Domande frequenti sul design e le caratteristiche del controller WLC (Wireless LAN Controller)

Sommario

Introduzione

Questo documento offre informazioni sulle domande più frequenti (FAQ) relative al progetto e alle funzionalità disponibili con un controller WLC.

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

Domande frequenti sulla progettazione

D. Come configurare lo switch per il collegamento al WLC?

A. Configurare la porta dello switch a cui è collegato il WLC, come porta trunk IEEE 802.1Q. Verificare che sullo switch siano consentite solo le VLAN necessarie. Di solito, la gestione e l'interfaccia AP-Manager del WLC non hanno tag. Ciò significa che essi assumono la VLAN nativa dello switch connesso. Questo non è necessario. È possibile assegnare una VLAN separata a queste interfacce. Per ulteriori informazioni, fare riferimento alla sezione *Configurazione dello switch per il WLC* degli esempi di configurazione base di Wireless LAN Controller e Lightweight Access Point.

D. Tutto il traffico di rete da e verso un tunnel client WLAN tramite un controller WLC (Wireless LAN Controller) viene registrato dal controller nel punto di accesso?

A. Quando l'access point si unisce a un WLC, tra i due dispositivi viene formato un tunnel Control and Provisioning of Wireless Access Point Protocol (CAPWAP). Tutto il traffico, incluso tutto il traffico client, viene inviato tramite il tunnel CAPWAP.

L'unica eccezione è quando un access point è in modalità ibrida-REAP. I punti di accesso ibrido-REAP possono commutare il traffico di dati client localmente ed eseguire l'autenticazione client localmente quando la connessione al controller viene persa. Una volta connessi al controller, possono anche inviare il traffico al controller.

D. Posso installare dei Lightweight Access Point (LAP) in una sede remota e un

Cisco Wireless LAN Controller (WLC) nella mia sede centrale? Il protocollo LWAPP/CAPWAP funziona su una WAN?

R. Sì, è possibile avere i WLC sulla WAN dagli access point. LWAPP/CAPWAP funziona su una WAN quando i LAP sono configurati in modalità Remote Edge AP (REAP) o Hybrid Remote Edge AP (H-REAP). Entrambe queste modalità consentono il controllo di un access point da parte di un controller remoto connesso tramite un collegamento WAN. Il traffico viene collegato localmente al collegamento LAN, evitando di inviare inutilmente il traffico locale sul collegamento WAN. Questo è esattamente uno dei maggiori vantaggi di avere WLC nella vostra rete wireless.

Nota: non tutti i Lightweight Access Point supportano queste modalità. Ad esempio, la modalità H-REAP è supportata solo sui LAP 1131, 1140, 1242, 1250 e AP801. La modalità REAP è supportata solo nell'access point serie 1030, mentre i access point serie 1010 e 1020 non supportano la modalità REAP. Prima di pianificare l'implementazione di queste modalità, verificare che i LAP la supportino. I Cisco IOS® Software AP (Autonomous AP) convertiti in LWAPP non supportano il protocollo REAP.

D. Come funzionano le modalità REAP e H-REAP?

A. In modalità **REAP**, tutto il traffico di controllo e di gestione, incluso il traffico di autenticazione, viene rimandato indietro al WLC. Tutto il traffico di dati viene però commutato localmente all'interno della LAN dell'ufficio remoto. Quando si perde la connessione al WLC, tutte le WLAN vengono terminate ad eccezione della prima WLAN (WLAN1). Tutti i client attualmente associati a questa WLAN vengono mantenuti. Per consentire ai nuovi client di autenticarsi e ricevere il servizio su questa WLAN entro il tempo di inattività, configurare il metodo di autenticazione per questa WLAN come WEP o WPA-PSK in modo che l'autenticazione venga eseguita localmente sul REAP. Per ulteriori informazioni sulla distribuzione di REAP, consultare la guida alla distribuzione di REAP nella succursale.

In modalità **H-REAP**, un punto di accesso crea un tunnel per il traffico di controllo e di gestione, compreso il traffico di autenticazione, fino al WLC. Il traffico di dati proveniente da una WLAN viene gestito localmente nell'ufficio remoto se la WLAN è configurata con la commutazione locale H-REAP o se il traffico di dati viene rinviato al WLC. Quando si perde la connessione al WLC, tutte le WLAN vengono terminate, ad eccezione delle prime otto WLAN configurate con la commutazione locale H-REAP. Tutti i client attualmente associati a queste WLAN vengono conservati. Per consentire ai nuovi client di autenticarsi e ricevere i servizi su queste WLAN entro il tempo di inattività, configurare il metodo di autenticazione per questa WLAN come WEP, WPA PSK o WPA2 PSK in modo che l'autenticazione venga eseguita localmente in H-REAP.

Per ulteriori informazioni su H-REAP, consultare la Guida alla progettazione e alla distribuzione di H-REAP.

D. Qual è la differenza tra Remote-Edge AP (REAP) e Hybrid-REAP (H-REAP)?

R. REAP non supporta il tagging VLAN IEEE 802.1Q. Di conseguenza, non supporta più VLAN. Il traffico proveniente da tutti gli SSID (Service Set Identifier) termina sulla stessa subnet, ma H-REAP supporta il tagging VLAN IEEE 802.1Q. Il traffico proveniente da ciascun SSID può essere segmentato su una VLAN univoca.

Quando la connettività al WLC viene persa, ossia in modalità standalone, il REAP serve una sola WLAN, ossia la prima WLAN. Tutte le altre WLAN sono disattivate. In H-REAP, sono supportate

fino a 8 WLAN in tempi di inattività.

Un'altra importante differenza è che, in modalità REAP, il traffico di dati può essere bloccato solo localmente. Non può essere riportato all'ufficio centrale, ma in modalità H-REAP è possibile ritrasferire il traffico all'ufficio centrale. Il traffico proveniente dalle WLAN configurate con la commutazione locale H-REAP viene commutato localmente. Il traffico di dati da altre WLAN viene rimandato all'ufficio centrale.

Per ulteriori informazioni sul protocollo REAP, fare riferimento agli esempi di configurazione dei Remote-Edge AP (REAP) con Lightweight AP e Wireless LAN Controller (WLC).

Per ulteriori informazioni su H-REAP, fare riferimento a Configurazione del punto di accesso ibrido.

D. Quante WLAN sono supportate sul WLC?

R. A partire dalla versione software 5.2.157.0, il WLC può ora controllare fino a 512 WLAN per punti di accesso lightweight. A ciascuna WLAN sono associati un ID WLAN (da 1 a 512), un nome di profilo e un SSID WLAN distinti. A ogni WLAN possono essere assegnati criteri di sicurezza univoci. Il controller può pubblicare fino a 16 WLAN su ciascun punto di accesso connesso, ma è possibile creare fino a 512 WLAN sul controller e quindi pubblicare selettivamente queste WLAN (utilizzando i gruppi di punti di accesso) su punti di accesso diversi per gestire meglio la rete wireless.

Nota: i controller Cisco 2106, 2112 e 2125 supportano solo fino a 16 WLAN.

Nota: per informazioni dettagliate sulle linee guida per la configurazione delle WLAN sui WLC, consultare la sezione Creazione di WLAN nella guida alla configurazione di Cisco Wireless LAN Controller, versione 7.0.116.0.

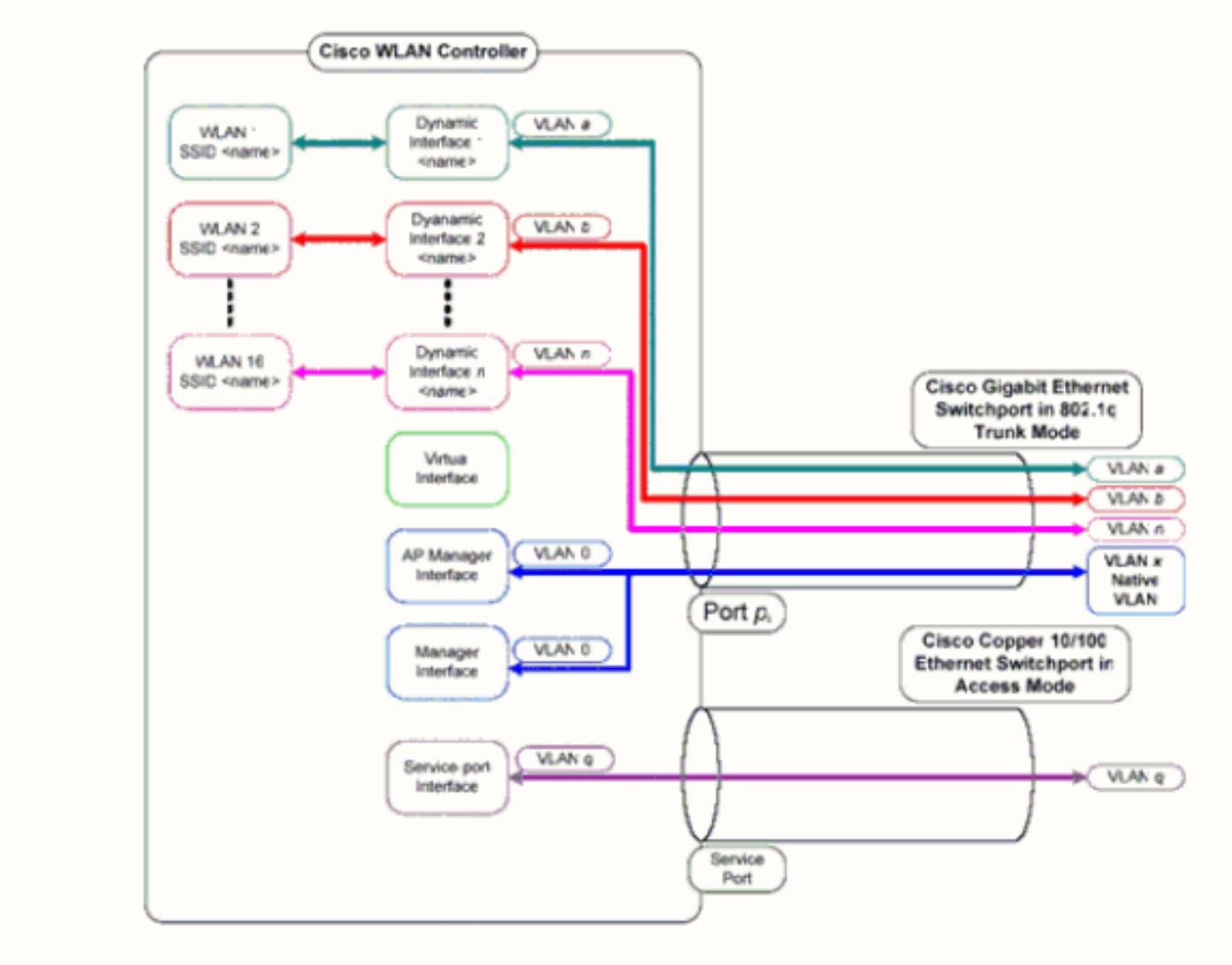
D. Come configurare le VLAN sul controller WLC?

R. Nel WLC, le VLAN sono legate a un'interfaccia configurata in una subnet IP univoca. L'interfaccia è mappata su una WLAN. Quindi, i client associati a questa WLAN appartengono alla VLAN dell'interfaccia e ricevono un indirizzo IP dalla subnet a cui appartiene l'interfaccia. Per configurare le VLAN sul WLC, completare la procedura descritta nell'esempio di configurazione delle VLAN sui controller LAN wireless.

D. Abbiamo effettuato il provisioning di due WLAN con due diverse interfacce dinamiche. Ogni interfaccia ha la propria VLAN, che è diversa dalla VLAN dell'interfaccia di gestione. Sembra che questa procedura funzioni, ma non è stato eseguito il provisioning delle porte trunk per consentire le VLAN usate dalle WLAN. Il punto di accesso (AP) assegna un tag ai pacchetti con l'interfaccia di gestione VLAN?

R. L'access point non assegna tag ai pacchetti con l'interfaccia di gestione VLAN. L'access point incapsula i pacchetti dai client nel protocollo LWAPP/CAPWAP (Lightweight AP Protocol) e quindi passa i pacchetti al WLC. Il WLC quindi rimuove l'intestazione LWAPP/CAPWAP e inoltra i pacchetti al gateway con il tag VLAN appropriato. Il tag VLAN dipende dalla WLAN a cui appartiene il client. Il WLC dipende dal gateway per indirizzare i pacchetti alla destinazione. Per poter trasmettere il traffico di più VLAN, è necessario configurare lo switch uplink come porta

trunk. Questo diagramma spiega come funzionano le VLAN con i controller:



D. Quale indirizzo IP del WLC viene utilizzato per l'autenticazione con il server AAA?

R. Il WLC utilizza l'indirizzo IP dell'interfaccia di gestione per qualsiasi meccanismo di autenticazione (layer 2 o layer 3) che coinvolge un server AAA. Per ulteriori informazioni sulle porte e le interfacce sul WLC, fare riferimento alla sezione *Configurazione delle porte e delle interfacce* della guida alla configurazione di Cisco Wireless LAN Controller, versione 7.0.116.0.

D. Ho dieci Cisco serie 1000 Lightweight Access Point (LAP) e due Wireless LAN Controller (WLC) nella stessa VLAN. Come registrare sei LAP da associare al WLC1 e gli altri quattro LAP da associare al WLC2?

R. LWAPP/CAPWAP consente la ridondanza dinamica e il bilanciamento del carico. Ad esempio, se si specificano più indirizzi IP per l'opzione 43, un LAP invia richieste di rilevamento LWAPP/CAPWAP a ciascuno degli indirizzi IP ricevuti dall'access point. Nella risposta al rilevamento WLC LWAPP/CAPWAP, il WLC incorpora queste informazioni:

- informazioni sul carico LAP corrente, definito come il numero di LAP che sono stati uniti al WLC in quel momento
- La capacità dei LAP

- Numero di client wireless connessi al WLC

Il LAP tenta quindi di collegarsi al WLC meno caricato, ossia il WLC con la capacità LAP più elevata disponibile. Inoltre, dopo che un LAP si è unito a un WLC, il LAP apprende gli indirizzi IP degli altri WLC nel gruppo di mobilità dal suo WLC unito.

Una volta che un LAP si unisce a un WLC, è possibile fare in modo che il LAP si unisca a un WLC specifico entro il successivo riavvio. A tal fine, assegnare un WLC primario, secondario e terziario per un LAP. Quando il LAP si riavvia, cerca il WLC primario e lo unisce in modo indipendente dal carico che grava sul WLC. Se il WLC primario non risponde, cerca il secondario e, in assenza di risposta, il terziario. Per ulteriori informazioni su come configurare il WLC primario per un LAP, fare riferimento alla sezione *Assegnazione dei controller primari, secondari e terziari per il Lightweight AP* nell'esempio di configurazione del failover dei controller WLAN per Lightweight Access Point.

D. Quali funzionalità non sono supportate sui Wireless LAN Controller (WLC) serie 2100?

R. Queste funzionalità hardware non sono supportate sui controller serie 2100:

- Porta di servizio (interfaccia Ethernet 10/100 Mb/s di gestione fuori banda separata)

Queste funzionalità software non sono supportate sui controller serie 2100:

- Terminazione VPN (IPSec o L2TP)
- Terminazione dei tunnel del controller guest (è supportata la creazione di tunnel del controller guest)
- Elenco dei server Web per l'autenticazione Web esterna
- Protocollo LWAPP sul Layer 2
- Spanning Tree
- Mirroring delle porte
- Cranite
- Fortezza
- AppleTalk
- Contratti QoS della larghezza di banda per utente
- Passthrough IPv6
- Aggregazione dei collegamenti (LAG)
- Modalità Multicast unicast
- Accesso guest cablato

D. Quali funzionalità non sono supportate sui controller serie 5500?

R. Queste funzionalità software non sono supportate sui controller serie 5500:

- Interfaccia statica AP-manager**Nota:** sui controller serie 5500, non è necessario configurare un'interfaccia AP-manager. Per impostazione predefinita, l'interfaccia di gestione funge da interfaccia AP-manager e i punti di accesso possono unirsi a questa interfaccia.
- Tunneling a mobilità asimmetrica
- STP (Spanning Tree Protocol)
- Mirroring delle porte
- Supporto ACL (Access Control List) di livello 2

- Terminazione VPN (IPSec o L2TP)
- Opzione passthrough VPN
- Configurazione di bridging 802.3, AppleTalk e PPPoE (Point-to-Point Protocol over Ethernet)

D. Quali funzionalità non sono supportate sulle reti mesh?

R. Queste funzionalità dei controller non sono supportate sulle reti mesh:

- Supporto di più paesi
- CAC basato sul carico (le reti mesh supportano solo CAC statiche o basate sulla larghezza di banda)
- Alta disponibilità (heartbeat veloce e timer di join per il rilevamento primario)
- Autenticazione EAP-FASTv1 e 802.1X
- Priorità di join dei punti di accesso (i punti di accesso mesh hanno una priorità fissa).
- Certificato significativo localmente
- Servizi basati sulla posizione

D. Qual è il periodo di validità dei certificati del produttore installati (MIC) su un controller LAN wireless e dei certificati del punto di accesso leggero?

R. Il periodo di validità di un MIC su un WLC è di 10 anni. Lo stesso periodo di validità di 10 anni si applica ai certificati Lightweight AP dalla creazione (che si tratti di un certificato MIC o di un certificato autofirmato (SSC)).

D. Ho due controller WLC (Wireless LAN Controller) denominati WLC1 e WLC2 configurati all'interno dello stesso gruppo di mobilità per il failover. Il mio Lightweight Access Point (LAP) è attualmente registrato con WLC1. Se il WLC1 ha esito negativo, l'access point viene registrato sul WLC1 e viene riavviato durante la transizione verso il WLC (WLC2) sopravvissuto? Inoltre, durante il failover, il client WLAN perde la connettività WLAN con il LAP?

R. Sì, il LAP elimina la registrazione dal WLC1, si riavvia, quindi si registra nuovamente sul WLC2, se il WLC1 non riesce. Al riavvio del LAP, i client WLAN associati perdono la connettività. Per informazioni correlate, fare riferimento a Bilanciamento del carico e fallback dell'access point in reti wireless unificate.

D. Il roaming dipende dalla modalità Lightweight Access Point Protocol (LWAPP) configurata per l'utilizzo dal controller WLC? Un WLC che funziona in modalità LWAPP di layer 2 può eseguire il roaming di layer 3?

R. Finché il raggruppamento della mobilità nei controller è configurato correttamente, il roaming dei client dovrebbe funzionare correttamente. Il roaming non è influenzato dalla modalità LWAPP (livello 2 o livello 3). Tuttavia, si consiglia di utilizzare LWAPP di layer 3 quando possibile.

Nota: la modalità di layer 2 è supportata solo dai Cisco serie 410x e 440x di WLC e dai Cisco serie 1000 Access Point. LWAPP di layer 2 non è supportato dalle altre piattaforme Wireless LAN Controller e Lightweight Access Point.

D. Qual è il processo di roaming che si verifica quando un client decide di eseguire il roaming verso un nuovo punto di accesso (access point) o controller?

R. Questa è la sequenza di eventi che si verifica quando un client esegue il roaming a un nuovo access point:

1. Il client invia una richiesta di riassociazione al WLC tramite il LAP.
2. Il WLC invia il messaggio relativo alla mobilità ad altri WLC nel gruppo di mobilità per sapere a quale WLC il client è stato associato in precedenza.
3. Il WLC originale risponde con le informazioni, come l'indirizzo MAC, l'indirizzo IP, QoS, il contesto di sicurezza, ecc., relative al client tramite il messaggio di mobilità.
4. Il WLC aggiorna il proprio database con i dettagli client forniti; il client passa quindi attraverso il processo di riautenticazione, se necessario. Il nuovo LAP a cui il client è attualmente associato viene aggiornato insieme ad altri dettagli nel database del WLC. In questo modo, l'indirizzo IP del client viene mantenuto tra i roaming tra i WLC, consentendo un roaming senza problemi.

Per ulteriori informazioni sul roaming in un ambiente unificato, fare riferimento alla sezione *Configurazione dei gruppi di mobilità* della guida alla configurazione di Cisco Wireless LAN Controller, versione 7.0.116.0.

Nota: il client wireless non invia una richiesta di autenticazione (802.11) durante la riassociazione. Il client wireless invia immediatamente la riassociazione. Quindi, passerà attraverso l'autenticazione 802.1x.

D. Quali porte devo autorizzare per la comunicazione LWAPP/CAPWAP quando nella rete è presente un firewall?

R. È necessario abilitare le seguenti porte:

- Abilita queste porte UDP per il traffico LWAPP:Dati - 12222Controllo - 12223
- Abilitare queste porte UDP per il traffico CAPWAP:Dati - 5247Controllo - 5246
- Abilitare queste porte UDP per il traffico di mobilità:1666 - Modalità protetta16667 - Modalità non protetta

I messaggi relativi alla mobilità e ai dati vengono in genere scambiati tramite pacchetti EtherIP. **Il protocollo IP 97** deve essere autorizzato sul firewall per consentire i pacchetti EtherIP. Se si usa **ESP** per incapsulare i pacchetti per la mobilità, è necessario autorizzare **ISAKMP** attraverso il firewall quando si apre la **porta UDP 500**. Inoltre, è necessario aprire il **protocollo IP 50** per consentire il passaggio dei dati crittografati attraverso il firewall.

Queste porte sono opzionali (in base ai requisiti):

- TCP 161 e 162 per SNMP (per Wireless Control System [WCS])
- UDP 69 per TFTP
- TCP 80 e/o 443 per HTTP o HTTPS per l'accesso GUI
- TCP 23 e/o 22 per Telnet o SSH (Secure Shell) per l'accesso CLI

D. I controller LAN wireless supportano sia SSHv1 che SSHv2?

R. I Wireless LAN Controller supportano solo SSHv2.

D. Il protocollo RARP (Reverse ARP) è supportato sui controller WLC (Wireless LAN Controller)?

R. Il protocollo RARP (Reverse Address Resolution Protocol) è un protocollo del livello di collegamento utilizzato per ottenere un indirizzo IP per un determinato livello di collegamento, ad esempio un indirizzo Ethernet. Il protocollo RARP è supportato sui WLC con firmware versione 4.0.217.0 o successive. RARP non è supportato in nessuna delle versioni precedenti.

D. È possibile utilizzare il server DHCP interno sul controller WLC (Wireless LAN Controller) per assegnare gli indirizzi IP ai Lightweight Access Point (LAP)?

R. I controller contengono un server DHCP interno. Questo server viene in genere utilizzato nelle succursali che non dispongono già di un server DHCP. Per accedere al servizio DHCP, fare clic sul menu **Controller** nell'interfaccia utente del WLC, quindi selezionare l'opzione **Internal DHCP Server** (Server DHCP interno) sul lato sinistro della pagina. Per ulteriori informazioni su come configurare l'ambito DHCP sul WLC, fare riferimento alla sezione *Configurazione del DHCP* della guida alla configurazione di Cisco Wireless LAN Controller, versione 7.0.116.0.

Il server interno fornisce indirizzi DHCP ai client wireless, ai LAP, ai punti di accesso in modalità appliance sull'interfaccia di gestione e alle richieste DHCP inoltrate dai LAP. I WLC non offrono mai indirizzi ai dispositivi a monte nella rete cablata. L'opzione DHCP 43 non è supportata sul server interno, quindi l'access point deve utilizzare un metodo alternativo per individuare l'indirizzo IP dell'interfaccia di gestione del controller, ad esempio la trasmissione della subnet locale, il DNS, il priming o il rilevamento via etere.

Nota: le versioni del firmware dei WLC precedenti alla 4.0 non supportano il servizio DHCP per i LAP a meno che i LAP non siano collegati direttamente al WLC. La funzionalità server DHCP interno è stata utilizzata solo per fornire indirizzi IP ai client che si connettono alla rete LAN wireless.

D. Cosa significa il campo DHCP obbligatorio in una WLAN?

R. DHCP Required è un'opzione che può essere abilitata per una rete WLAN. Infatti, è necessario che tutti i client associati a quella particolare WLAN ottengano indirizzi IP tramite DHCP. I client con indirizzi IP statici non possono essere associati alla WLAN. Questa opzione è disponibile nella scheda Advanced (Avanzate) di una rete WLAN. Il WLC consente il traffico da/verso un client solo se il relativo indirizzo IP è presente nella tabella MSCB del WLC. WLC registra l'indirizzo IP di un client durante la richiesta DHCP o il rinnovo DHCP. A tal fine, è necessario che il client rinnovi il proprio indirizzo IP ogni volta che si associa nuovamente al WLC, in quanto ogni volta che il client si dissocia come parte del timeout del processo di roaming o della sessione, la relativa voce viene cancellata dalla tabella MSCB. Il client deve ripetere l'autenticazione e la riassociazione al WLC, che a sua volta crea la voce client nella tabella.

D. Come funziona la gestione centralizzata delle chiavi (CCKM) Cisco in un ambiente LWAPP/CAPWAP?

R. Durante l'associazione iniziale del client, il punto di accesso o il WLC negozia una chiave master (PMK) per coppia dopo che il client wireless ha superato l'autenticazione 802.1x. Il WLC o il WDS AP memorizza nella cache la chiave PMK per ciascun client. Quando un client wireless si riassocia o esegue il roaming, ignora l'autenticazione 802.1x e convalida immediatamente PMK.

L'unica implementazione speciale del WLC nella CCKM è che i WLC scambiano la PMK del client tramite pacchetti per la mobilità, come UDP 1666.

D. Come configurare le impostazioni duplex sul controller WLC (Wireless LAN Controller) e sui LAP (Lightweight Access Point)?

R. I prodotti Cisco Wireless funzionano meglio quando la velocità e il duplex sono negoziati automaticamente, ma è possibile impostare la modalità duplex sui WLC e sui LAP. Per impostare la velocità/duplex dell'access point, è possibile configurare le impostazioni duplex per i LAP sul controller e quindi, a turno, spostarle sui LAP.

configure ap ethernet duplex <auto/half/full> speed <auto/10/100/1000> <all/Cisco AP Name> è il comando per impostare le impostazioni duplex dalla CLI. Questo comando è supportato solo nella versione 4.1 e successive.

Per impostare le impostazioni duplex per le interfacce fisiche del WLC, usare il comando **config port physical mode {all | porta} {100h | 100 septies | 10 ore | 10f}**.

Questo comando imposta le porte Ethernet 10/100BASE-T del pannello anteriore specificate o tutte per il funzionamento dedicato a 10 Mbps o 100 Mbps, half-duplex o full-duplex. Notare che è necessario disabilitare la negoziazione automatica con il comando **config port auto-registrazione disable** prima di configurare manualmente qualsiasi modalità fisica sulla porta. Inoltre, il comando **config port auto** ignora le impostazioni configurate con il comando **config port physical mode**. Per impostazione predefinita, tutte le porte sono impostate sulla negoziazione automatica.

Nota: non è possibile modificare le impostazioni di velocità sulle porte in fibra.

D. È possibile tenere traccia del nome del Lightweight Access Point (LAP) quando non è registrato sul controller?

R. Se l'access point è completamente spento e non è registrato sul controller, non è possibile rilevare il LAP tramite il controller. L'unico modo per accedere allo switch su cui sono connessi gli access point è tramite questo comando:

```
show mac-address-table address
```

In questo modo viene visualizzato il numero della porta dello switch a cui è collegato l'access point. Quindi, usare questo comando:

```
show cdp nei detail
```

L'output di questo comando restituisce anche il nome LAP. Tuttavia, questo metodo è possibile solo quando il punto di accesso è acceso e collegato allo switch.

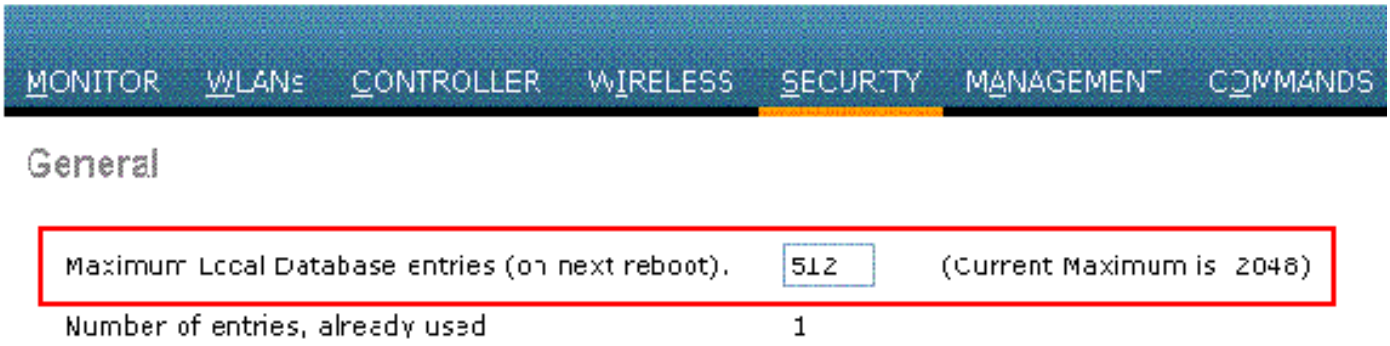
D. Sono stati configurati 512 utenti sul controller. Esiste un modo per aumentare il numero di utenti sul controller WLC?

R. Il database degli utenti locali è limitato a un massimo di 2048 voci nella pagina **Protezione >Generale**. Questo database è condiviso dagli utenti di gestione locale (che includono gli ambasciatori della sala di attesa), dagli utenti di rete (che includono gli utenti guest), dalle voci del filtro MAC, dalle voci dell'elenco di autorizzazioni dei punti di accesso e dalle voci dell'elenco di esclusione. Nel loro insieme, tutti questi tipi di utenti non possono superare le dimensioni del database configurato.

Per aumentare il numero del database locale, usare questo comando dalla CLI:

```
<Cisco Controller>config database size ?
<count>  Enter the maximum number of entries (512-2048)
```

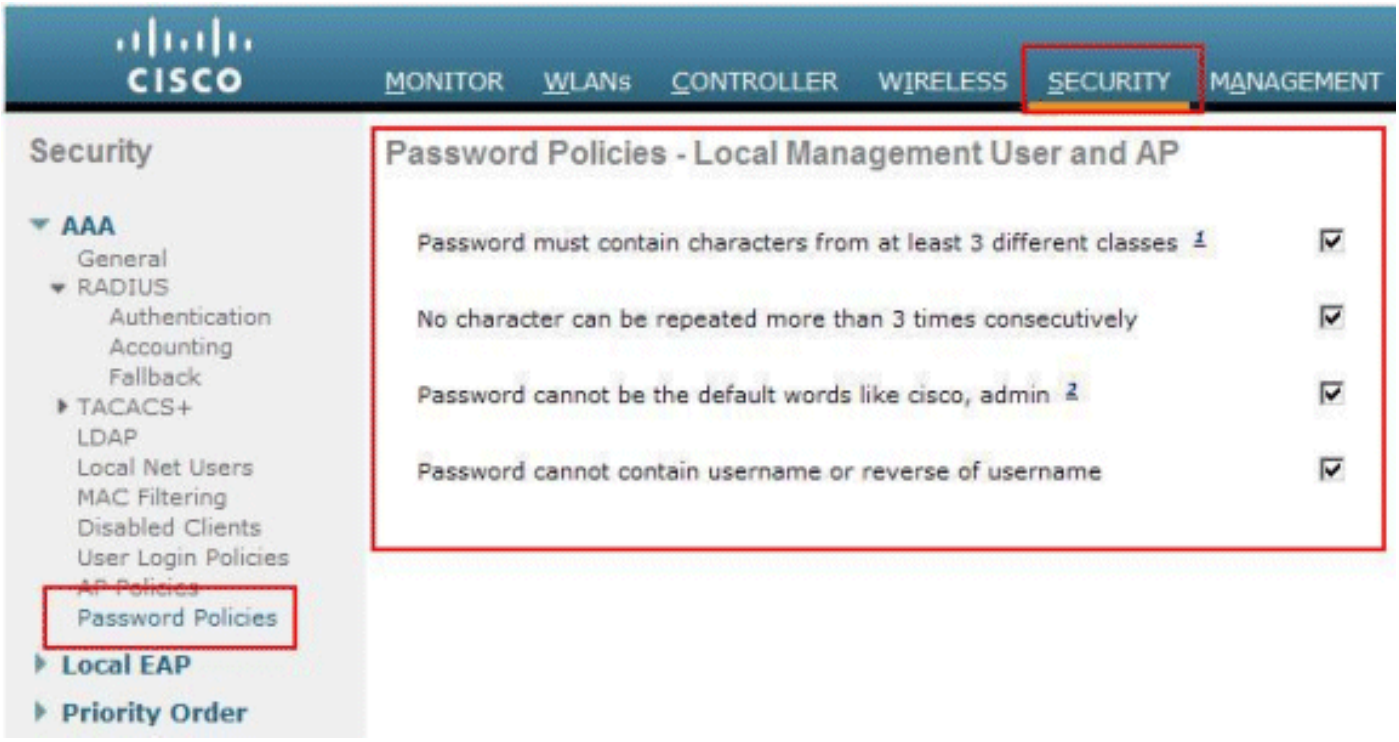
Nota: per rendere effettiva la modifica, è necessario salvare la configurazione e ripristinare il sistema (utilizzando il comando **reset system**).



D. Come posso applicare una policy per le password complesse sui WLC?

R. I WLC consentono di definire una policy per le password complesse. a tal fine, è possibile usare la CLI o la GUI.

Dalla GUI, selezionare **Security > AAA > Password Policies** (Policy di sicurezza > AAA). In questa pagina è possibile selezionare una serie di opzioni per applicare una password complessa. Di seguito è riportato un esempio:



A tale scopo, dalla CLI del WLC, usare il comando **config switchconfig strong-pwd** {case-check | *controllo consecutivo* | *controllo di default* | *username-check* | *all-check}* {*abilitazione* | *disable}* comando:

- **case-check**: controlla l'occorrenza dello stesso carattere tre volte consecutivamente.
- **continuous-check** - Controlla se vengono utilizzati i valori di default o le relative varianti.
- **default-check** - Controlla se è in uso il nome utente o il suo nome inverso.
- **all-checks**: abilita/disabilita tutti i controlli della password complessa.

D. Come viene utilizzata la funzione client passivo sui controller LAN wireless?

R. I client passivi sono dispositivi wireless, quali scale e stampanti, configurati con un indirizzo IP statico. Questi client non trasmettono alcuna informazione IP, ad esempio l'indirizzo IP, la subnet mask e le informazioni sul gateway, quando vengono associati a un punto di accesso. Di conseguenza, quando si utilizzano client passivi, il controller non conosce mai l'indirizzo IP a meno che non utilizzi DHCP.

I WLC funzionano attualmente come proxy per le richieste ARP. Quando riceve una richiesta ARP, il controller risponde con una risposta ARP anziché passare la richiesta direttamente al client. Questo scenario presenta due vantaggi:

- Il dispositivo upstream che invia la richiesta ARP al client non saprà dove si trova il client.
- L'alimentazione per i dispositivi a batteria, come telefoni cellulari e stampanti, viene mantenuta in quanto non devono rispondere a ogni richiesta ARP.

Poiché il controller wireless non dispone di informazioni relative all'indirizzo IP sui client passivi, non può rispondere ad alcuna richiesta ARP. Il comportamento corrente non consente il trasferimento di richieste ARP a client passivi. Qualsiasi applicazione che tenti di accedere a un client passivo avrà esito negativo.

La funzionalità client passivo consente lo scambio di richieste e risposte ARP tra client cablati e

wireless. Questa funzionalità, se attivata, consente al controller di passare le richieste ARP dai client cablati a quelli wireless fino a quando il client wireless desiderato non raggiunge lo stato RUN.

Per informazioni su come configurare la funzione client passivo, consultare la sezione relativa all'uso della GUI per configurare il client passivo nella guida alla configurazione di Cisco Wireless LAN Controller, versione 7.0.116.0.

D. Come è possibile configurare il client per la riautenticazione con il server RADIUS ogni tre minuti o in un periodo di tempo specificato?

A. A tal fine, è possibile usare il parametro del timeout di sessione sul WLC. Per impostazione predefinita, il parametro di timeout della sessione è configurato per 1800 secondi prima che si verifichi una riautenticazione.

Modificare questo valore in 180 secondi per consentire al client di eseguire nuovamente l'autenticazione dopo tre minuti.

Per accedere al parametro del timeout della sessione, fare clic sul menu **WLAN** nell'interfaccia utente. Visualizza l'elenco delle WLAN configurate nel WLC. Fare clic sulla WLAN a cui appartiene il client. Andare alla scheda **Advanced** e trovare il parametro *Enable Session Timeout*. Impostate il valore di default a 180 e fate clic su **Applica (Apply)** per rendere effettive le modifiche.

Quando viene inviato in Access-Accept, insieme al valore Termination-Action di RADIUS-Request, l'attributo Session-Timeout specifica il numero massimo di secondi di servizio forniti prima della riautenticazione. In questo caso, l'attributo Session-Timeout viene utilizzato per caricare la costante ReAuthPeriod nella macchina a stati del timer di riautenticazione di 802.1X.

D. Ho un tunneling guest, il tunnel Ethernet over IP (EoIP), configurato tra il mio controller WLC (Wireless LAN Controller) 4400, che agisce da WLC di ancoraggio, e diversi WLC remoti. La subnet WLC di ancoraggio può inoltrare le trasmissioni attraverso il tunnel EoIP dalla rete cablata ai client wireless associati ai controller remoti?

R. No, il WLC 4400 non inoltra le trasmissioni della subnet IP dal lato cablato ai client wireless attraverso il tunnel EoIP. Funzionalità non supportata. Cisco non supporta il tunneling della trasmissione subnet o del multicast nella topologia di accesso guest. Poiché la WLAN guest forza il punto di presenza del client in una posizione molto specifica nella rete, per lo più all'esterno del firewall, il tunneling della trasmissione della subnet può rappresentare un problema di sicurezza.

D. In una configurazione Wireless LAN Controller (WLC) e Lightweight Access Point Protocol (LWAPP), quali valori DSCP (Differentiated Services Code Point) vengono passati per il traffico vocale? Come viene implementato QoS sul WLC?

R. Le WLAN della soluzione Cisco Unified Wireless Network (UWN) supportano quattro livelli di QoS:

- Platinum/Voice
- Oro/Video
- Argento/Massimo sforzo (predefinito)

- Bronzo/Sfondo

È possibile configurare la WLAN del traffico vocale in modo che utilizzi QoS di platino, assegnare la WLAN a larghezza di banda ridotta in modo che usi QoS di bronzo e assegnare tutto il resto del traffico tra gli altri livelli QoS. per ulteriori informazioni, fare riferimento a Assegnazione di un profilo QoS a una WLAN.

D. I bridge Ethernet Linksys sono supportati in una soluzione Cisco Wireless Unified?

R. No, il WLC supporta solo prodotti Cisco WGB. Le WGB di Linksys non sono supportate. Sebbene Cisco Wireless Unified Solution non supporti i bridge Ethernet Linksys WET54G e WET11B, è possibile utilizzare questi dispositivi in una configurazione di soluzione unificata wireless se si utilizzano le seguenti linee guida:

- Collegare un solo dispositivo a WET54G o WET11B.
- Abilitare la funzione di clonazione MAC su WET54G o WET11B per clonare il dispositivo collegato.
- Installare i driver e il firmware più recenti sui dispositivi collegati a WET54G o WET11B. Questa linea guida è particolarmente importante per le stampanti JetDirect poiché le versioni precedenti del firmware causano problemi con DHCP.

Nota: altri bridge di terze parti non sono supportati. I passaggi citati possono essere eseguiti anche per altri bridge di terze parti.

D. Come memorizzare i file di configurazione sul controller WLC?

A. Il WLC contiene due tipi di memoria:

- RAM volatile: mantiene la configurazione corrente del controller attivo
- NVRAM (Nonvolatile RAM) - Mantiene la configurazione di riavvio

Quando si configura il sistema operativo nel WLC, si modifica la RAM volatile. È necessario salvare la configurazione dalla RAM volatile alla NVRAM per essere certi che il WLC si riavvii nella configurazione corrente.

Èimportante sapere quale memoria si sta modificando quando si eseguono le seguenti attività:

- Utilizzare la configurazione guidata.
- Cancellare la configurazione del controller.
- Salvare le configurazioni.
- Reimpostare il controller.
- Uscire dalla CLI.

Domande frequenti sulle funzionalità

D. Come impostare il tipo EAP (Extensible Authentication Protocol) sul controller WLC? Si desidera eseguire l'autenticazione su un accessorio Access Control Server (ACS) e nei registri viene visualizzato il tipo "EAP" non supportato.

R. Non esiste un'impostazione separata del tipo EAP sul WLC. Per Light EAP (LEAP), EAP

Flexible Authentication via Secure Tunneling (EAP-FAST) o Microsoft Protected EAP (MS-PEAP), è sufficiente configurare IEEE 802.1x o Wi-Fi Protected Access (WPA) (se si utilizza 802.1x con WPA). Tutti i tipi EAP supportati sul back-end RADIUS e sul client sono supportati tramite il tag 802.1x. L'impostazione EAP nel client e nel server RADIUS deve corrispondere.

Completare questi passaggi per abilitare EAP dalla GUI sul WLC:

1. Dall'interfaccia utente del WLC, fare clic su **WLAN**.
2. Viene visualizzato un elenco di WLAN configurate nel WLC. Fare clic su una rete WLAN.
3. In **WLAN > Modifica**, fare clic sulla scheda **Sicurezza**.
4. Fare clic su **Layer 2**, quindi scegliere Layer 2 Security come 802.1x o WPA+WPA2. È inoltre possibile configurare i parametri 802.1x disponibili nella stessa finestra. Infine, il WLC inoltra i pacchetti di autenticazione EAP tra il client wireless e il server di autenticazione.
5. Fare clic sui server **AAA**, quindi scegliere il server di autenticazione dal menu a discesa per questa WLAN. Si presume che il server di autenticazione sia già configurato a livello globale. Per informazioni su come abilitare l'opzione EAP sui WLC tramite l'interfaccia della riga di comando (CLI), fare riferimento alla sezione *Using the CLI to Configure RADIUS* della Cisco Wireless LAN Controller Configuration Guide, versione 7.0.116.0.

D. Che cos'è Fast SSID Changing?

R. La modifica rapida dell'SSID consente ai client di spostarsi tra gli SSID. Quando il client invia una nuova associazione per un SSID diverso, la voce del client nella tabella di connessione del controller viene cancellata prima che il client venga aggiunto al nuovo SSID. Quando Cambio rapido SSID è disabilitato, il controller applica un ritardo prima che i client possano passare a un nuovo SSID. Per informazioni su come abilitare Fast SSID Changing, consultare la sezione *Configurazione di Fast SSID Changing* della guida alla configurazione di Cisco Wireless LAN Controller, versione 7.0.116.0.

D. È possibile impostare un limite al numero di client che possono connettersi a una LAN wireless?

R. È possibile impostare un limite al numero di client che possono connettersi a una WLAN. Questa opzione è utile negli scenari in cui è presente un numero limitato di client che possono connettersi a un controller. Il numero di client che è possibile configurare per ciascuna WLAN dipende dalla piattaforma in uso.

Per informazioni sui limiti dei client per ciascuna WLAN per le diverse piattaforme dei controller, consultare la sezione Configurazione del numero massimo di client per WLAN della guida alla configurazione di Cisco Wireless LAN Controller, versione 7.0.116.0.

D. Che cos'è il PKC e come funziona con il controller WLC?

R. PKC è l'acronimo di Proactive Key Caching (CAC proattiva). È stato progettato come un'estensione dello standard 802.11i IEEE.

PKC è una funzione abilitata nei controller Cisco serie 2006/410x/440x che consente ai client wireless adeguatamente attrezzati di effettuare il roaming senza riautenticazione completa con un server AAA. Per comprendere il PKC, è necessario innanzitutto comprendere la memorizzazione nella cache delle chiavi.

La memorizzazione nella cache della chiave è una funzionalità che è stata aggiunta a WPA2. In questo modo, una stazione mobile può memorizzare nella cache le chiavi master (Pairwise Master Key [PMK]) ottenute tramite un'autenticazione riuscita con un punto di accesso (AP) e **riutilizzarle in un'associazione futura con lo stesso AP**. Ciò significa che un determinato dispositivo mobile deve eseguire l'autenticazione una sola volta con un punto di accesso specifico e memorizzare la chiave nella cache per un utilizzo futuro. La memorizzazione nella cache delle chiavi viene gestita tramite un meccanismo noto come PMKID (PMK Identifier), che è un hash della PMK, una stringa, la stazione e gli indirizzi MAC dell'access point. PMKID identifica in modo univoco PMK.

Anche con la memorizzazione nella cache delle chiavi, una stazione wireless deve autenticarsi con ogni access point da cui desidera ottenere il servizio. Questo comporta una latenza e un sovraccarico significativi, che ritardano il processo di consegna e possono impedire il supporto di applicazioni in tempo reale. Per risolvere questo problema, PKC è stato introdotto con WPA2.

PKC consente a una stazione di riutilizzare un PMK ottenuto in precedenza tramite un processo di autenticazione riuscito. In questo modo, non è più necessario che la stazione esegua l'autenticazione sui nuovi access point in roaming.

Pertanto, in un roaming all'interno del controller, quando un dispositivo mobile si sposta da un punto di accesso all'altro sullo stesso controller, il client ricalcola un PMKID utilizzando la chiave PMK utilizzata in precedenza e lo presenta durante il processo di associazione. Il WLC esegue una ricerca nella cache PMK per determinare se dispone di una voce di questo tipo. In caso affermativo, ignora il processo di autenticazione 802.1x e avvia immediatamente lo scambio di chiavi WPA2. In caso contrario, viene eseguito il processo di autenticazione 802.1X standard.

PKC è abilitato per impostazione predefinita con WPA2. Pertanto, quando si abilita WPA2 come protezione di layer 2 nella configurazione WLAN del WLC, il PKC viene abilitato sul WLC. Inoltre, configurare il server AAA e il client wireless per l'autenticazione EAP appropriata.

Il supplicant utilizzato dal lato client deve inoltre supportare WPA2 per consentire il funzionamento di PKC. PKC può essere implementato anche in un ambiente di roaming tra controller.

Nota: PKC non funziona con Aironet Desktop Utility (ADU) come supplicant client.

D. Quali sono le spiegazioni per queste impostazioni di timeout sul controller: Timeout ARP (Address Resolution Protocol), Timeout di inattività utente e Timeout sessione?

A. Il **timeout ARP** viene usato per eliminare le voci ARP sul WLC per i dispositivi provenienti dalla rete.

Il **timeout di inattività dell'utente:** quando un utente è inattivo senza alcuna comunicazione con il LAP per il periodo di tempo impostato come timeout di inattività dell'utente, il client viene deautenticato dal WLC. Il client deve eseguire nuovamente l'autenticazione e la riassociazione al WLC. Si usa in situazioni in cui un client può uscire dal LAP associato senza avvertire il LAP. Ciò può verificarsi se la batteria si esaurisce sul client o se gli associati del client si allontanano.

Nota: per accedere ad ARP e al timeout di inattività dell'utente sull'interfaccia utente del WLC, accedere al menu **Controller**. Scegliere **Generale** dal lato sinistro per trovare i campi ARP e Timeout inattività utente.

Il valore di Timeout sessione è il tempo massimo per una sessione client con il WLC. Dopo questo

periodo, il WLC disautentica il client e il client riesegue l'intero processo di autenticazione (riautenticazione). Ciò fa parte di una misura precauzionale di protezione per la rotazione delle chiavi di crittografia. Se si utilizza un metodo EAP (Extensible Authentication Protocol) con la gestione delle chiavi, la rigenerazione delle chiavi viene eseguita a ogni intervallo regolare per ottenere una nuova chiave di crittografia. Senza la gestione delle chiavi, questo valore di timeout indica il tempo necessario ai client wireless per eseguire una riautenticazione completa. Il timeout della sessione è specifico della WLAN. È possibile accedere a questo parametro dal menu **WLAN > Modifica**.

D. Che cos'è un sistema RFID? Quali tag RFID sono attualmente supportati da Cisco?

R. L'identificazione a radiofrequenza (RFID) è una tecnologia che utilizza la comunicazione a radiofrequenza per una comunicazione a corto raggio. Un sistema RFID di base è composto da etichette RFID, lettori RFID e software di elaborazione.

Attualmente Cisco supporta i tag RFID di AeroScout e Pango. Per ulteriori informazioni su come configurare i tag AeroScout, fare riferimento alla configurazione WLC per i tag RFID di AeroScout.

D. È possibile eseguire l'autenticazione EAP localmente sul WLC? C'è qualche documento che spiega questa funzione EAP locale?

R. Sì, l'autenticazione EAP può essere eseguita localmente sul WLC. Local EAP è un metodo di autenticazione che consente agli utenti e ai client wireless di essere autenticati localmente sul WLC. È progettato per l'utilizzo in uffici remoti che desiderano mantenere la connettività ai client wireless quando il sistema back-end viene interrotto o il server di autenticazione esterno si blocca. Quando si abilita EAP locale, il WLC funge da server di autenticazione. Per ulteriori informazioni su come configurare un WLC per l'autenticazione EAP-Fast locale, fare riferimento all'esempio di autenticazione EAP locale sul controller LAN wireless con EAP-FAST e configurazione del server LDAP.

D. In cosa consiste la funzione di sostituzione WLAN? Come configurare questa funzionalità? I LAP manterranno i valori di override della WLAN quando eseguono il failover sul WLC di backup?

R. La funzione di override della WLAN ci permette di scegliere le WLAN tra le WLAN configurate su un WLC che possono essere usate attivamente su un singolo LAP. Per configurare un override della WLAN, completare i seguenti passaggi:

1. Nell'interfaccia utente del WLC, fare clic sul menu **Wireless**.
2. Fate clic sull'opzione **Radio** sul lato sinistro, quindi scegliete **802.11 a/n** o **802.11 b/g/n**.
3. Fare clic sul collegamento **Configure** (Configura) dal menu a discesa sul lato destro che corrisponde al nome dell'access point su cui si desidera configurare la sostituzione WLAN.
4. Scegliere **Abilita** dal menu a discesa Override WLAN. Il menu Sostituzione WLAN è l'ultima voce sul lato sinistro della finestra.
5. Viene visualizzato l'elenco di tutte le WLAN configurate sul WLC.
6. Da questo elenco, selezionare le **WLAN** che si desidera visualizzare sul LAP e fare clic su **Apply** (Applica) per rendere effettive le modifiche.
7. Salvare la configurazione dopo aver apportato le modifiche.

Quando vengono registrati su altri WLC, gli AP conservano i valori di override WLAN, a condizione che i profili WLAN e gli SSID che si desidera sostituire siano configurati su tutti i WLC.

Nota: nel software del controller versione 5.2.157.0, la funzione di override WLAN è stata rimossa sia dalla GUI del controller che dalla CLI. Se il controller è configurato per l'override WLAN e si esegue l'aggiornamento al software del controller versione 5.2.157.0, il controller elimina la configurazione WLAN e trasmette tutte le WLAN. È possibile specificare che solo alcune WLAN devono essere trasmesse se si configurano i gruppi di punti di accesso. Ogni punto di accesso annuncia solo le WLAN abilitate che appartengono al suo gruppo di punti di accesso.

Nota: i gruppi di punti di accesso non consentono la trasmissione delle WLAN su ciascuna interfaccia radio dell'access point.

D. L'IPv6 è supportato sui Cisco Wireless LAN Controller (WLC) e sui Lightweight Access Point (LAP)?

R. Al momento, i controller serie 4400 e 4100 supportano solo il passthrough client IPv6. Supporto IPv6 nativo non supportato.

Per abilitare IPv6 sul WLC, selezionare la casella di controllo **IPv6 Enable** (Abilita IPv6) nella configurazione dell'SSID della WLAN nella pagina WLAN > Edit (Modifica).

Per supportare IPv6 è inoltre necessario disporre di EMM (Ethernet Multicast Mode). Se si disabilita EMM, i dispositivi client che utilizzano IPv6 perdono la connettività. Per abilitare EMM, andare alla pagina Controller > Generale e dal menu a discesa Ethernet Multicast Mode, scegliere **Unicast** o **Multicast**. In questo modo il multicast viene attivato in modalità Unicast o Multicast. Quando il multicast è abilitato come multicast unicast, i pacchetti vengono replicati per ogni punto di accesso. Poiché questa operazione può richiedere un utilizzo intensivo del processore, è consigliabile procedere con cautela. Multicast abilitato come multicast utilizza l'indirizzo multicast assegnato dall'utente per eseguire un'uscita multicast più tradizionale verso i punti di accesso (AP).

Nota: IPv6 non è supportato nei controller 2006.

Inoltre, è presente l'ID bug Cisco CSCsg78176, che impedisce l'uso del pass-through IPv6 quando si usa la funzione di override AAA.

D. Cisco serie 2000 Wireless LAN Controller (WLC) supporta l'autenticazione Web per gli utenti guest?

R. L'autenticazione Web è supportata su tutti i WLC Cisco. L'autenticazione Web è un metodo di autenticazione di livello 3 utilizzato per autenticare gli utenti con credenziali di autenticazione semplici. Non viene utilizzata alcuna crittografia. Per abilitare questa funzione, completare i seguenti passaggi:

1. Dalla GUI, fare clic sul menu **WLAN**.
2. Fare clic su una **rete WLAN**.
3. Andare alla scheda **Sicurezza** e scegliere **Layer 3**.
4. Selezionare la casella **Criteri Web** e scegliere **Autenticazione**.
5. Per salvare le modifiche, fare clic su **Apply** (Applica).
6. Per creare un database sul WLC con cui autenticare gli utenti, andare al menu **Security** sulla

GUI, selezionare **Local Net User** (Utente rete locale), quindi completare le seguenti azioni: Definire il nome utente e la password guest da utilizzare per l'accesso. Questi valori fanno distinzione tra maiuscole e minuscole.Scegli l'ID WLAN che utilizzi.**Nota:** per una configurazione più dettagliata, fare riferimento all'esempio di configurazione dell'autenticazione Web del controller LAN wireless.

D. È possibile gestire il WLC in modalità wireless?

R. Una volta abilitato, il WLC può essere gestito in modalità wireless. Per ulteriori informazioni su come abilitare la modalità wireless, consultare la sezione *Abilitazione delle connessioni wireless sulla GUI e sulla CLI* nella guida alla configurazione di Cisco Wireless LAN Controller, versione 7.0.116.0.

D. Che cos'è l'aggregazione dei collegamenti (LAG)? Come abilitare il LAG sui controller WLC?

A. LAG raggruppa tutte le porte del WLC in un'unica interfaccia EtherChannel. Il sistema gestisce in modo dinamico il bilanciamento del carico del traffico e la ridondanza delle porte con LAG.

In genere, all'interfaccia del WLC sono associati più parametri, tra cui l'indirizzo IP, il gateway predefinito (per la subnet IP), la porta fisica primaria, la porta fisica secondaria, il tag VLAN e il server DHCP. Quando non si usa il LAG, ogni interfaccia è solitamente mappata su una porta fisica, ma è possibile mappare più interfacce su una singola porta WLC. Quando si usa il LAG, il sistema mappa dinamicamente le interfacce sul canale della porta aggregata. Ciò contribuisce alla ridondanza delle porte e al bilanciamento del carico. Se una porta ha esito negativo, l'interfaccia viene mappata dinamicamente sulla successiva porta fisica disponibile e i LAP vengono bilanciati tra le porte.

Quando il LAG è abilitato su un WLC, il WLC inoltra i frame di dati sulla stessa porta su cui sono stati ricevuti. Il WLC si basa sullo switch adiacente per bilanciare il carico del traffico su EtherChannel. Il WLC non esegue da solo il bilanciamento del carico di EtherChannel.

D. Quali modelli di Wireless LAN Controller (WLC) supportano l'aggregazione dei collegamenti (LAG)?

R. I controller Cisco serie 5500 supportano il LAG nella versione software 6.0 o successive, i controller Cisco serie 4400 supportano il LAG nella versione software 3.2 o successive e il LAG è abilitato automaticamente sui controller in Cisco WiSM e nello switch Catalyst 3750G Integrated Wireless LAN Controller. Senza LAG, ciascuna porta del sistema di distribuzione su un controller Cisco serie 4400 supporta fino a 48 punti di accesso. Se il LAG è abilitato, la porta logica di un controller Cisco 4402 supporta fino a 50 punti di accesso, la porta logica di un controller Cisco 4404 supporta fino a 100 punti di accesso, mentre la porta logica dello switch Catalyst 3750G Integrated Wireless LAN Controller e di ciascun controller Cisco WiSM supporta fino a 150 punti di accesso.

i Cisco WLC 2106 e 2006 non supportano i LAG. I modelli precedenti, ad esempio i Cisco serie 4000 WLC, non supportano i LAG.

D. Qual è la funzione di mobilità con ancoraggio automatico in Unified Wireless Networks?

R. La mobilità con ancoraggio automatico (o mobilità WLAN guest) viene utilizzata per migliorare il bilanciamento del carico e la sicurezza dei client in roaming sulle WLAN (Wireless LAN). In condizioni di roaming normali, i dispositivi client si collegano a una WLAN e sono ancorati al primo controller che contattano. Se un client esegue il roaming in una subnet diversa, il controller su cui il client esegue il roaming imposta una sessione esterna per il client con il controller di ancoraggio. Con la funzione di mobilità con ancoraggio automatico, è possibile specificare un controller o un insieme di controller come punti di ancoraggio per i client su una WLAN.

Nota: l'ancoraggio di mobilità non deve essere configurato per la mobilità di layer 3. L'ancora per la mobilità viene utilizzata solo per il tunneling guest.

D. È possibile configurare un controller WLC (Cisco 2006 Wireless LAN Controller) come ancoraggio per una WLAN?

R. Un WLC di Cisco serie 2000 non può essere designato come ancoraggio per una WLAN. Tuttavia, una WLAN creata su un Cisco serie 2000 WLC può avere un Cisco serie 4100 WLC e un Cisco serie 4400 WLC come ancoraggio.

D. Che tipo di tunneling di mobilità viene utilizzato dal controller LAN wireless?

R. Il software dei controller versioni da 4.1 a 5.1 supporta il tunneling a mobilità asimmetrica e simmetrica. Il software del controller versione 5.2 o successive supporta solo il tunneling a mobilità simmetrica, ora sempre abilitato per impostazione predefinita.

Nel tunneling asimmetrico, il traffico dei client verso la rete cablata viene instradato direttamente tramite il controller esterno. Il tunneling asimmetrico si interrompe quando un router upstream ha abilitato il filtro del percorso inverso (RPF). In questo caso, il traffico client viene scartato sul router perché il controllo RPF assicura che il percorso di ritorno all'indirizzo di origine corrisponda al percorso da cui proviene il pacchetto.

Quando il tunneling a mobilità simmetrica è abilitato, tutto il traffico client viene inviato al controller di ancoraggio e può superare il controllo RPF. Il tunneling simmetrico per la mobilità è utile anche in queste situazioni:

- Questa operazione è utile se l'installazione di un firewall nel percorso del pacchetto client scarta i pacchetti perché l'indirizzo IP di origine non corrisponde alla subnet su cui i pacchetti vengono ricevuti.
- Se la VLAN del gruppo di access point sul controller di ancoraggio è diversa dalla VLAN dell'interfaccia WLAN sul controller esterno: in questo caso, il traffico del client può essere inviato su una VLAN non corretta durante gli eventi di mobilità.

D. Come è possibile accedere al WLC quando la rete non è operativa?

R. Quando la rete non è operativa, il WLC è accessibile tramite la porta di servizio. A questa porta viene assegnato un indirizzo IP in una subnet completamente diversa da quelle di altre porte del WLC, per questo motivo viene definita gestione fuori banda. Per ulteriori informazioni, fare riferimento alla sezione *Configurazione di porte e interfacce* della guida alla configurazione di Cisco Wireless LAN Controller, versione 7.0.116.0.

D. I Cisco Wireless LAN Controller (WLC) supportano la funzione di failover (o

ridondanza)?

R. Sì, se la rete WLAN contiene due o più WLC, è possibile configurarli per la ridondanza. In genere, un LAP si unisce al WLC primario configurato. Una volta che il WLC primario si guasta, il LAP si riavvia e si unisce a un altro WLC nel gruppo di mobilità. Il failover è una funzione in cui il LAP esegue il polling del WLC primario e, una volta funzionante, si unisce al WLC primario. Per ulteriori informazioni, fare riferimento all'esempio di configurazione del failover del controller WLAN per i Lightweight Access Point.

D. Qual è l'uso degli Access Control List (ACL) di preautenticazione nei Wireless LAN Controller (WLC)?

R. Con gli ACL di preautenticazione, come suggerisce il nome, è possibile autorizzare il traffico dei client da e verso un indirizzo IP specifico anche prima che il client venga autenticato. Quando si usa un server Web esterno per l'autenticazione Web, alcune piattaforme WLC richiedono un ACL di preautenticazione per il server Web esterno (il controller Cisco serie 5500, un controller Cisco serie 2100, la serie 2000 e il modulo di rete del controller). Per le altre piattaforme WLC, l'ACL di preautenticazione non è obbligatorio. Tuttavia, è buona norma configurare un ACL di preautenticazione per il server Web esterno quando si utilizza l'autenticazione Web esterna.

D. Ho una WLAN filtrata dall'indirizzo MAC e una WLAN completamente aperta nella mia rete. Il client sceglie la WLAN aperta per impostazione predefinita? Oppure il client si associa automaticamente all'ID WLAN impostato sul filtro MAC? Inoltre, perché è presente un'opzione "interface" (interfaccia) su un filtro MAC?

R. Il client può associarsi a qualsiasi WLAN a cui il client è configurato per connettersi. L'opzione interface (interfaccia) nel filtro MAC permette di applicare il filtro a una WLAN o a un'interfaccia. Se più WLAN sono collegate alla stessa interfaccia, è possibile applicare il filtro MAC all'interfaccia senza dover creare un filtro per ciascuna WLAN.

D. Come configurare l'autenticazione TACACS per gli utenti con privilegi di gestione sul controller WLC?

A. A partire dalla versione WLC 4.1, TACACS è supportato sui WLC. Per informazioni su come configurare TACACS+ in modo da autenticare gli utenti della gestione del WLC, fare riferimento alla configurazione di TACACS+.

D. A cosa serve l'impostazione di un errore di autenticazione eccessivo in un controller WLC?

R. Questa impostazione è uno dei criteri di esclusione dei client. L'esclusione dei client è una funzionalità di sicurezza nel controller. Il criterio viene utilizzato per creare una blacklist dei client allo scopo di impedire l'accesso non autorizzato alla rete o attacchi alla rete wireless.

Con questo criterio di errore di autenticazione Web eccessivo abilitato, quando il numero di tentativi di autenticazione Web non riusciti di un client supera il numero 5, il controller considera che il client ha superato il numero massimo di tentativi di autenticazione Web ed inserisce in una blacklist il client.

Per abilitare o disabilitare questa impostazione, completare la procedura seguente:

1. Dalla GUI del WLC, selezionare **Security > Wireless Protection Policies > Client Exclusion Policies** (Sicurezza > Criteri di protezione wireless > Criteri di esclusione client).
2. Selezionare o deselezionare **Errori di autenticazione Web eccessivi**.

D. Il punto di accesso autonomo (AP) è stato convertito in modalità lightweight. In modalità Lightweight AP Protocol (LWAPP) con il server AAA RADIUS per l'accounting dei client, in genere il client viene registrato con l'accounting RADIUS basato sull'indirizzo IP del WLC. È possibile impostare l'accounting RADIUS in base all'indirizzo MAC dell'access point associato al WLC e non all'indirizzo IP del WLC?

R. Sì, è possibile eseguire questa operazione con la configurazione laterale del WLC. Attenersi alla seguente procedura:

1. Dalla GUI del controller, in **Sicurezza > Contabilità Radius**, è disponibile una casella a discesa per Tipo di ID stazione di chiamata. Scegliere **Indirizzo MAC AP**.
2. Verificare questa condizione tramite il log del punto di accesso LWAPP. Qui è possibile vedere il campo ID stazione chiamata in cui viene visualizzato l'indirizzo MAC dell'access point a cui è associato il client specifico.

D. Come è possibile modificare il valore di timeout dell'handshake WPA (Wi-Fi Protected Access) su un controller WLC (Wireless LAN Controller) tramite CLI? So che è possibile farlo sui Cisco IOS® Access Point (AP) con il comando dot11 wpa handshake *value*, ma come si esegue questa operazione su un WLC?

R. La capacità di configurare il timeout dell'handshake WPA tramite i WLC è stata integrata nel software versione 4.2 e successive. Nelle versioni precedenti del software WLC, questa opzione non è necessaria.

Questi comandi possono essere utilizzati per modificare il timeout dell'handshake WPA:

```
    config advanced eap eapol-key-timeout <value>
    config advanced eap eapol-key-retries <value>
```

I valori predefiniti continuano a riflettere il comportamento corrente dei WLC.

```
   - the default value for eapol-key-timeout is 1 second.
   - the default value for eapol-key-retries is 2 retries
```

Nota: sugli access point IOS, questa impostazione è configurabile con il comando **dot11 wpa handshake**.

Èpossibile anche configurare gli altri parametri EAP con le opzioni del comando **config advanced eap**.

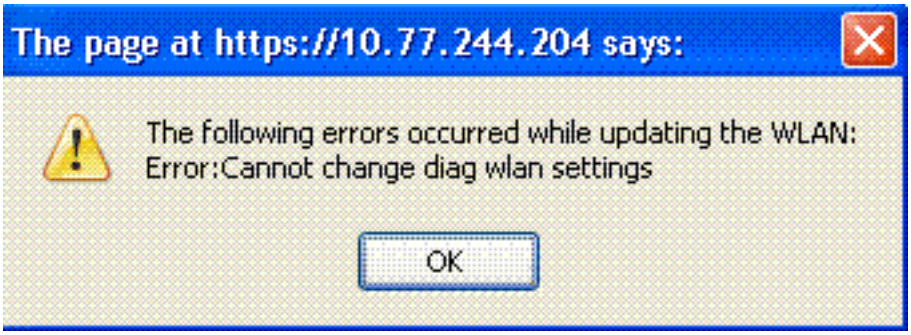
```
(Cisco Controller) >config advanced eap ?

eapol-key-timeout
   Configures EAPOL-Key Timeout in seconds.
eapol-key-retries
   Configures EAPOL-Key Max Retries.
```

```
identity-request-timeout
   Configures EAP-Identity-Request Timeout in seconds.
identity-request-retries
   Configures EAP-Identity-Request Max Retries.
key-index
   Configure the key index used for
   dynamic WEP(802.1x) unicast key (PTK).
max-login-ignore-identity-response
   Configure to ignore the same username count
   reaching max in the EAP identity response
request-timeout
   Configures EAP-Request Timeout in seconds.
request-retries
   Configures EAP-Request Max Retries.
```

D. A cosa serve la funzione del canale di diagnostica nella pagina WLAN > Modifica > Avanzate?

R. La funzionalità del canale diagnostico consente di risolvere i problemi di comunicazione con i client tramite una WLAN. Il client e i punti di accesso possono essere sottoposti a una serie definita di test per identificare la causa delle difficoltà di comunicazione che il client incontra e quindi consentire l'adozione di misure correttive per rendere il client operativo sulla rete. È possibile utilizzare la GUI o la CLI del controller per abilitare il canale di diagnostica e la CLI o il WCS del controller per eseguire i test di diagnostica.

Il canale di diagnostica può essere utilizzato solo per il test. Se si cerca di configurare l'autenticazione o la crittografia per la WLAN con il canale di diagnostica abilitato, viene visualizzato questo errore:



D. Qual è il numero massimo di gruppi di access point che possono essere configurati su un WLC?

R. Questo elenco mostra il numero massimo di gruppi di access point che è possibile configurare su un WLC:

- Massimo 50 gruppi di access point per i Cisco serie 2100 Controller e i moduli di rete dei controller
- Un massimo di 300 gruppi di punti di accesso per i controller Cisco serie 4400, Cisco WiSM e Cisco 3750G Wireless LAN Controller Switch
- Massimo 500 gruppi di access point per i controller Cisco serie 5500

Informazioni correlate

- Domande frequenti sui Wireless LAN Controller (WLC)

- Domande frequenti (FAQ) sui messaggi di errore e di sistema del controller WLC
- Domande frequenti su Lightweight Access Point
- Guida alla configurazione di Cisco Wireless LAN Controller, versione 7.0.116.0
- Supporto IPv6 sul controller LAN wireless
- Supporto dei prodotti wireless
- 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).