-AP1242AG-A-K9 è un access point basato su software Cisco IOS.
- AIR-LAP1242AG-P-K9 è un access point basato su LWAPP.

Nota: i punti di accesso serie 1000 e 1500 sono eccezioni a questo criterio. Tutti i access point serie 1000 e 1500 supportano solo LWAPP.

D. Come installare e configurare un punto di accesso abilitato per LWAPP?

R. Gli access point abilitati per LWAPP fanno parte di Cisco Integrated Wireless Network Solution e non richiedono alcuna configurazione manuale prima del montaggio. L'access point è configurato da un Cisco Wireless LAN Controller (WLC) compatibile con LWAPP. Per informazioni su come installare e configurare inizialmente un access point abilitato per LWAPP, consultare la guida introduttiva ai Cisco Aironet Access Point abilitati per LWAPP.

D. Come configurare il LAP e il controller WLC insieme?

A. I LAP utilizzano il protocollo LWAPP (Lightweight AP Protocol) e, quando si uniscono a un WLC, il WLC invia ai LAP tutti i parametri di configurazione e il firmware. Per un'installazione di base, fare riferimento agli esempi di configurazione base di Wireless LAN Controller e Lightweight Access Point.

D. È possibile collegare un punto di accesso autonomo a un controller WLC (Wireless LAN Controller) e prevedere il corretto funzionamento dell'access point?

R. No, solo i LAP funzionano quando sono collegati a un WLC. I punti di accesso autonomi non comprendono il protocollo LWAPP (Lightweight AP Protocol) o il protocollo CAPWAP utilizzato dal WLC. Per connettere un access point autonomo a un WLC, è necessario prima convertire l'access point autonomo in modalità lightweight.

D. Dispongo di un access point autonomo basato su software Cisco IOS. È possibile convertirlo in modalità Lightweight?

R. Sì, ma non tutti i modelli AP autonomi basati su software Cisco IOS possono essere convertiti. Di seguito sono riportati i modelli che è possibile convertire in modalità Lightweight AP Protocol (LWAPP):

- Tutti i Cisco Aironet 1130 AG AP
- Tutti i access point Aironet 1240 AG
- In tutte le piattaforme modulari Aironet serie 1200 AP (1200/1220 Cisco IOS Software upgrade, 1210 e 1230 AP) basate su software Cisco IOS, la capacità di convertire l'access point dipende dalla radio.Se la radio è IEEE 802.11g, sono supportati MP21G e MP31G.Se la radio è IEEE 802.11a, sono supportati RM21A e RM22A.Èpossibile aggiornare i access point serie 1200 con qualsiasi combinazione di radio supportate:Solo GSolo ASia G che A

Nota: prima di poter essere convertito in LWAPP, un access point autonomo deve eseguire il software Cisco IOS versione 12.3(7)JA o successive.

Nota: solo i controller WLC (Wireless LAN Controller) Cisco 4400 e 2006 supportano i punti di accesso autonomi convertiti in modalità Lightweight. I WLC Cisco devono eseguire una versione minima del software 3.1. Cisco Wireless Control System (WCS) deve eseguire una versione minima della 3.1. L'utilità di aggiornamento è supportata sulle piattaforme Microsoft Windows 2000 e Windows XP.

Per ulteriori informazioni su come eseguire la conversione, fare riferimento a Aggiornamento dei Cisco Aironet Access Point autonomi in modalità Lightweight.

D. Quali restrizioni vengono applicate ai punti di accesso basati sul software Cisco IOS dopo la conversione in modalità Lightweight?

R. Tenere presenti le seguenti linee guida quando si utilizzano punti di accesso autonomi convertiti in modalità Lightweight:

- I punti di accesso convertiti in Lightweight AP Protocol (LWAPP) non supportano Servizi di dominio wireless (WDS). I punti di accesso convertiti in LWAPP comunicano solo con i

controller WLC (Cisco Wireless LAN) e non possono comunicare con i dispositivi WDS. Tuttavia, il WLC fornisce una funzionalità equivalente al WDS quando l'AP viene associato al WLC.

- I punti di accesso convertiti supportano solo i controller 2006, 4400 e WiSM. Quando si converte un punto di accesso autonomo in modalità lightweight, il punto di accesso può comunicare solo con i controller Cisco serie 2006, serie 4400 o con i controller di un Cisco WiSM.
- Nel software del controller versione 4.2 o successive, tutti i Cisco Lightweight Access Point supportano 16 BSSID per radio e un totale di 16 LAN wireless per access point. Nelle versioni precedenti, supportavano solo 8 BSSID per radio e un totale di 8 LAN wireless per punto di accesso. Quando un punto di accesso convertito viene associato a un controller, solo le LAN wireless con ID da 1 a 16 vengono inviate al punto di accesso.
- I punti di accesso convertiti in LWAPP devono ottenere un indirizzo IP e individuare il WLC usando DHCP, un DNS (Domain Name System) o una trasmissione subnet IP.
- I punti di accesso convertiti in LWAPP non supportano LWAPP di layer 2.
- I punti di accesso convertiti in LWAPP forniscono una porta console di sola lettura.
- Lo strumento di conversione dell'aggiornamento aggiunge l'hash della chiave SSC (Self-Sign Certificate) solo a uno dei controller del modulo WiSM Cisco. Al termine della conversione, aggiungere l'hash della chiave SSC al secondo controller del Cisco WiSM copiando l'hash della chiave SSC dal primo controller al secondo. Per copiare l'hash della chiave SSC, aprire la pagina Criteri AP della GUI del controller (**Security > AAA > Criteri AP**) e copiare l'hash della chiave SSC dalla colonna Hash della chiave SHA1 in AP Authorization List. Quindi, con la GUI del secondo controller, aprire la stessa pagina e incollare l'hash della chiave nel campo Hash chiave SHA1 in Aggiungi AP all'elenco di autorizzazioni. Se si dispone di più Cisco WiSM, utilizzare WCS per eseguire il push dell'hash della chiave SSC in tutti gli altri controller.

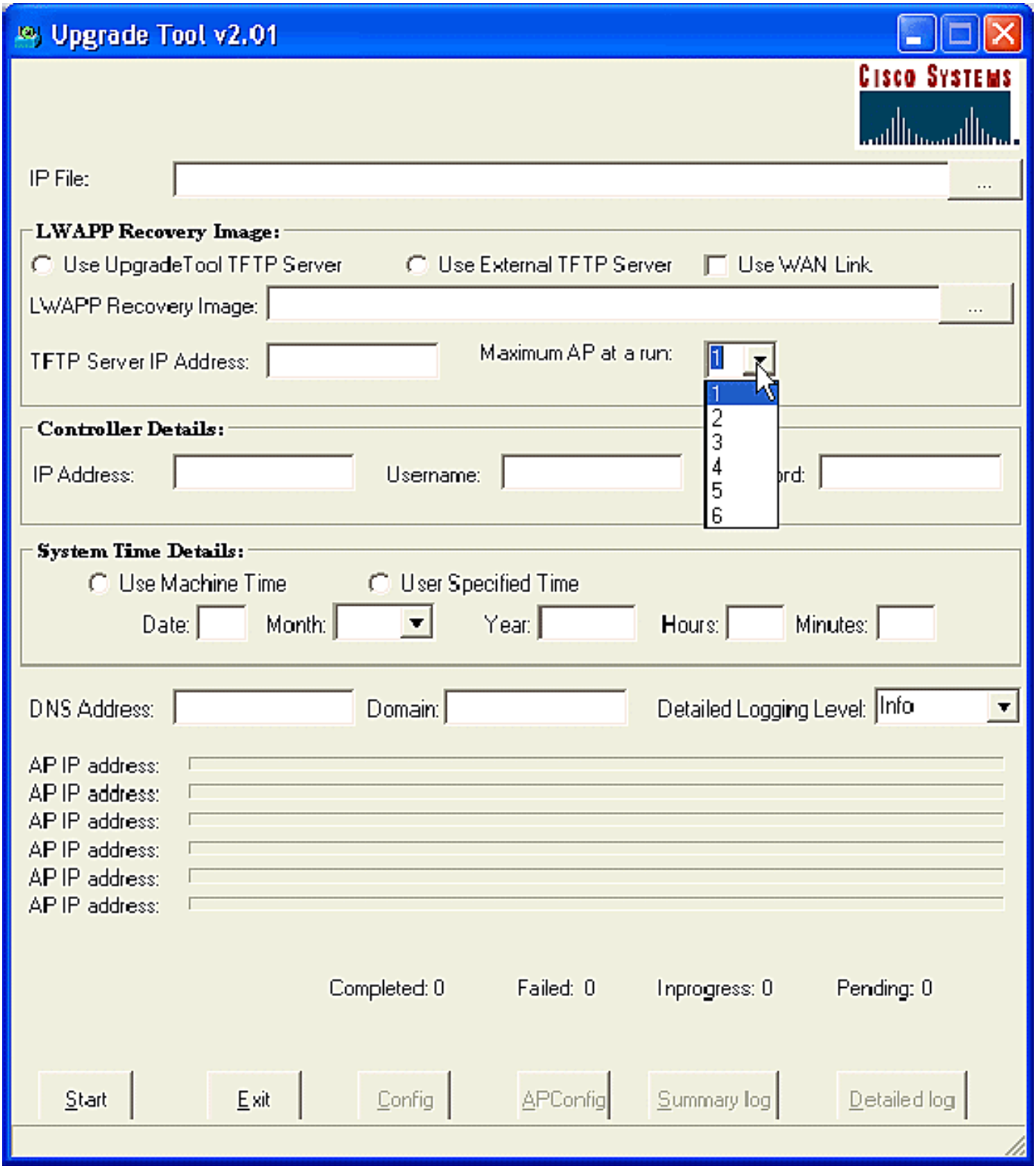
Per ulteriori informazioni, consultare le note di rilascio dei Cisco Aironet serie 1130AG, 1200, 1230AG e 1240AG Access Point per Cisco IOS versione 12.3(7)JX.

D. Il punto di accesso è stato convertito in modalità lightweight, ma è necessario riconvertirlo in modalità autonoma. È possibile?

R. Sì, è possibile riconvertire i punti di accesso autonomi convertiti in modalità lightweight in modalità autonoma. Completare la procedura descritta nella sezione *Riconversione di un Lightweight Access Point in modalità autonoma* in Aggiornamento dei Cisco Aironet Access Point autonomi in modalità Lightweight.

D. Quanti punti di accesso possono essere convertiti contemporaneamente tramite lo strumento di aggiornamento?

R. Con la versione 2.01 più recente dello strumento, è possibile aggiornare un massimo di sei access point alla volta.



D. L'access point è stato convertito in Lightweight AP Protocol (LWAPP), ma non viene registrato con il controller. Viene visualizzato il messaggio "`LWAPP Join-Request does not include valid certificate in CERTIFICATE_PAYLOAD from AP`." Quali sono le cause del problema?

R. Questo errore indica che i certificati digitali X.509 non sono validi. È possibile che l'ID bug Cisco sia CSCsd42296 (solo utenti registrati). Per risolvere questo problema, ripristinare gli access point ai valori predefiniti.

Un'altra possibilità è che il certificato autofirmato (SSC) non sia registrato sul WLC. Può essere

necessario aggiungere manualmente il SSC al controller. Per la procedura, fare riferimento al documento Self-Signed Certificate Manual Addition to the Controller for LWAPP-Converter AP (Aggiunta manuale certificato autofirmato al controller per gli access point convertiti in LWAPP).

D. È possibile configurare un access point basato su software Cisco IOS come bridge di gruppi di lavoro e associarlo a un access point basato su Lightweight AP Protocol (LWAPP)?

R. È possibile configurare un punto di accesso in modo che operi come bridge di gruppi di lavoro in modo che possa fornire connettività wireless a un punto di accesso leggero per conto dei client connessi tramite Ethernet al punto di accesso bridge di gruppi di lavoro. Quando si configura il punto di accesso come bridge di gruppi di lavoro e si esegue la connessione a una rete Cisco Unified, è possibile fornire connettività wireless ai client cablati connessi tramite Ethernet al punto di accesso del bridge di gruppi di lavoro. Ad esempio, se è necessario fornire connettività wireless a un gruppo di dispositivi cablati, è possibile collegare i dispositivi a un hub o a uno switch, collegare l'hub o lo switch alla porta Ethernet del punto di accesso e configurare il punto di accesso come bridge di gruppi di lavoro.

Il documento Workgroup Bridge in a Cisco Unified Wireless Network Configuration Example fornisce un esempio di configurazione.

D. Un client wireless può spostarsi tra i punti di accesso LWAPP e i punti di accesso autonomi?

R. No, il roaming tra LAP e AP autonomi NON è supportato. Il motivo è che, quando collegato ai punti di accesso LWAPP, il traffico viene trasmesso tramite un tunnel LWAPP. Poiché non esiste un tunnel per la mobilità tra il controller LAN wireless e i punti di accesso autonomi, il roaming non funziona.

D. Quali opzioni di antenna sono disponibili con i diversi modelli di Cisco Aironet serie 1000 LAP?

R. L'enclosure LAP serie 1000 contiene:

- Un'antenna radio IEEE 802.11a o 802.11b/g
- Quattro antenne interne ad alto guadagno (due 802.11a e due 802.11b/g)

Èpossibile attivare o disattivare queste antenne in modo indipendente in modo da produrre un'area di copertura a 180 gradi in più sezioni o omnidirezionale a 360 gradi. Alcuni LAP serie 1000 possono usare anche antenne esterne. I LAP serie 1000 sono disponibili in tre modelli:

- 1010 LAP
- 1020 LAP
- 1030 LAP

Le opzioni disponibili per l'antenna sono le seguenti:

- LAP 1010:Quattro antenne interne ad alto guadagnoNessun adattatore per antenna esterna
- 1020 LAP:Quattro antenne interne ad alto guadagnoUn adattatore per antenna esterna da 5 GHzDue adattatori per antenna esterna da 2,4 GHz
- 1030 LAP (remote-edge LAP):Quattro antenne interne ad alto guadagnoUn adattatore per

antenna esterna da 5 GHzDue adattatori per antenna esterna da 2,4 GHz

A. External-Antenna Model B. Internal-Antenna Model

Nota: i LAP serie 1000 devono usare antenne interne o esterne fornite in fabbrica per evitare una violazione dei requisiti FCC e l'annullamento dell'autorizzazione utente per l'uso dell'apparecchiatura.

D. Quali opzioni di alimentazione sono disponibili per i Cisco Aironet serie 1000 LAP?

R. Aironet serie 1000 LAP può ricevere alimentazione da un alimentatore esterno da 110 a 220 V CA a 48 V CC o da un'apparecchiatura Power over Ethernet. L'alimentatore esterno (AIR-PWR-1000) è collegato a una presa elettrica sicura da 110 a 220 V CA. Il convertitore produce l'uscita da 48 V CC richiesta per i LAP serie 1000. L'uscita del convertitore viene inserita nel lato del LAP serie 1000 tramite un jack da 48 V DC.

Nota: è possibile ordinare l'alimentatore esterno AIR-PWR-1000 con cavi di alimentazione specifici del paese. Per ricevere il cavo di alimentazione corretto, contattare Cisco al momento dell'ordine.

D. È possibile utilizzare Telnet/SSH in un access point basato su LWAPP?

R. In Wireless LAN Controller release 5.0 e successive, il controller supporta l'uso dei protocolli Telnet o Secure Shell (SSH) per la risoluzione dei problemi dei Lightweight Access Point. È possibile utilizzare questi protocolli per semplificare il debug, in particolare quando il punto di accesso non è in grado di connettersi al controller. Il supporto Telnet e SSH può essere configurato solo dalla CLI del controller.

Per abilitare la connettività Telnet o SSH su un punto di accesso, usare il comando **config ap {telnet | ssh}**. Il Cisco Lightweight Access Point viene associato a questo controller LAN wireless Cisco per tutte le operazioni di rete e in caso di ripristino dell'hardware.

```
config ap {telnet | ssh} {enable | disable} Cisco_AP
```

Esempi

```
> config ap telnet enable cisco_ap1
> config ap telnet disable cisco_ap1
> config ap ssh enable cisco_ap2
> config ap ssh disable cisco_ap2
```

D. Come configurare le credenziali globali per i punti di accesso. Quali sono il nome utente e la password predefiniti nella release 5.0?

R. I punti di accesso Cisco IOS vengono forniti dalla fabbrica con Cisco come password di abilitazione predefinita. Questa password consente agli utenti di accedere in modalità non privilegiata e di eseguire i comandi show e debug, il che rappresenta una minaccia per la sicurezza. Per impedire accessi non autorizzati e consentire agli utenti di eseguire i comandi di configurazione dalla porta della console del punto di accesso, è necessario modificare la password di abilitazione predefinita.

Nel software del controller precedente alla versione 5.0, è possibile impostare la password di abilitazione del punto di accesso solo per i punti di accesso attualmente connessi al controller. Nel software controller versione 5.0, è possibile impostare un nome utente globale, una password e una password di abilitazione che tutti i punti di accesso ereditano quando si uniscono al controller. Sono inclusi tutti i punti di accesso attualmente collegati al controller e quelli che verranno aggiunti in futuro. Se lo si desidera, è possibile ignorare le credenziali globali e assegnare un nome utente, una password e una password di abilitazione univoci per un punto di accesso specifico.

Per informazioni su come configurare le credenziali globali dell'access point, consultare il documento sulla configurazione delle credenziali globali per i punti di accesso.

D. Se si dispone di Wireless LAN Controller (WLC) 2006 e di un access point (AP) 1242 con versione firmware 3.2.78.0, si verificano problemi con i punti di accesso che si connettono ad esso e si ricevono questi messaggi di errore: "lwapp_client_error;not receive read response(3). Lwapp_image_broc;cannot to open TAR file" (Impossibile aprire il file TAR)

R. Gli access point serie 1242 vengono convertiti in Lightweight Access Point Protocol (LWAPP) AP. Una volta convertiti e usati, cercano il controller per potersi unire. Se gli access point non trovano il controller, sulla console viene visualizzato questo tipo di messaggio. Tuttavia, in questo caso, il controller ha una versione firmware 3.2.78.0 che non è compatibile con i punti di accesso aggiornati. Per utilizzare i punti di accesso aggiornati è necessario disporre della versione firmware 3.2.116.21. Una volta aggiornato il firmware del controller, questi AP si uniscono al controller e iniziano a funzionare.

D. I client mostrano un indirizzo MAC di 00:17:0f:37:65:c4 quando sono collegati a un punto di accesso, ma il punto di accesso mostra che l'indirizzo MAC radio di base è 00:17:0f:37:65:c0. Perché il client mostra un indirizzo MAC diverso dal punto di accesso? È possibile determinare quale indirizzo MAC viene registrato dal dispositivo se si dispone di due punti di accesso con indirizzi MAC molto vicini?

R. Se si controlla un punto di accesso in modalità dettagliata, si osserverà che ha un indirizzo MAC Radio di base e un indirizzo MAC FastEthernet. Inoltre, questo è l'indirizzo MAC della radio di base che cambia con la WLAN. Il client vede effettivamente il BSSID sotto forma di indirizzo MAC.

D. Dispongo già di una rete wireless (access point autonomi) con un access point configurato come ripetitore. È necessario eseguire la migrazione della rete a una rete wireless LWAPP. È possibile utilizzare gli access point LWAPP come ripetitori?

R. Gli access point LWAPP devono essere collegati a un controller e non supportano la modalità ripetitore in quanto prima devono essere connessi al controller. I Cisco AP autonomi possono essere configurati come ripetitori, ma a causa della riduzione della larghezza di banda effettiva disponibile per i client finali, i ripetitori non sono la configurazione più consigliata. Mentre qualsiasi modello Cisco Aironet AP o LAP può essere utilizzato in modalità LWAPP o autonoma, per apportare la modifica è necessaria una nuova immagine software. Questo è particolarmente complesso quando va da autonomo a LWAPP, quindi direttamente, no, un AIR-LAP1232AG-A-K9 non supporta la modalità ripetitore in modo nativo. Potrebbe essere caricato con un software autonomo ed essere fatto per supportare la modalità ripetitore, ma ciò implicherebbe una modifica del software e una configurazione separata.

D. Quanti access point possono supportare i WLC?

R. Il numero di AP supportati per WLC dipende dal numero di modello:

- **2106**: un WLC standalone che supporta fino a 6 AP con 8 interfacce Fast Ethernet.
- **4402** - WLC standalone che supporta 12, 25 o 50 AP.
- **4404**: un WLC standalone che supporta 100 AP.
- **5500**: WLC standalone che supporta 12, 25, 50, 100 o 250 punti di accesso per i servizi wireless business-critical in ubicazioni di tutte le dimensioni.
- **WLCM**: modulo WLC progettato specificamente per la serie Cisco Integrated Service Router (ISR). Attualmente è disponibile nelle versioni 6, 8 o 12 AP.
- **WS-C3750G**: un WLC che supporta 25 o 50 AP integrati con lo switch Catalyst 3750. Le connessioni backplane del WLC vengono visualizzate come porte Ethernet a 2 Gigabit che possono essere configurate separatamente come trunk dot1q per fornire la connessione allo switch 3750. In alternativa, le porte Gig possono essere collegate in modo aggregato per fornire una singola connessione EtherChannel allo switch 3750. Poiché il WLC è integrato direttamente, ha accesso a tutte le funzionalità avanzate di routing e switching disponibili nello switch 3750 con stack. Questo WLC è ideale per uffici o edifici di medie dimensioni. La versione `50 AP' può scalare fino a 200 AP quando quattro 3750 sono impilati insieme come switch virtuale.
- **WiSM**: modulo WLC progettato appositamente per gli switch Catalyst serie 6500 di Cisco. Supporta fino a 300 AP per modulo. A seconda della piattaforma 6500, è possibile installare

più WISM per offrire funzionalità di scalabilità significative. Il WiSM appare come un'unica interfaccia di collegamento aggregato sullo switch 6500 che può essere configurata come trunk dot1 per fornire la connessione al backplane 6500. Questo modulo è ideale per grandi edifici o campus.

D. Qual è il numero massimo di associazioni client supportate dai punti di accesso?

R. Il numero massimo di associazioni client che i punti di accesso possono supportare dipende dai seguenti fattori:

- Il numero massimo di associazioni client è diverso per i punti di accesso IOS lightweight e autonomi.
- Èpossibile che vi sia un limite per radio e un limite complessivo per access point.
- Hardware AP (i punti di accesso da 16 MB hanno un limite inferiore rispetto ai punti di accesso da 32 MB e superiori).

Per dettagli completi sui limiti delle associazioni dei client, fare riferimento alla sezione *Client Association Limits* della guida alla configurazione di Cisco Wireless LAN Controller, versione 7.0.

D. L'access point serie 1252 supporta il bridging?

R. Sì, la modalità bridging è supportata sui access point serie 1252.

D. L'infrastruttura LWAPP (Lightweight AP Protocol) supporta PPP over Ethernet (PPPoE) (da client PC a server PPPoE)?

R. No, l'infrastruttura LWAPP non supporta PPPoE. Il motivo è che l'Ethertype PPPoE viene scartato nel controller.

D. Come ripristinare manualmente i Cisco Aironet serie 1000 LAP?

A. È possibile ripristinare l'access point ai valori predefiniti tramite il controller WLAN (Wireless LAN). Per effettuare il reset, il LAP deve essere registrato sul WLC.

Attenersi alla seguente procedura:

1. Dall'interfaccia utente del WLC, fare clic su **Wireless**. La scheda Wireless consente di accedere alla configurazione di rete wireless della soluzione Cisco WLAN.
2. Scegliere **Access Point > Cisco AP**, quindi fare clic su **Detail** per passare alla finestra dell'access point specifico.
3. Fare clic su **Clear Config** in fondo alla finestra. In questo modo la configurazione sul LAP viene cancellata e ripristinata ai valori predefiniti.

Per ripristinare i LAP ai valori predefiniti con l'uso dell'interfaccia della riga di comando (CLI), usare il comando **clear ap-config** ***ap-name*** dalla CLI del WLC.

D. Dove posso trovare ulteriori informazioni sui Cisco Aironet serie 1000 LAP?

R. Fare riferimento a Cisco serie 1000 Lightweight Access Point - Domande e Risposte. Il documento contiene le risposte a molte domande relative ai LAP serie 1000.

D. Quali dispositivi Cisco supportano la modalità LWAPP (Lightweight AP Protocol) Layer 2?

R. La modalità LWAPP layer 2 è supportata solo sui seguenti dispositivi Cisco:

- Cisco serie 4100 Wireless LAN Controller (WLC)
- Cisco serie 4400 WLC
- Cisco Aironet serie 1000 LAP

D. I Cisco LAP utilizzano una stringa VCI (Vendor Class Identifier) con l'opzione DHCP 43 per rilevare i controller. Qual è il valore della stringa VCI per i Cisco LAP?

A. I Cisco Aironet serie 1000 AP utilizzano un formato di stringa per l'opzione DHCP 43, mentre gli altri access point Aironet utilizzano il formato tipo, lunghezza e valore (TLV) per l'opzione DHCP 43. È necessario programmare i server DHCP in modo che restituiscano l'opzione sulla base della stringa VCI DHCP del access point (opzione DHCP 60). Questa tabella fornisce i valori della stringa VCI per i diversi LAP:

Access Point	Vendor Class Identifier (VCI)
Cisco Aironet 1000 series	Airespace.AP1200
Cisco Aironet 1100 series	Cisco AP c1100
Cisco Aironet 1130 series	Cisco AP c1130
Cisco Aironet 1200 series	Cisco AP c1200
Cisco Aironet 1240 series	Cisco AP c1240
Cisco Aironet 1300 series	Cisco AP c1300
Cisco Aironet 1500 series	Cisco AP c1500[1]
	Cisco AP.OAP1500[2]
	Cisco AP.LAP1505[3]
	Cisco AP.LAP1510[4]
	Airespace.AP1200[5]
Cisco 3201 Lightweight Access Point	Cisco AP C3201WMIC

D. Qual è il significato dei valori del blocco TLV (Type Length Value) rispetto all'opzione DHCP 43? Come viene calcolato il valore TLV?

A. L'opzione DHCP 43 può essere abilitata sul server DHCP del router Cisco IOS usando questo comando:

```
Option 43 hex <string>
```

La stringa esadecimale di questo comando viene assemblata concatenando i valori TLV dell'opzione secondaria dell'opzione 43.

tipo, lunghezza e valore

- **Il tipo** è sempre il codice dell'opzione secondaria 0xf1.
- **La lunghezza è il numero degli indirizzi IP di gestione dei controller moltiplicato per 4 in formato esadecimale.**
- **Il valore è l'indirizzo IP del controller riportato in sequenza in formato esadecimale.**

Si supponga, ad esempio, di avere due controller con i seguenti indirizzi IP dell'interfaccia di gestione 10.126.126.2 e 10.127.127.2:

- Il tipo è 0xf1.
- La lunghezza è 2 * 4 = 8 = 0x08.
- Gli indirizzi IP sono convertiti in 0a7e7e02 (10.126.126.2) e 0a7f7f02 (10.127.127.2).
- L'assemblaggio della stringa restituisce f1080a7e7e020a7f7f02. Il comando IOS aggiunto all'ambito DHCP è:

```
option 43 hex f1080a7e7e020a7f7f02
```

D. Il controller WLC supporta il bilanciamento del carico del punto di accesso?

R. Sì, è possibile eseguire il bilanciamento del carico AP su un WLC. Per ulteriori informazioni, fare riferimento alle domande frequenti (FAQ) sulla risoluzione dei problemi dei controller WLC.

D. Come configurare il failover del controller WLC (Wireless LAN Controller) per i LAP?

A. Per i dettagli su come configurare il failover WLC, consultare l'esempio di configurazione del failover del controller WLAN per i Lightweight Access Point.

D. Come è possibile disattivare il pulsante di reset sugli access point dopo la conversione dalla modalità autonoma a Lightweight?

R. È possibile disattivare il pulsante di ripristino sui punti di accesso convertiti in modalità lightweight. Il pulsante di reset è etichettato "MODE" sulla parte esterna dell'access point. Utilizzare questo comando per disabilitare o abilitare il pulsante reset su uno o tutti gli access point convertiti associati a un controller:

```
config ap reset-button {enable | disable} {ap-name | all}
```

Per impostazione predefinita, il pulsante Reimposta sui punti di accesso convertiti è attivato.

D. Posso avere un Lightweight AP Protocol (LWAPP) compatibile con AP collegato su un collegamento WAN dal controller WLC? In caso affermativo, come funziona?

R. Sì, alcuni LAP supportano la funzione denominata REAP (Remote-Edge AP). Con questa funzione, è possibile avere un LAP su un collegamento WAN dal WLC a cui si connette il LAP. 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. Per un esempio dettagliato dell'installazione, fare riferimento agli esempi di configurazione dei Remote-Edge AP (REAP) con Lightweight AP e Wireless LAN Controller (WLC).

Nota: a questo punto, la modalità REAP è supportata solo sui Cisco Aironet 1030 LAP. In futuro, la funzionalità REAP sarà disponibile su una gamma più ampia di LAP.

D. Sui punti di accesso in modalità monitor abbiamo ancora gli stessi vincoli WAN applicati ai punti di accesso normali e ai punti di accesso H-REAP? In altre parole, è necessario un tempo di RTD di 100 ms o superiore tra il controller e un punto di accesso in modalità monitor?

R. No, l'access point in modalità monitoraggio non ha la restrizione di 100 ms perché non c'è associazione client, questo è il motivo della restrizione. Il limite di latenza di 100 ms è stato creato sulla base di requisiti di autorizzazione client diversi e spesso rigidi, motivo per cui sia la modalità locale che i punti di accesso H-REAP hanno limiti di latenza identici. Ovviamente, i punti di accesso in modalità monitor non hanno le stesse limitazioni del client.

D. La versione WLC è 3.2. È configurata per il protocollo LWAPP (Lightweight Access Point Protocol) di layer 3. L'MTU della rete tra il WLC e il mio Lightweight Access Point (LAP) è configurata come 900 byte. L'access point LWAPP non riesce a collegarsi a questo WLC. Quale può essere la ragione di questo?

R. L'MTU configurata nello scenario è 900 byte. Tuttavia, una richiesta di aggiunta LWAPP supera i 1500 byte. LWAPP richiede un frammento della richiesta di partecipazione a LWAPP. La logica di tutti gli access point LWAPP è che le dimensioni del primo frammento sono 1500 byte (incluse le intestazioni IP e UDP) e del secondo frammento sono 54 byte (incluse le intestazioni IP e UDP). Se la rete tra gli access point LWAPP e il WLC ha una dimensione MTU inferiore a 1500 (ad esempio VPN, GRE, MPLS e così via), come nel tuo caso, il WLC non può gestire la richiesta di aggiunta LWAPP. Pertanto, LWAPP non è in grado di collegarsi al controller.

Per gestire questa situazione, aggiornare il controller alla versione 4.0. Questa versione è in grado di gestire frammenti di layer 3. Per ulteriori informazioni sul problema, fare riferimento all'ID bug Cisco CSCsd94967 (solo utenti registrati).

D: Ho un WLC che ho ricevuto da Singapore. Con questo WLC, intendevo connettere un ufficio remoto per la connettività wireless. Ho uffici in altri paesi. Tuttavia, ricevo messaggi di errore del dominio normativo dal WLC di Singapore. Esiste un modo per forzare il WLC ad accettare punti di accesso (AP) con domini normativi diversi? Il messaggio di errore che ricevo è: "**Impossibile associare il punto di accesso 'AP_NAME'. Il dominio normativo configurato su di esso '-R' non corrisponde al codice paese 'A.B.C.D' del controller 'SG - Singapore**"

R. Il WLC supporta un solo dominio normativo. Pertanto, un WLC che utilizza il dominio normativo -A può essere utilizzato solo con i punti di accesso che utilizzano il dominio normativo -A (e così via). In questo caso, il WLC è impostato su -SG per Singapore, quindi supporta solo gli access point nel dominio normativo di Singapore.

Quando si acquistano access point e WLC, accertarsi che condividano lo stesso dominio normativo. Solo in questo caso gli AP possono registrarsi sul WLC.

Supporto di più codici di paese: con WLC versione 4.1.171.0 e successive, il supporto di più codici di paese è stato introdotto con i WLC. Con la versione 4.1.171.0 e successive, è possibile configurare fino a 20 codici paese per controller. Il supporto di più codici paese consente di gestire

gli access point in vari paesi da un unico controller. Questa funzione non è supportata per l'uso con i punti di accesso mesh Cisco Aironet.

D. Quali sono le diverse modalità di funzionamento di un Lightweight Access Point (LAP)?

R. Un LAP può funzionare in una delle seguenti modalità:

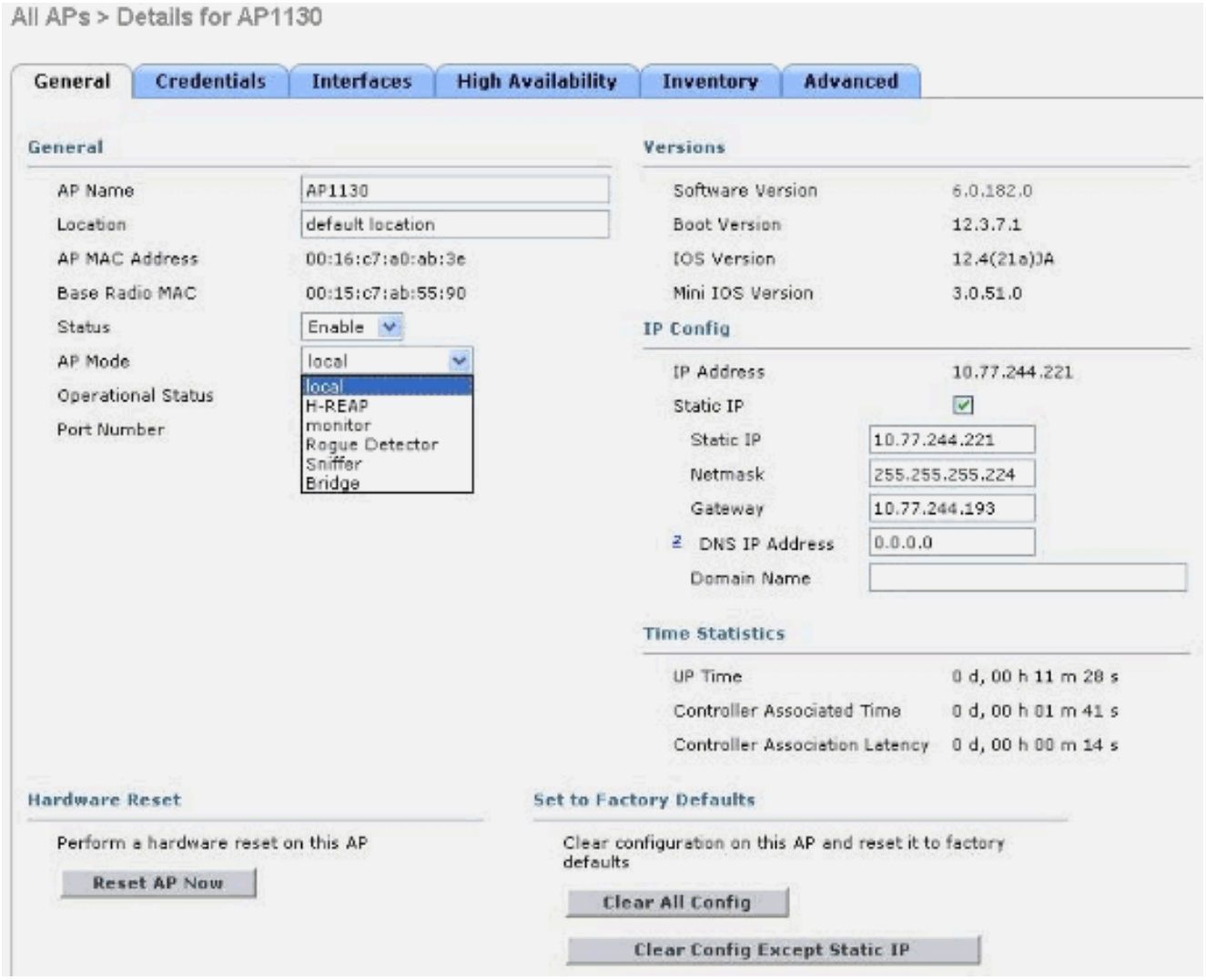
- **Modalità locale (Local mode**) - Questa è la modalità operativa di default. Quando si attiva la modalità locale per un LAP, l'AP trasmette sul canale normalmente assegnato. Tuttavia, l'access point controlla anche tutti gli altri canali nella banda per un periodo di 180 secondi, per scansionare ciascuno degli altri canali per 60 ms durante il tempo di non trasmissione. Durante questo periodo, l'access point esegue misurazioni della soglia del rumore, misura le interferenze e cerca gli eventi IDS.
- **Modalità REAP**: la modalità REAP (Remote Edge Access Point) consente a un LAP di risiedere su un collegamento WAN e di essere in grado di comunicare con il WLC e di fornire la funzionalità di un LAP normale. La modalità REAP è supportata solo sui LAP 1030.
- **Modalità H-REAP**: H-REAP è una soluzione wireless per installazioni in filiali e uffici remoti. H-REAP consente ai clienti di configurare e controllare i punti di accesso (AP) in una filiale o in un ufficio remoto dall'ufficio aziendale tramite un collegamento WAN senza la necessità di installare un controller in ogni ufficio. Gli H-REAP possono commutare il traffico di dati client localmente ed eseguire l'autenticazione client localmente quando la connessione al controller viene persa. Quando collegati al controller, gli H-REAP possono anche eseguire il tunnel del traffico verso il controller.
- **Modalità di monitoraggio**: la modalità di monitoraggio è una funzionalità progettata per consentire ai punti di accesso abilitati per LWAPP di escludersi dalla gestione del traffico di dati tra i client e l'infrastruttura. Agiscono invece come sensori dedicati per i servizi basati sulla posizione (LBS), il rilevamento di punti di accesso non autorizzati e il rilevamento delle intrusioni (IDS). Quando i punti di accesso sono in modalità di monitoraggio, non possono servire i client e scorrono continuamente tutti i canali configurati in ascolto di ogni canale per circa 60 ms.**Nota:** dalla versione 5.0 del controller, i LWAPP possono anche essere configurati in modalità LOMM (Location Optimized Monitor Mode), che ottimizza il monitoraggio e il calcolo della posizione delle etichette RFID. Per ulteriori informazioni su questa modalità, consultare il software Cisco Unified Wireless Network versione 5.0.**Nota:** con la release 5.2 del controller, la sezione **LOMM (Location Optimized Monitor Mode)** è stata rinominata **Ottimizzazione rilevamento**, mentre la casella a discesa **LOMM abilitato** è stata rinominata **Abilita ottimizzazione rilevamento**.**Nota:** per ulteriori informazioni su come configurare l'ottimizzazione del rilevamento, consultare la sezione Ottimizzazione del rilevamento RFID sugli access point.
- **Modalità Rogue Detector**: i LAP che operano in modalità Rogue Detector controllano i punti di accesso non autorizzati. Non trasmettono né contengono punti di accesso non autorizzati. L'idea è che il rilevatore della rogue debba essere in grado di vedere tutte le VLAN nella rete, in quanto i punti di accesso non autorizzati possono essere collegati a una qualsiasi VLAN nella rete (per questo motivo, la colleghiamo a una porta trunk). Lo switch invia tutti gli elenchi di indirizzi MAC AP/client non autorizzati al rilevatore di errori (RD). Il RD inoltra quindi tali dati al WLC in modo da confrontarli con i MAC dei client ascoltati dagli AP WLC via etere. Se i MAC corrispondono, il WLC sa che il punto di accesso non autorizzato a cui sono connessi i client si trova sulla rete cablata.

- **Modalità sniffer**: una LWAPP che funziona in modalità Sniffer funziona come sniffer e cattura e inoltra tutti i pacchetti su un particolare canale a un computer remoto che esegue Airopeek. Questi pacchetti contengono informazioni su timestamp, potenza del segnale, dimensioni e così via. La funzione Sniffer può essere attivata solo se si esegue Airopeek, un software di analisi della rete di terze parti che supporta la decodifica dei pacchetti di dati.
- **Modalità Bridge**: la modalità Bridge viene utilizzata quando i punti di accesso vengono impostati in un ambiente mesh e utilizzati per creare un bridge tra di loro.

D. Come modificare la modalità di un Lightweight Access Point?

R. Per modificare la modalità di un Lightweight Access Point, attenersi alla seguente procedura.

1. Dalla GUI del WLC, selezionare **Wireless > Access Point > Tutti gli AP**, quindi selezionare l'AP per cui modificare la modalità dall'elenco degli AP registrati.
2. Viene visualizzata la pagina **Tutti gli access point > Dettagli per access point**. Nella scheda **General** (Generale) di questa pagina, selezionare **AP Mode** (Modalità AP) dal menu a discesa, come
mostrato:



D. Ho appena installato i punti di accesso LAP-1131AG che sono stati avviati a un particolare controller. La versione del controller è 4.0.155.5. Quando vengono avviati con lo stesso Wireless LAN Controller (WLC) su cui sono avviati, alla fine

diventano verdi. Come indicato nella documentazione, questo LED di stato verde indica che i dispositivi sono collegati al WLC. Ma non sono riuscito a trovare questo access point nell'elenco degli access point del WLC. Perché? Il protocollo LWAPP (Lightweight Access Point Protocol) è stato associato?

A. Se l'access point è innescato su un WLC al layer 3, ma non riesce a ottenere un indirizzo IP durante l'avvio, il LED di stato del WLC diventa verde e non passa alla sequenza di ricerca e riavvio finché non ottiene un indirizzo IP dal DHCP.

Pertanto, in tali scenari, il LED di stato verde non indica che LWAPP è registrato con il controller. Dopo aver ottenuto gli indirizzi DHCP, i punti di accesso cercano il WLC e, se non vengono trovati, avviano un processo di riavvio e procedono come previsto. È presente un bug associato a questo.

per ulteriori informazioni, fare riferimento all'ID bug Cisco CSCsf10580 (solo utenti registrati).

D. Cosa indicano i LED sui LAP?

R. Questo è il collegamento a un breve video che spiega come interpretare i LED su un Lightweight Access Point 1130AG:

Interpretazione dei LED LAP - LAP1130

D. Qual è la differenza tra i punti di accesso dal tetto (RAP) e i punti di accesso Pole-Top (PAP) come modalità dei punti di accesso Mesh leggeri (MAP)?

R. Queste sono le modalità che le MAPPE esterne possono usare come parte della rete mesh. La soluzione di rete mesh, che fa parte di Cisco Unified Wireless Network Solution, consente a due o più Cisco Aironet Lightweight MAP di comunicare tra loro su uno o più hop wireless per connettersi a più LAN o estendere la copertura wireless 802.11b.

Questi punti di accesso sono usati come parte della rete mesh e operano in due modalità:

1. RAP
2. PAP

RAP - Le MAPPE Cisco che funzionano in modalità RAP sono il nodo padre di qualsiasi rete con bridging o mesh e connettono un bridge o una rete mesh alla rete cablata. Pertanto, può esistere un solo criterio di autorizzazione delle risorse per ogni segmento di rete con bridge o mesh. In una rete mesh, le mappe Cisco vengono configurate, monitorate e gestite da e tramite qualsiasi controller WLAN (WLC) Cisco implementato. Qualsiasi MAP con connessione cablata al WLC assume il ruolo di RAP. Questo sistema RAP utilizza l'interfaccia wireless backhaul per comunicare con i PAP adiacenti.

PAP: le mappe Cisco che funzionano in modalità PAP non hanno una connessione cablata a un WLC Cisco. Possono essere completamente wireless e supportare client che comunicano con altri PAP o RAP, oppure possono essere utilizzati per connettersi a periferiche o reti cablate. La porta Ethernet è disabilitata per impostazione predefinita per motivi di sicurezza, ma è necessario abilitarla per i PAP.

Per ulteriori informazioni su come una mappa assume il ruolo di RAP e PAP, consultare la sezione Zero Touch Configuration della Guida all'implementazione di una soluzione di rete Mesh Cisco.

D. Come interpreta il modello di radiazione delle antenne Lightweight Access Point (LAP) serie 1000?

A. I diagrammi di Azimuth sono generalmente con il dispositivo/antenna in normale orientamento operativo (verticale, in alto, al centro del diagramma per omni; orizzontale, al centro, in avanti (verso "0" nel diagramma). Il lato A è molto probabilmente in avanti e rappresentato al punto 0 per l'azimuth, e al punto 90 per l'elevazione. Il lato B è rappresentato al punto 180 per l'azimuth e al punto 270 per l'elevazione. Se l'unità è invertita, lo schema non cambia nello spazio libero. Ma le superfici immediate possono causare riflessione/assorbimento e possono alterare il pattern. Anche gli oggetti metallici vicino ai radiatori (entro circa 2 lunghezze d'onda) possono distorcere significativamente il pattern. Per ulteriori informazioni, consultare la Cisco Aironet Antenna Reference Guide. Le antenne della serie 1000 sono spiegate nell'ultima sezione del documento.

D. È possibile limitare i punti di accesso che si uniscono a un controller? Viene visualizzata la pagina SECURITY/AAA/AP Policies (Policy di sicurezza/AAA/AP), in cui è possibile autorizzare gli access point sulla base del certificato o dell'AAA. È possibile aggiungere un access point all'elenco delle autorizzazioni, ma queste operazioni limitano solo l'elenco degli access point autorizzati a unirsi al controller?

R. No, i controller gestiscono gli access point in base al principio "primo arrivato, primo server". È possibile utilizzare i campi primario, secondario e terziario per aumentare le probabilità sulle connessioni AP in base alle proprie preferenze.

D. Con LWAPP, è possibile determinare gli SSID di un access point su base individuale? Quali sono i requisiti per disporre di punti di accesso specifici in una zona che utilizza un SSID univoco e tutti gli altri che utilizzano un altro set di SSID?

R. Con l'opzione di sostituzione WLAN, è possibile scegliere gli SSID offerti da un access point. I controller supportano solo fino a 16 SSID ciascuno, pertanto è possibile scegliere solo tra i 16 supportati. Questa operazione viene eseguita per singolo access point.

D. Quando si abilitano alcuni comandi LWAPP sul LAP, viene visualizzato un messaggio di errore che indica che il comando è disabilitato. Perché?

```
AccessPoint#clear lwapp ap controller ip address
ERROR!!! Command is disabled.
```

R. Dopo che l'access point è stato aggiunto correttamente a un controller, i comandi LWAPP sono disabilitati. Per abilitare di nuovo i comandi LWAPP, impostare il nome utente e la password dell'access point dalla CLI del controller con il comando **config ap nome utente <nome> password <pwd> <cisco-ap>/all**. Al termine, è possibile eseguire una **clear lwapp private-config** nella CLI dell'access point per eseguire nuovamente manualmente i comandi di configurazione di AP LWAPP.

Nota: se si esegue WLC versione 5.0 e successive, utilizzare questo comando per impostare il nome utente e la password sull'access point:

config ap mgmtuser add username *AP_username* **password** *AP_password* **secret** *secret* **{all | Cisco_AP}**

D. Quando due access point si trovano sullo stesso canale e possono vedersi, quali sono le implicazioni (per il roaming, ecc.) dell'uso di quattro canali invece di tre? Come reagiscono gli access point in una situazione del genere e come reagisce un cliente?

R. Indipendentemente dal fatto che i punti di accesso si trovino o meno sullo stesso canale, l'impatto del roaming client non è particolarmente rilevante. Ciò che conta è una sufficiente sovrapposizione delle celle in modo che i client possano effettuare transizioni graduali dall'area di copertura di un punto di accesso al successivo. Lo scopo di un passaggio da un design a tre canali a un design a quattro canali è quello di aumentare la flessibilità del design (a causa del canale "extra"). Si tratta di un approccio miope in quanto, pur aggiungendo un po' di flessibilità di distribuzione (dal momento che si dispone di un altro canale), in realtà si aumenta la quantità di interferenze del co-canale. Ciò che si potrebbe ottenere in termini di flessibilità di progettazione con l'approccio a quattro canali, si perde nell'interferenza aggiunta al co-canale. Conclusione: non utilizzare un modello a quattro canali.

D. Possiamo controllare quando i clienti vagano? È possibile consentire al client di eseguire il roaming unicamente in base alla potenza del segnale su un singolo punto di accesso e per tutte le schede di rete client?

R. Oggi, il roaming è sempre una funzione del cliente, e la scelta di effettuare o meno il roaming è implementata in modo diverso nei vari client. Il roaming diretto fa parte di CCX, ma è una funzione opzionale e attualmente non viene utilizzata.

D. Sono previsti requisiti o consigli specifici per un collegamento WAN implementato tra REAP/HREAP AP sul sito remoto e WLC sul sito principale?

R. Questi sono alcuni dei principali fattori da prendere in considerazione per il collegamento WAN:

- Verificare che la larghezza di banda del collegamento WAN sia almeno 128 kbps.
- Verificare che la latenza o il ritardo di andata e ritorno tra i due siti sul collegamento WAN non sia superiore a 300 ms perché un ritardo superiore a 300 ms può creare problemi di autenticazione per il client, soprattutto quando viene implementata l'autenticazione centrale.

D. La rete è rimasta chiusa per alcune ore, a causa delle quali i LAP hanno perso la comunicazione con i WLC. Dopo il riavvio della rete, i LAP hanno prelevato l'indirizzo IP dal server DHCP, anche se questi AP sono configurati con un indirizzo IP statico. In "**show ap config general <ap-name>**" viene visualizzato come "**Fallback IP Address**". Perché questo accade?

R. Il LAP cerca di associare il WLC fino a 20 volte con i messaggi di rilevamento LWAPP. Nel caso in cui non sia in grado di connettersi, cerca di ottenere un nuovo indirizzo IP tramite DHCP. Se il LAP è in grado di ottenere un indirizzo IP dal server DHCP, questo è l'indirizzo IP attivo e l'indirizzo IP assegnato staticamente viene utilizzato per il fallback. Se i LAP vengono spostati su una VLAN diversa (ad esempio, su un altro edificio), possono recuperare un indirizzo IP e unirsi al WLC. Questo comportamento è spiegato nel bug CSCse6714. È necessario aggiornare il WLC alla versione software 4.0.206.0.

D. È obbligatorio configurare il nome di un gruppo di bridge per una rete mesh?

A. È possibile utilizzare il nome di un gruppo di bridge (BGN) per raggruppare logicamente gli access point nella rete. Sebbene per impostazione predefinita gli access point siano dotati di un valore BGN nullo per consentire l'associazione, si consiglia di impostare un valore BGN. È possibile apportare questa modifica alla configurazione dalla CLI o dalla GUI con questo comando:

```
config ap bridgegroupname set Bridge Group Name Cisco AP
```

Nota: I BGN possono contenere un massimo di dieci caratteri. Se si immettono più di 10 caratteri nel campo BGN della pagina di configurazione del punto di accesso mesh dell'interfaccia utente del controller, viene generato un messaggio di errore. Viene visualizzato un errore anche quando si configura questo parametro tramite il comando **config ap bridgegroupname set groupname Cisco_MAP** CLI o WCS (CSCsk64812).

Quando si configura BGN su una rete attiva, accertarsi di eseguire la configurazione dalla MAP più lontana e di tornare al RAP. Questa operazione è molto importante perché è possibile estrarre una mappa figlio che non può essere associata a un elemento padre, che può avere un BGN aggiornato. Utilizzare BGN diversi per raggruppare logicamente parti diverse della rete. Ciò è utile nelle situazioni in cui si dispone di RAP all'interno della stessa area RF e si desidera mantenere separati i segmenti della rete.

Per aggiungere un nuovo access point a una rete attiva, è necessario preconfigurare il BGN sul nuovo access point. Se si richiama la rete mesh da zero con i nuovi access point predefiniti, il valore BGN negli access point è impostato su NULL. Gli access point si uniscono in una nuova rete con questo valore predefinito del BGN. È possibile verificare il valore BGN di un access point con questo comando:

```
show ap config general Cisco AP
```

D. Cosa succede se il BGN non è configurato correttamente?

A. Se all'access point è stato assegnato erroneamente un nome di gruppo di bridge diverso da quello a cui è destinato, a seconda della progettazione della rete, l'access point può o non può essere in grado di raggiungere e trovare il settore o l'albero corretto. Se non riesce a raggiungere un settore compatibile, può diventare isolato. Per ripristinare un punto di accesso bloccato, è stato introdotto il concetto di nome del gruppo di bridge predefinito. L'idea di base è che un access point, che non è in grado di connettersi a nessun altro access point con il relativo bridgegroupname configurato, tenti di connettersi con il bridgegroupname predefinito.

Questo è l'algoritmo usato per rilevare la condizione del trefolo e il recupero:

1. Esegue una scansione passiva e trova tutti i nodi adiacenti, indipendentemente dal relativo nome del gruppo di bridge.
2. L'access point tenta di connettersi ai router adiacenti che vengono ascoltati con il proprio nome di gruppo di bridge tramite il protocollo AWPP (Adaptive Wireless Path Protocol).
3. Se il passaggio 2 ha esito negativo, provare a connettersi con il nome del gruppo di bridge predefinito con AWPP.
4. Per ogni tentativo non riuscito di eseguire il passaggio 3, elencare il router adiacente e tentare di connettersi al router adiacente migliore.

5. Se nel passaggio 4 l'access point non riesce a connettersi a tutti i router adiacenti, riavviarlo.
6. Se la connessione è stata stabilita con il nome del gruppo di bridge predefinito per 30 minuti, ripetere la scansione di tutti i canali e tentare di connettersi con il nome del gruppo di bridge corretto.

Nota: quando un access point è in grado di connettersi con il nome del gruppo di bridge predefinito, il nodo padre indica l'access point come voce figlio/nodo/router adiacente predefinita sul controller WLAN, in modo che un amministratore di rete sia a conoscenza dell'access point bloccato. Tale access point non può accettare alcun client o altri nodi mesh come suoi figli, né può attraversare alcun traffico di dati.

D. È possibile collegare un LAP 1030 a qualsiasi altro modello di bridge? È possibile utilizzare un LAP 1020 anche per il bridging?

R. Il modello LAP 1020 non supporta il bridging. Attualmente, il LAP 1030 supporta il bridging (un hop) di un altro LAP 1030, ma non di un BR1310, BR1400 o LAP 1500.

D. È possibile configurare il bridging wireless tra i LAP AP? Desidero che una radio sui LAP non cablati esegua il bridging ai LAP (LAP collegati a un WLC) di root bridge cablata. È possibile?

R. No. Non è possibile usare i LAP AP. I Mesh AP possono eseguire il bridging point-to-point di base in una rete wireless unificata Cisco. L'unico altro tipo di bridging possibile è tramite gli access point IOS in modalità WGB (Workgroup Bridge). Questi access point IOS funzionano come client (con i dispositivi cablati dietro di essi) per un access point LAP. Tuttavia, i client wireless non possono connettersi a questi access point IOS.

D. Si dispone di un LAP 1131 e questo punto di accesso è stato registrato correttamente sui Wireless LAN Controller. Quando si collega il punto di accesso senza l'iniettore di alimentazione, le radio sono accese (lo stato del LED è verde), ma quando si collega l'access point con l'iniettore di alimentazione, le radio sono spente (lo stato del LED è arancione). Come risolvere il problema?

R. Questo problema può essere dovuto a parametri Power over Ethernet (POE) configurati in modo errato; per risolvere il problema, completare i seguenti passaggi:

1. Per accedere a questi parametri, fare clic su **Wireless**.
2. Fare clic sul collegamento **Detail** (Dettagli) del punto di accesso desiderato. I nuovi parametri vengono visualizzati nella pagina Tutti gli access point > Dettagli sotto le impostazioni POE.
3. Nella pagina AP > Dettagli del punto di accesso per le impostazioni POE, fare clic su **Power Injector State**, quindi selezionare **Installato**.
4. Selezionare la casella di controllo per attivare lo stato dell'iniettore di alimentazione per il punto di accesso. Questo parametro è obbligatorio se lo switch collegato non supporta IPM e viene utilizzato un alimentatore. Questo parametro non è necessario se lo switch collegato supporta IPM.

D. Nei punti di accesso autonomi, PSPF (Public Secure Packet Forwarding) viene utilizzato per evitare che i dispositivi client associati a questo punto di accesso condividano inavvertitamente file con altri dispositivi client della rete wireless. I

Lightweight Access Point offrono funzionalità equivalenti?

R. La funzionalità o la modalità che esegue la funzione simile di PSPF in un'architettura lightweight è denominata modalità di blocco peer-to-peer. La modalità di blocco peer-to-peer è effettivamente disponibile con i controller che gestiscono il LAP.

Se questa modalità è disattivata sul controller (impostazione predefinita), consente ai client wireless di comunicare tra loro tramite il controller. Se la modalità è attivata, la comunicazione tra i client tramite il controller viene bloccata.

Funziona solo tra gli access point che sono stati collegati allo stesso controller. Se attivata, questa modalità non impedisce ai client wireless terminati su un controller di raggiungere i client wireless terminati su un controller diverso, anche nello stesso gruppo di mobilità.

D. Un LAP AP può gestire i messaggi SNMP come un IOS AP?

R. I LAP AP non possono gestire i messaggi SNMP da soli. Per gestire i messaggi SNMP, è necessario configurare una community SNMP sul WLC in cui è registrato il LAP. Tutte le informazioni dell'access point sono gestite dal WLC.

Informazioni correlate

- Domande frequenti (FAQ) sul controller WLC
- Moduli Cisco Wireless LAN Controller
- Domande frequenti (FAQ) su Cisco Wireless LAN Controller (WLC)
- Guida alla configurazione di Cisco Wireless LAN Controller, versione 3.2
- Esempio di configurazione base di Wireless LAN Controller e Lightweight Access Point
- Documentazione e supporto tecnico – Cisco Systems