Risoluzione dei problemi in seguito a un errore di connessione di Lightweight Access Point (LAP) a un WLC

Sommario

Introduzione

In questo documento viene descritto il processo di rilevamento e unione di AireOS Wireless LAN Controller (WLC).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenze base della configurazione dei Lightweight Access Point (LAP) e dei Cisco AireOS WLC
- Nozioni base sul protocollo Lightweight Access Point Protocol (CAPWAP)

Componenti usati

Questo documento è incentrato sui WLC di AireOS e non copre Catalyst 9800, anche se il processo di join è per lo più simile.

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

Convenzioni

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

Panoramica del processo di individuazione e aggiunta a WLC

In una Cisco Unified Wireless Network, i LAP devono individuare e collegarsi a un WLC prima di poter servire i client wireless.

Tuttavia, la domanda è: come hanno fatto i LAP a trovare l'indirizzo IP di gestione del controller quando si trova su una subnet diversa?

Se non si indica al LAP dove si trova il controller con l'opzione DHCP 43, la risoluzione DNS (Domain Name System) di Cisco-capwap-controller.local_domain o la configurazione statica, il LAP non sa dove trovare l'interfaccia di gestione del controller nella rete.

Oltre a questi metodi, il LAP cerca automaticamente i controller con indirizzo di broadcast locale 255.255.255.255 nella subnet locale. Inoltre, il LAP ricorda l'indirizzo IP di gestione del suo controller e i controller presenti come peer di mobilità anche dopo il riavvio. Tuttavia, non appena l'AP si unisce a un altro WLC, ricorda solo l'IP di quel nuovo WLC e dei suoi peer mobili e non quelli precedenti. Pertanto, se si posiziona il LAP per primo sulla subnet locale dell'interfaccia di gestione, questo trova l'interfaccia di gestione del controller e ricorda l'indirizzo. Questa operazione è chiamata priming. Tuttavia, se il LAP viene in seguito sostituito, ciò non sarà sufficiente a trovare il controller. Cisco consiglia pertanto di utilizzare l'opzione DHCP 43 o i metodi DNS.

I LAP si connettono sempre all'indirizzo dell'interfaccia di gestione del controller con una richiesta di rilevamento. Il controller quindi comunica al LAP l'indirizzo IP dell'interfaccia AP-manager di layer 3 (che può coincidere con l'interfaccia di gestione predefinita) in modo che il LAP possa inviare una richiesta di collegamento all'interfaccia AP-manager in un secondo momento.

L'access point esegue questo processo all'avvio:

• **Il LAP si avvia e, se non ha già un indirizzo IP statico associato, gliene viene assegnato dinamicamente uno tramite il protocollo DHCP.**

• **Il LAP invia le richieste di rilevamento ai controller tramite vari algoritmi e compila un elenco di controller. In sostanza, il LAP apprende quanti più indirizzi di interfacce di gestione possibili per compilare l'elenco dei controller tramite:**

a. **Opzione DHCP 43 (valida per le aziende globali in cui uffici e controller si trovano in continenti diversi).**

b. **La voce DNS per** cisco-capwap-controller (utile per le aziende locali - può essere utilizzata anche per trovare dove si uniscono i nuovi access point) Se si utilizza CAPWAP, assicurarsi che esista una voce DNS per cisco-capwap-controller.

- **Gli indirizzi IP di gestione dei controller che il LAP ha già memorizzato.**
- **Un indirizzo di broadcast di layer 3 sulla subnet.**
- **Informazioni configurate staticamente.**
- **I controller presenti nel gruppo di mobilità del WLC a cui l'access point si è collegato ultimamente.**

Tra i metodi elencati, il più semplice da adottare per l'implementazione è avere i LAP sulla stessa subnet dell'interfaccia di gestione del controller in modo che i LAP possano trovare il controller usando l'indirizzo di broadcast di layer 3. Questo metodo deve essere utilizzato per le società che dispongono di una rete di piccole dimensioni e non dispongono di un server DNS locale.

Il secondo metodo di implementazione consigliato consiste nell'utilizzare una voce DNS con DHCP. È possibile avere più voci con lo stesso nome DNS. Ciò consente al LAP di rilevare più controller. Questo metodo deve essere utilizzato dalle società che dispongono di tutti i controller in un'unica posizione e sono proprietarie di un server DNS locale. Oppure, da aziende con più suffissi DNS e controller separati dal suffisso.

L'opzione DHCP 43 viene utilizzata dalle aziende di grandi dimensioni per localizzare le informazioni tramite DHCP. Questo metodo viene utilizzato dalle grandi aziende che hanno un solo suffisso DNS. Ad esempio, Cisco ha sedi in Europa, Australia e Stati Uniti. Per garantire che i LAP si colleghino solo ai controller locali, Cisco non può utilizzare una voce DNS e deve usare le informazioni dell'opzione DHCP 43 per comunicare ai LAP qual è l'indirizzo IP di gestione del controller locale.

Infine, la configurazione statica viene utilizzata per una rete senza server DHCP. È possibile configurare in modo statico le informazioni necessarie per collegarsi a un controller tramite la porta della console e la CLI degli access point. Per informazioni su come configurare in modo statico le informazioni sui controller tramite la CLI dell'access point, utilizzare questo comando:

```
AP#capwap ap primary-base <WLCName> <WLCIP>
```

Per informazioni su come configurare l'opzione DHCP 43 su un server DHCP, consultare l'esempio di configurazione dell'opzione DHCP 43

• Inviare una richiesta di rilevamento a ogni controller incluso nell'elenco e attendere la risposta di rilevamento del controller contenente il nome del sistema, gli indirizzi IP di AP-manager, il numero di AP già collegati a ogni interfaccia di AP-manager e la capacità in eccesso complessiva per il controller.

- Esaminare l'elenco dei controller e inviare una richiesta di collegamento a un controller in questo ordine (solo se l'access point ha ricevuto una risposta di rilevamento):

a. Nome del sistema del controller primario (precedentemente configurato sul LAP).

b. Nome del sistema del controller secondario (precedentemente configurato sul LAP).

c. Nome del sistema del terzo controller (precedentemente configurato sul LAP).

d. Controller primario (se il LAP non è stato precedentemente configurato con un nome di controller primario, secondario o terziario). Utilizzato per sapere sempre quale controller è un nuovo LAP (join).

e. Se non viene rilevata nessuna delle condizioni precedenti, bilanciare il carico tra i controller utilizzando il valore di capacità in eccesso nella risposta di rilevamento.

Se due controller hanno la stessa capacità in eccesso, inviare la richiesta di collegamento al primo controller che ha risposto alla richiesta di rilevamento. Se un singolo controller ha più AP-manager su più interfacce, scegliere l'interfaccia AP-manager con il minor numero di access point.

Il controller risponde a tutte le richieste di individuazione senza un controllo certificato o credenziali AP. Le richieste di join devono tuttavia disporre di un certificato valido per ottenere una risposta di join dal controller. Se il LAP non riceve una risposta di join a sua scelta, prova a usare il controller successivo nell'elenco, a meno che il controller non sia configurato (Primario/Secondario/Terziario).

- Quando riceve la risposta di collegamento, l'access point verifica che abbia la stessa immagine di quella del controller. In caso contrario, l'access point scarica l'immagine dal controller e si riavvia per caricare la nuova immagine, quindi inizia nuovamente il processo dal punto 1.

- Se l'immagine software è la stessa, l'access point chiede al controller la configurazione e passa allo stato registrato sul controller.

Dopo aver scaricato la configurazione, l'access point può ricaricarsi di nuovo per applicare la nuova configurazione. Pertanto, può verificarsi un ulteriore caricamento, ma è un comportamento normale.

Debug dal controller

Ci sono alcuni **debug** comandi sul controller che è possibile usare per vedere questo intero processo sulla CLI:

•

debug capwap events enable:mostra i pacchetti di rilevamento e i pacchetti di collegamento.

- **debug capwap packet enable**:mostra le informazioni sul livello dei pacchetti di rilevamento e collegamento.

- **debug pm pki enable**:mostra il processo di convalida del certificato.

- **debug disable-all**:disattiva il debug.

Da un'applicazione terminale in grado di acquisire l'output in un file di log, accedere alla console o alla Secure Shell (SSH) / Telnet del controller e immettere i seguenti comandi:

<#root>

config session timeout 120

config serial timeout 120

show run-config

(and spacebar thru to collect all)

debug mac addr <ap-radio-mac-address>

(in xx:xx:xx:xx:xx format)

debug client <ap-mac-address>

debug capwap events enable

debug capwap errors enable

debug pm pki enable

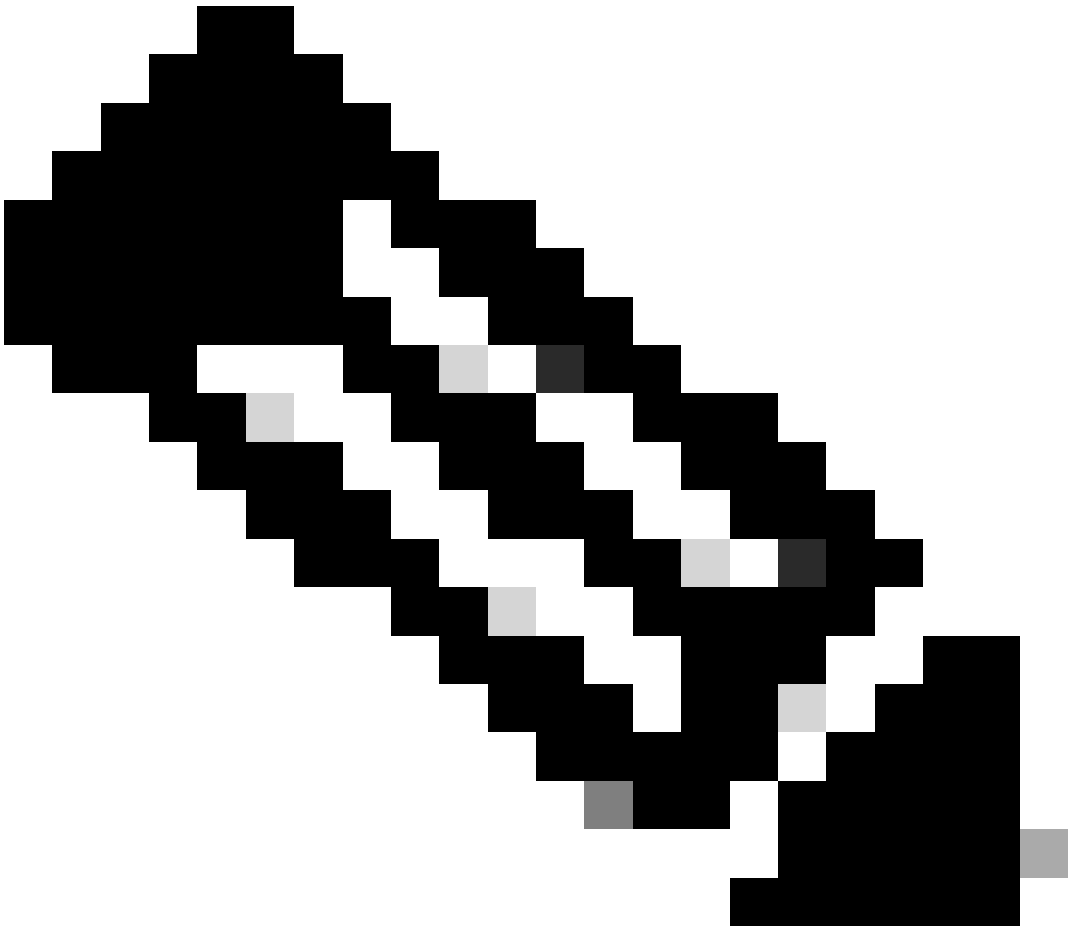
Dopo aver acquisito i debug, usare il comandodebug disable-all per disabilitare tutti i debug.

Le sezioni seguenti mostrano l'output di questi **debug** comandi quando il LAP si registra con il controller.

debug capwap events enable

Questo comando fornisce informazioni sugli eventi e sugli errori CAPWAP che si verificano durante il processo di individuazione e unione di CAPWAP.

Questo è l'output del **debug capwap events enable** comando per un LAP con la stessa immagine del WLC:



Nota: alcune righe dell'output sono state spostate nella seconda riga a causa di vincoli di spazio.

<#root>

debug capwap events enable

*spamApTask7: Jun 16 12:37:36.038: 00:62:ec:60:ea:20 Discovery Request from 172.16.17.99:46317

!--- CAPWAP discovery request sent to the WLC by the LAP.

*spamApTask7: Jun 16 12:37:36.039: 00:62:ec:60:ea:20 Discovery Response sent to 172.16.17.99 port 46317

!--- WLC responds to the discovery request from the LAP.

*spamApTask7: Jun 16 12:38:43.469: 00:62:ec:60:ea:20 Join Request from 172.16.17.99:46317

!--- LAP sends a join request to the WLC.

*spamApTask7: Jun 16 12:38:33.039: 00:62:ec:60:ea:20 Join Priority Processing status = 0, Incoming Ap's
*spamApTask7: Jun 16 12:38:43.469: 00:62:ec:60:ea:20 Join Request from 172.16.17.99:46317

*spamApTask7: Jun 16 12:38:43.472: 00:62:ec:60:ea:20 Join Version: = 134256640

*spamApTask7: Jun 16 12:38:43.473: 00:62:ec:60:ea:20 apType = 46 apModel: AIR-CAP2702I-E-K9

*spamApTask7: Jun 16 12:38:43.473: 00:62:ec:60:ea:20 Join resp: CAPWAP Maximum Msg element len = 90

*spamApTask7: Jun 16 12:38:43.473: 00:62:ec:60:ea:20 Join Response sent to 172.16.17.99:46317
*spamApTask7: Jun 16 12:38:43.473: 00:62:ec:60:ea:20 CAPWAP State: Join

!--- WLC responds with a join reply to the LAP.

*spamApTask7: Jun 16 12:38:43.964: 00:62:ec:60:ea:20 Configuration Status from 172.16.17.99:46317

*spamApTask7: Jun 16 12:38:43.964: 00:62:ec:60:ea:20 CAPWAP State: Configure

!--- LAP requests for the configuration information from the WLC.

*spamApTask7: Jun 16 12:38:43.964: 00:62:ec:60:ea:20 Updating IP info for AP 00:62:ec:60:ea:20 -- stati
*spamApTask7: Jun 16 12:38:43.964: 00:62:ec:60:ea:20 Updating IP 172.16.17.99 ===> 172.16.17.99 for AP
*spamApTask7: Jun 16 12:38:43.964: 00:62:ec:60:ea:20 Running spamDecodeVlanProfMapPayload for00:62:ec:6
*spamApTask7: Jun 16 12:38:43.964: 00:62:ec:60:ea:20 Setting MTU to 1485
*spamApTask7: Jun 16 12:38:44.019: 00:62:ec:60:ea:20 Configuration Status Response sent to 172:16:17:99

!--- WLC responds by providing all the necessary configuration information to the LAP.

*spamApTask7: Jun 16 12:38:46.882: 00:62:ec:60:ea:20 Change State Event Request from 172.16.17.99:46317

*spamApTask7: Jun 16 12:38:46.883: 00:62:ec:60:ea:20 Radio state change for slot: 0 state: 2 cause: 0 d
*spamApTask7: Jun 16 12:38:46.883: 00:62:ec:60:ea:20 Change State Event Response sent to 172.16.17.99:4
.
.
.
.

*spamApTask7: Jun 16 12:38:46.883: 00:62:ec:60:ea:20 CAPWAP State: Run

*spamApTask7: Jun 16 12:38:46.883: 00:62:ec:60:ea:20 Sending the remaining config to AP 172.16.17.99:46
.
.
.
.

!--- LAP is up and ready to service wireless clients.

```
*spamReceiveTask: Jun 16 12:38:46.897: 00:62:ec:60:ea:20 Configuration update request for RrmInterferen
*spamReceiveTask: Jun 16 12:38:46.897: 00:62:ec:60:ea:20 Configuration update request for RrmNeighbourC
*spamReceiveTask: Jun 16 12:38:46.897: 00:62:ec:60:ea:20 Configuration update request for RrmReceiveCtr
*spamReceiveTask: Jun 16 12:38:46.897: 00:62:ec:60:ea:20 Configuration update request for CcxRmMeas pay
```

!--- WLC sends all the RRM and other configuration parameters to the LAP.

Come accennato nella sezione precedente, una volta che un LAP si registra sul WLC, controlla se ha la stessa immagine del controller. Se le immagini sul LAP e sul WLC sono diverse, i LAP scaricano per prima cosa la nuova immagine dal WLC. Se il LAP ha la stessa immagine, continua a scaricare la configurazione e gli altri parametri dal WLC.

Questi messaggi vengono visualizzati nell'output del **debug capwap events enable** comando se il LAP scarica un'immagine dal controller come parte del processo di registrazione:

```
*spamApTask6: Jun 17 14:23:28.677: 00:62:ec:60:ea:20 Sending image data block of length 1324 and msgLen
*spamApTask6: Jun 17 14:23:28.677: 00:62:ec:60:ea:20 Image Data Request sent to 172.16.17.201:46318
*spamApTask6: Jun 17 14:23:28.693: 00:62:ec:60:ea:20 Image data Response from 172.16.17.201:46318
```

Una volta completato il download dell'immagine, il LAP si riavvia, esegue il rilevamento e si unisce di nuovo all'algoritmo.

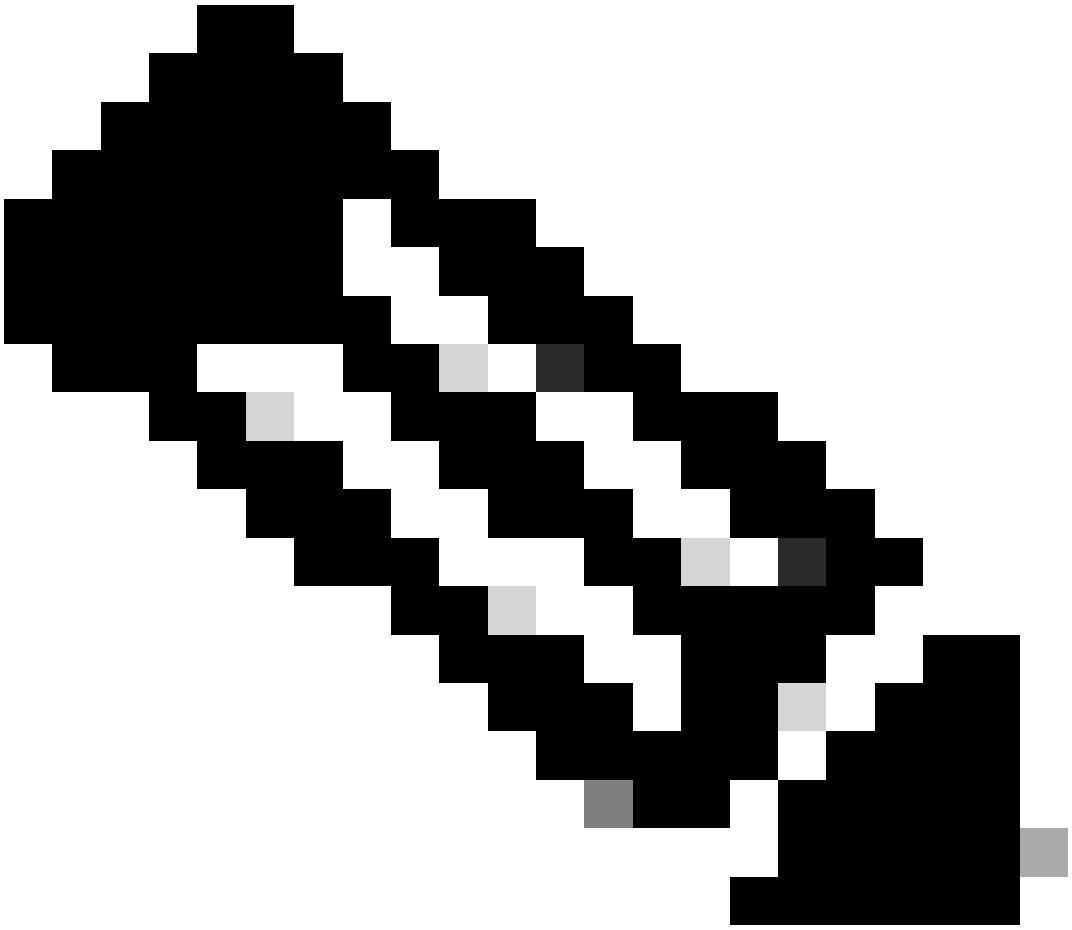
debug pm pki enable

Come parte del processo di join, il WLC autentica ogni LAP confermando la validità del relativo certificato.

Quando l'access point invia la richiesta di collegamento CAPWAP al WLC, incorpora il certificato X.509 nel messaggio CAPWAP. L'access point genera anche un ID di sessione casuale incluso nella richiesta di collegamento CAPWAP. Quando il WLC riceve la richiesta di aggiunta CAPWAP, convalida la firma del certificato X.509 con la chiave pubblica dell'access point e verifica che il certificato sia stato rilasciato da un'autorità di certificazione attendibile.

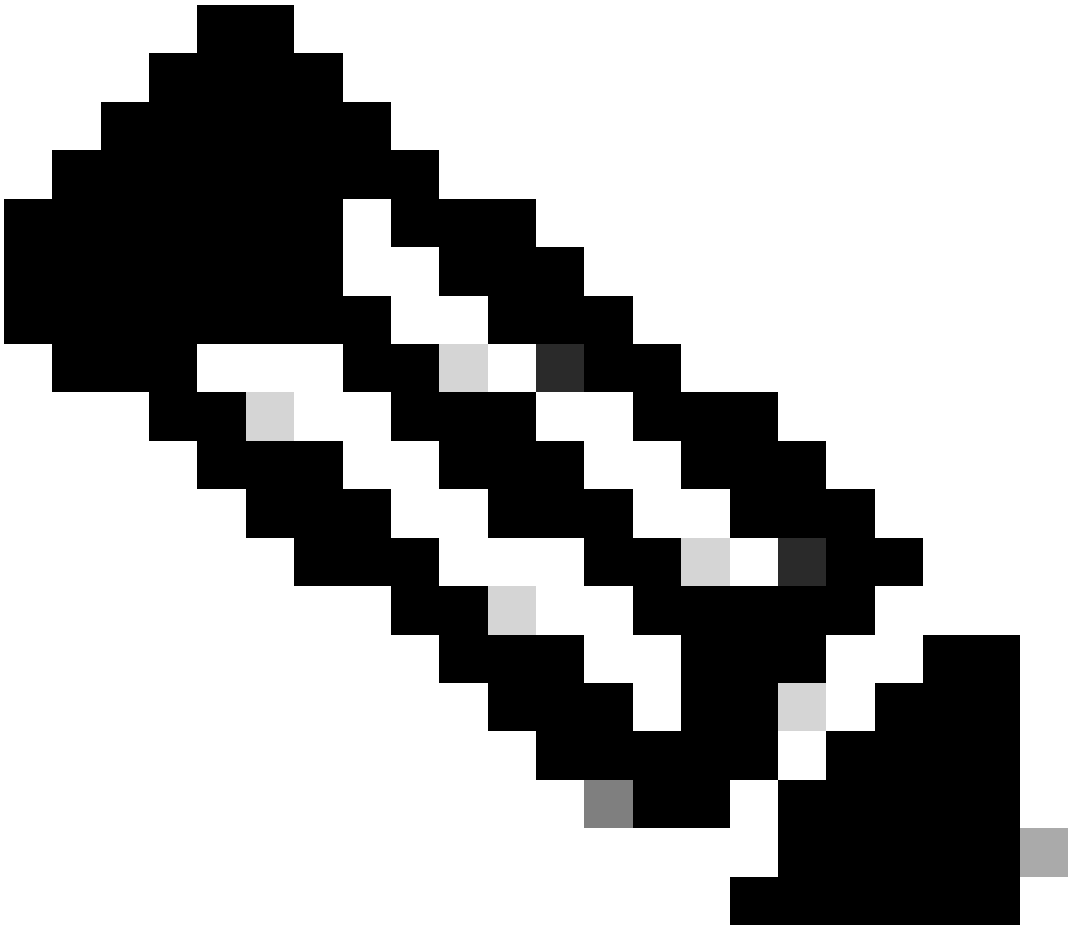
Vengono inoltre analizzate la data e l'ora di inizio per l'intervallo di validità del certificato AP e vengono confrontate la data e l'ora con la data e l'ora corrispondenti (pertanto è necessario impostare l'orologio del controller in prossimità della data e dell'ora correnti). Se il certificato X.509 è convalidato, il WLC genera una chiave di crittografia AES casuale. Il WLC inserisce le chiavi AES nel suo motore di crittografia in modo da poter crittografare e decrittografare i futuri messaggi di controllo CAPWAP scambiati con l'AP. Tenere presente che i pacchetti di dati vengono inviati in chiaro nel tunnel CAPWAP tra il LAP e il controller.

Il **debug pm pki enable** comando mostra il processo di convalida della certificazione che si verifica nella fase di join sul controller. Il **debug pm pki enable** comando visualizza anche la chiave hash AP al processo di join, se l'access point ha un certificato autofirmato (SSC) creato dal programma di conversione LWAPP. Se il punto di accesso dispone di un certificato di installazione prodotto (MIC), non verrà visualizzata alcuna chiave hash.



Nota: tutti gli access point prodotti dopo giugno 2006 hanno un certificato MIC.

Di seguito è riportato l'output del **debug pm pki enable** comando quando il LAP con un MIC si unisce al controller:



Nota: alcune righe dell'output sono state spostate nella seconda riga a causa di vincoli di spazio.

<#root>

```
*spamApTask4: Mar 20 11:05:15.687: [SA] OpenSSL Get Issuer Handles: locking ca cert table

*spamApTask4: Mar 20 11:05:15.688: [SA] OpenSSL Get Issuer Handles: x509 subject_name /C=US/ST=Californ
CN=AP3G2-1005cae83a42/emailAddress=support@cisco.com
*spamApTask4: Mar 20 11:05:15.688: [SA] OpenSSL Get Issuer Handles:
```

issuer_name /O=Cisco Systems/CN=Cisco Manufacturing CA

```
*spamApTask4: Mar 20 11:05:15.688: [SA] OpenSSL Get Issuer Handles: CN AP3G2-1005cae83a42
*spamApTask4: Mar 20 11:05:15.688: [SA] OpenSSL Get Issuer Handles: issuerCertCN Cisco Manufacturing CA
*spamApTask4: Mar 20 11:05:15.688: [SA] GetMac: MAC: 1005.cae8.3a42
*spamApTask4: Mar 20 11:05:15.688: [SA] OpenSSL Get Issuer Handles: openssl Mac Address in subject is 1
*spamApTask4: Mar 20 11:05:15.688: [SA] OpenSSL Get Issuer Handles: CN AP3G2-1005cae83a42
*spamApTask4: Mar 20 11:05:15.688: [SA] OpenSSL Get Issuer Handles: issuerCertCN Cisco Manufacturing CA
*spamApTask4: Mar 20 11:05:15.688: [SA] GetMac: MAC: 1005.cae8.3a42
*spamApTask4: Mar 20 11:05:15.688: [SA] OpenSSL Get Issuer Handles: openssl Mac Address in subject is 1
*spamApTask4: Mar 20 11:05:15.688: [SA] OpenSSL Get Issuer Handles: Cert Name in subject is AP3G2-1005c

*spamApTask4: Mar 20 11:05:15.688: [SA] OpenSSL Get Issuer Handles: Extracted cert issuer from subject

*spamApTask4: Mar 20 11:05:15.688: [SA] OpenSSL Get Issuer Handles:
```

Cert is issued by Cisco Systems.

```
*spamApTask4: Mar 20 11:05:15.688: [SA] Retrieving x509 cert for CertName cscoDefaultMfgCaCert
*spamApTask4: Mar 20 11:05:15.688: [SA] sshpmGetCID: called to evaluate <cscoDefaultMfgCaCert>
*spamApTask4: Mar 20 11:05:15.688: [SA] sshpmGetCID: Found matching CA cert cscoDefaultMfgCaCert in row
*spamApTask4: Mar 20 11:05:15.688: [SA] Found CID 260e5e69 for certname cscoDefaultMfgCaCert

*spamApTask4: Mar 20 11:05:15.688: [SA] CACertTable: Found matching CID cscoDefaultMfgCaCert in row 5 x

*spamApTask4: Mar 20 11:05:15.688: [SA] Retrieving x509 cert for CertName cscoDefaultNewRootCaCert
*spamApTask4: Mar 20 11:05:15.688: [SA] sshpmGetCID: called to evaluate <cscoDefaultNewRootCaCert>
*spamApTask4: Mar 20 11:05:15.688: [SA] sshpmGetCID: Found matching CA cert cscoDefaultNewRootCaCert in

*spamApTask4: Mar 20 11:05:15.688: [SA] Found CID 28d7044e for certname cscoDefaultNewRootCaCert
*spamApTask4: Mar 20 11:05:15.688: [SA] CACertTable: Found matching CID cscoDefaultNewRootCaCert in row
*spamApTask4: Mar 20 11:05:15.691: [SA] Verify User Certificate: X509 Cert Verification return code: 1
*spamApTask4: Mar 20 11:05:15.691: [SA] Verify User Certificate: X509 Cert Verification result text: ok
*spamApTask4: Mar 20 11:05:15.691: [SA] sshpmGetCID: called to evaluate <cscoDefaultMfgCaCert>
*spamApTask4: Mar 20 11:05:15.691: [SA] sshpmGetCID: Found matching CA cert cscoDefaultMfgCaCert in row

*spamApTask4: Mar 20 11:05:15.691: [SA]
```

Verify User Certificate: OPENSSL X509_Verify: AP Cert Verfied Using >cscoDefaultMfgCaCert<

```
*spamApTask4: Mar 20 11:05:15.691: [SA] OpenSSL Get Issuer Handles:
```

Check cert validity times (allow expired NO)

```
*spamApTask4: Mar 20 11:05:15.691: [SA] sshpmGetCID: called to evaluate <cscoDefaultIdCert>
*spamApTask4: Mar 20 11:05:15.691: [SA] sshpmGetCID: Found matching ID cert cscoDefaultIdCert in row 2
*spamApTask4: Mar 20 11:05:15.691: [SA] sshpmFreePublicKeyHandle: called with 0x1b0b9380

*spamApTask4: Mar 20 11:05:15.691: [SA] sshpmFreePublicKeyHandle:
```

freeing public key

Debug dall'access point

Se i debug del controller non indicano una richiesta di join, è possibile eseguire il debug del processo dall'access point se quest'ultimo dispone di una porta console. È possibile visualizzare il processo di avvio dell'access point con questi comandi, a condizione che venga prima attivata la modalità di abilitazione (la password predefinita è Cisco).

- **debug dhcp detail** :mostra le informazioni DHCP opzione 43.
- **debug ip udp**: visualizza tutti i pacchetti UDP ricevuti e trasmessi dall'access point.
- debug capwap client event :mostra gli eventi capwap dell'access point.

- **debug capwap client error**:mostra gli errori capwap dell'access point.

- **debug dtls client event**:mostra gli eventi DTLS dell'access point.
- **debug dtls error enable**:mostra gli errori DTLS dell'access point.
- **undebug all**:disabilita i debug sull'access point.

Di seguito è riportato un esempio dell'output dei debug capwapcomandi. Questo output parziale fornisce un'idea dei pacchetti inviati dall'access point durante il processo di avvio per individuare un controller e aggiungerlo.

```
<#root>

AP can discover the WLC via one of these options :


!--- AP discovers the WLC via option 43


*Jun 28 08:43:05.839: %CAPWAP-5-DHCP_OPTION_43: Controller address 10.63.84.78 obtained through DHCP
*Jun 28 08:43:15.963: %CAPWAP-3-EVENTLOG: Discovery Request sent to 10.63.84.78 with discovery type set


!--- capwap Discovery Request using the statically configured controller information.


*Jun 28 08:43:15.963: %CAPWAP-3-EVENTLOG: Discovery Request sent to 10.63.84.32 with discovery type set


!--- Capwap Discovery Request sent using subnet broadcast.
```

```
*Jun 28 08:43:15.963: %CAPWAP-3-EVENTLOG: Discovery Request sent to 255.255.255.255 with discovery type
```

!--- capwap Join Request sent to AP-Manager interface on DHCP discovered controller.

```
*Jun 28 08:40:29.031: %CAPWAP-5-SENDJOIN: sending Join Request to 10.63.84.78
```

Perché il LAP non si collega al controller?

Verifica delle condizioni principali

- L'access point e il WLC possono comunicare?
- Accertarsi che l'access point ottenga un indirizzo da DHCP (verificare che il server DHCP abbia in lease l'indirizzo MAC dell'access point).
- Eseguire il ping tra l'access point e il controller.
- Verificare che la configurazione STP sullo switch sia corretta, in modo che i pacchetti alle VLAN non vengano bloccati.
- Se i ping hanno esito positivo, assicurarsi che l'access point abbia almeno un metodo con cui rilevare almeno una singola console WLC o telnet/ssh nel controller con cui eseguire i debug.

-

Ad ogni riavvio dell'access point, viene avviata la sequenza di rilevamento del WLC e si cerca di individuare l'access point. Riavviare l'access point e verificare se si collega al WLC.

Ecco alcuni dei problemi più comuni che impediscono il collegamento dei LAP al WLC.

Avviso sul campo: scadenze dei certificati - FN63942

I certificati integrati nell'hardware sono validi per un periodo di 10 anni dopo la produzione. Se i punti di accesso o il WLC hanno più di 10 anni, i certificati scaduti possono causare problemi di aggiunta ai punti di accesso. Ulteriori informazioni su questo problema sono disponibili nel seguente avviso: Notifica: FN63942.

Problemi potenziali da cercare: esempi

Problema 1: l'ora del controller non rientra nell'intervallo di validità del certificato

Completare questa procedura per risolvere il problema:

- Immettere i comandidebug dtls client error + debug dtls client event nell'access point:

<#root>

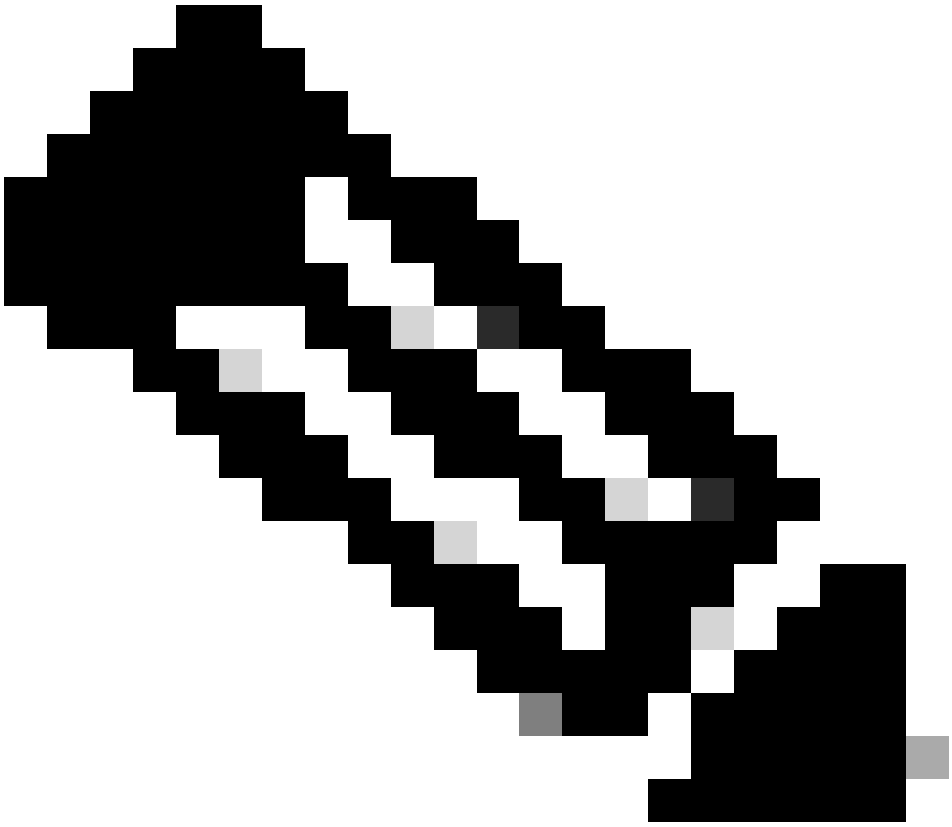
```
*Jun 28 09:21:25.011: DTLS_CLIENT_EVENT: dtls_process_Certificate: Processing...Peer certificate v
*Jun 28 09:21:25.031: DTLS_CLIENT_ERROR: ../capwap/base_capwap/capwap/base_capwap_wtp_dtls.c:509 C
*Jun 28 09:21:25.031: DTLS_CLIENT_EVENT: dtls_send_Alert: Sending FATAL :
```

Bad certificate Alert

```
*Jun 28 09:21:25.031: DTLS_CLIENT_EVENT: dtls_client_process_record: Error processing Certificate.
*Jun 28 09:21:25.031: DTLS_CLIENT_EVENT: dtls_disconnect: Disconnecting DTLS connection 0x8AE7FD0
*Jun 28 09:21:25.031: DTLS_CLIENT_EVENT: dtls_free_connection: Free Called... for Connection 0x8AE
*Jun 28 09:21:25.031: DTLS_CLIENT_EVENT: dtls_send_Alert: Sending FATAL : Close notify Alert
```

Queste informazioni indicano chiaramente che l'ora del controller non rientra nell'intervallo di validità del certificato del punto di accesso. Pertanto, l'access point non può registrarsi sul controller. I certificati installati nell'access point hanno un intervallo di validità predefinito. È necessario impostare l'ora del controller in modo che rientri nell'intervallo di validità del certificato del punto di accesso.

• Eseguire il **show time** comando dalla CLI del controller per verificare che la data e l'ora impostate sul controller rientrino in questo intervallo di validità. Se la data e l'ora del controller non rientrano nell'intervallo di validità del certificato, modificarle opportunamente.



Nota: se l'ora non è impostata correttamente sul controller, scegliere Commands > Set Time in modalità GUI del controller o usare il comando config time nella CLI del controller per impostare l'ora del controller.

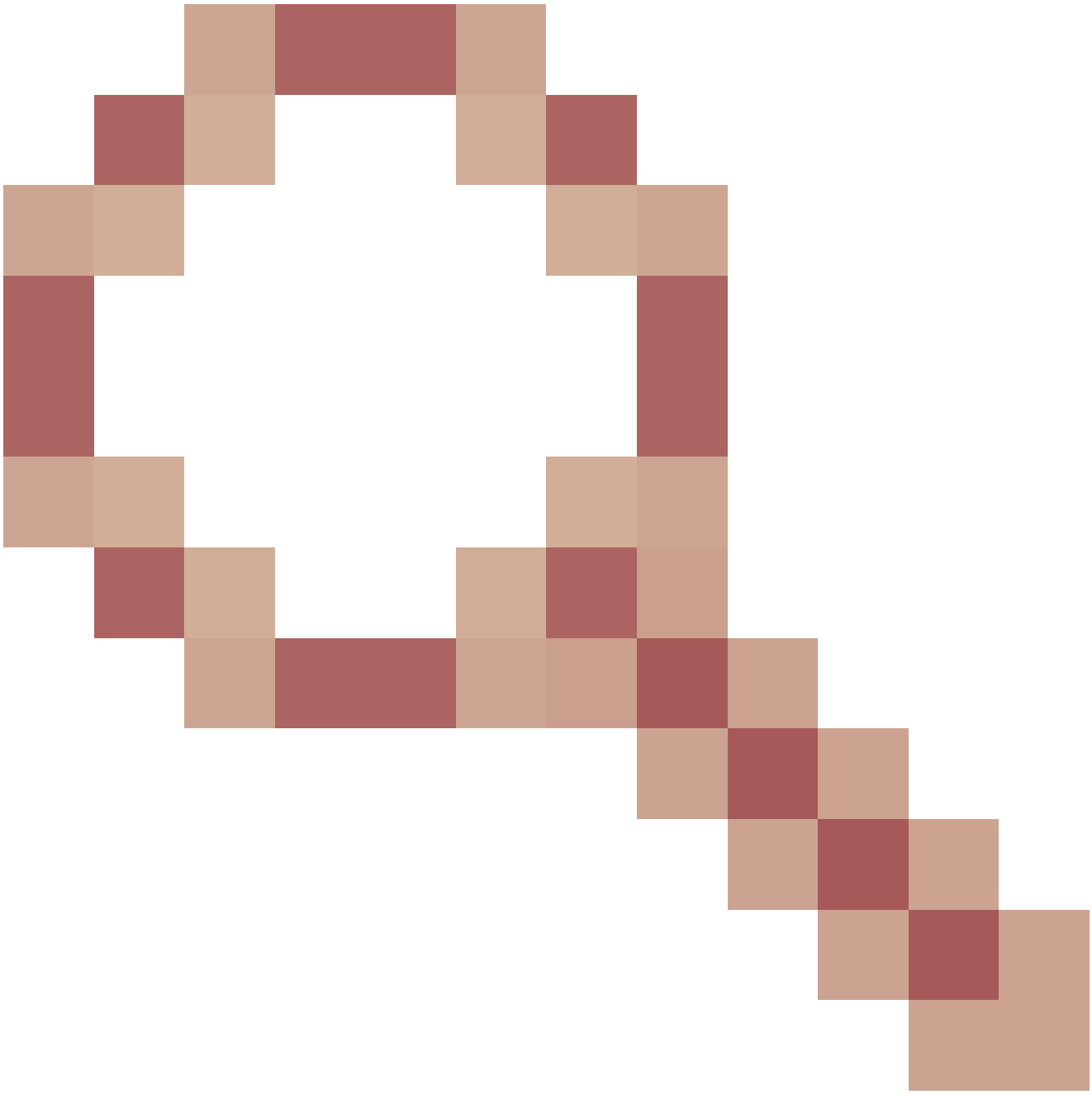
- Sugli access point con accesso CLI, verificare i certificati con il **show crypto ca certificates** comando da AP CLI.

Questo comando consente di verificare l'intervallo di validità del certificato impostato nell'access point. Ecco un esempio:

```
AP00c1.649a.be5c#show crypto ca cert
.........................................
.........................................
.........................................
.........................................
Certificate
Status: Available
Certificate Serial Number (hex): 7D1125A900000002A61A
Certificate Usage: General Purpose
Issuer:
cn=Cisco Manufacturing CA SHA2
o=Cisco
Subject:
Name: AP1G2-00c1649abe5c
e=support@cisco.com
cn=AP1G2-00c1649abe5c
o=Cisco Systems
l=San Jose
st=California
c=US
CRL Distribution Points:
http://www.cisco.com/security/pki/crl/cmca2.crl
Validity Date:
start date: 01:05:37 UTC Mar 24 2016
end date: 01:15:37 UTC Mar 24 2026
Associated Trustpoints: Cisco_IOS_M2_MIC_cert
Storage:
.................................
.................................
.................................
```

L'intero output non è elencato perché all'output di questo comando possono essere associati molti intervalli di validità. Prendere in considerazione solo l'intervallo di validità specificato dal Trustpoint associato: Cisco_IOS_MIC_cert con il nome dell'access point appropriato nel campo del nome. In questo output di esempio, è `Nome: C1200-001563e50c7e`. Questo è l'intervallo di validità del certificato effettivo da prendere in considerazione.

- Fare riferimento all'ID bug Cisco CSCuq19142



LAP/WLC MIC o SSC life expiration cause DTLS failure: Cisco bug ID CSCuq19142.

Problema 2: mancata corrispondenza nel dominio normativo

Nell'output del **debug capwap events enable** comando viene visualizzato questo messaggio:

<#root>

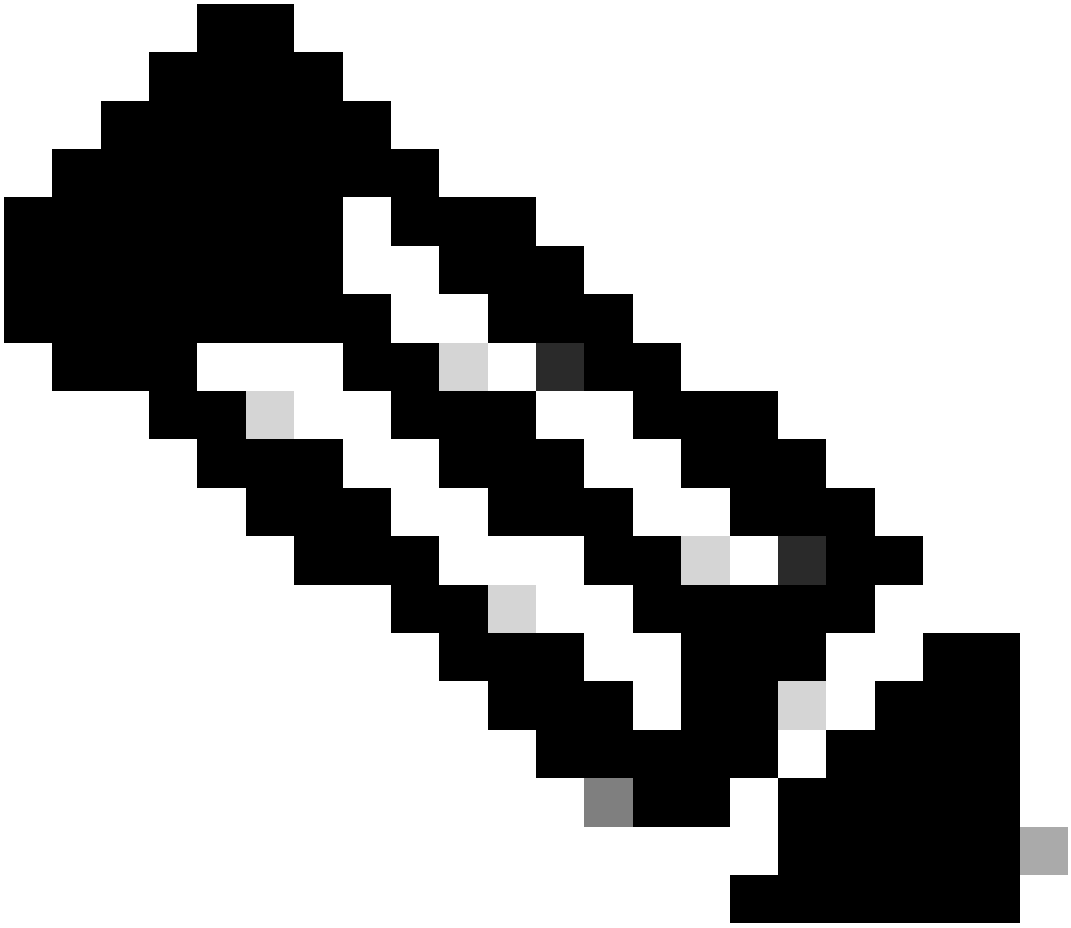
```
*spamApTask7: Jun 28 11:56:49.177: 00:cc:fc:13:e5:e0 AP 00:cc:fc:13:e5:e0: Country code is not configure
*spamApTask7: Jun 28 11:56:49.177: 00:cc:fc:13:e5:e0 AP 00:cc:fc:13:e5:e0: Country code is not configure
```

***spamApTask7: Jun 28 11:56:49.177: 00:cc:fc:13:e5:e0 Setting MTU to1485**
***spamApTask7: Jun 28 11:56:49.177: 00:cc:fc:13:e5:e0 AP 00:cc:fc:13:e5:e0: Country code is not configure**
***spamApTask7: Jun 28 11:56:49.177: 00:cc:fc:13:e5:e0 Regulatory Domain Mismatch: AP 00:cc:fc:13:e5:e0 no**
***spamApTask7: Jun 28 11:56:49.177: 00:cc:fc:13:e5:e0 Finding DTLS connection to delete for AP (192:168:4**
***spamApTask7: Jun 28 11:56:49.177: 00:cc:fc:13:e5:e0 Disconnecting DTLS Capwap-Ctrl session 0x1d4df620 f**
***spamApTask7: Jun 28 11:56:49.177: 00:cc:fc:13:e5:e0 acDtlsPlumbControlPlaneKeys: lrad:192.168.47.29(603**

WLC msglog show these messages :

*spamApTask5: Jun 28 11:52:06.536: %CAPWAP-3-DTLS_CLOSED_ERR: capwap_ac_sm.c:7095 00:cc:fc:13:e5:e0: DT
closed forAP 192:168:47:28 (60389), Controller: 10:63:84:78 (5246) Regulatory Domain Mismatch

Il messaggio indica chiaramente che c'è una mancata corrispondenza nel dominio normativo del LAP e del WLC. Il WLC supporta più domini normativi, ma ogni dominio normativo deve essere selezionato prima che un access point possa essere aggiunto da quel dominio. Ad esempio, il WLC che usa il dominio normativo -A può essere usato solo con gli access point che usano il dominio normativo -A (e così via). Quando si acquistano access point, assicurarsi che condividano lo stesso dominio normativo. Solo in questo modo gli l'access point possono registrarsi sul WLC.



Nota: le onde radio 802.1b/g e 802.11a devono trovarsi nello stesso dominio normativo di un unico access point.

Problema 3: elenco di autorizzazioni AP abilitato sul WLC; LAP non presente nell'elenco di autorizzazioni

In questi casi, il messaggio seguente viene visualizzato sul controller nell'output del debug capwap events enable comando:

<#root>

```
Wed Sep 12 17:42:39 2007: 00:0b:85:51:5a:e0 Received CAPWAP DISCOVERY REQUEST
from AP 00:0b:85:51:5a:e0 to 00:0b:85:33:52:80 on port '1'
```

```
Wed Sep 12 17:42:39 2007: 00:0b:85:51:5a:e0 Successful transmission of
CAPWAP Discovery-Response to AP 00:0b:85:51:5a:e0 on Port 1
Wed Sep 12 17:42:39 2007: 00:0b:85:51:5a:e0 Received LWAPP DISCOVERY REQUEST
from AP 00:0b:85:51:5a:e0 to ff:ff:ff:ff:ff:ff on port '1'
Wed Sep 12 17:42:39 2007: 00:0b:85:51:5a:e0 Successful transmission of
CAPWAP Discovery-Response to AP 00:0b:85:51:5a:e0 on Port 1
Wed Sep 12 17:42:50 2007: 00:0b:85:51:5a:e0 Received CAPWAP JOIN REQUEST
from AP 00:0b:85:51:5a:e0 to 00:0b:85:33:52:80 on port '1'
Wed Sep 12 17:42:50 2007: 00:0b:85:51:5a:e0 AP ap:51:5a:e0: txNonce  00:0B:85:33:52:80
rxNonce  00:0B:85:51:5A:E0
Wed Sep 12 17:42:50 2007: 00:0b:85:51:5a:e0 CAPWAP Join-Request MTU path from
AP 00:0b:85:51:5a:e0 is 1500, remote debug mode is 0
Wed Sep 12 17:42:50 2007:
```

spamRadiusProcessResponse: AP Authorization failure

for 00:0b:85:51:5a:e0

Se si usa un LAP con una porta console, quando si usa il comando viene visualizzato questo messaggiodebug capwap client error:

```
<#root>

APO01d.a245.a2fb#
*Mar  1 00:00:52.267: LWAPP_CLIENT_ERROR_DEBUG: spamHandleJoinTimer: Did not receive the
Join response
*Mar  1 00:00:52.267: LWAPP_CLIENT_ERROR_DEBUG:
```

No more AP manager IP addresses remain.

Anche in questo caso, è chiaro che il LAP non fa parte dell'elenco di autorizzazioni dei punti di accesso sul controller.

È possibile visualizzare lo stato dell'elenco di autorizzazioni AP con questo comando:

<#root>

```
(Cisco Controller) >
```

show auth-list

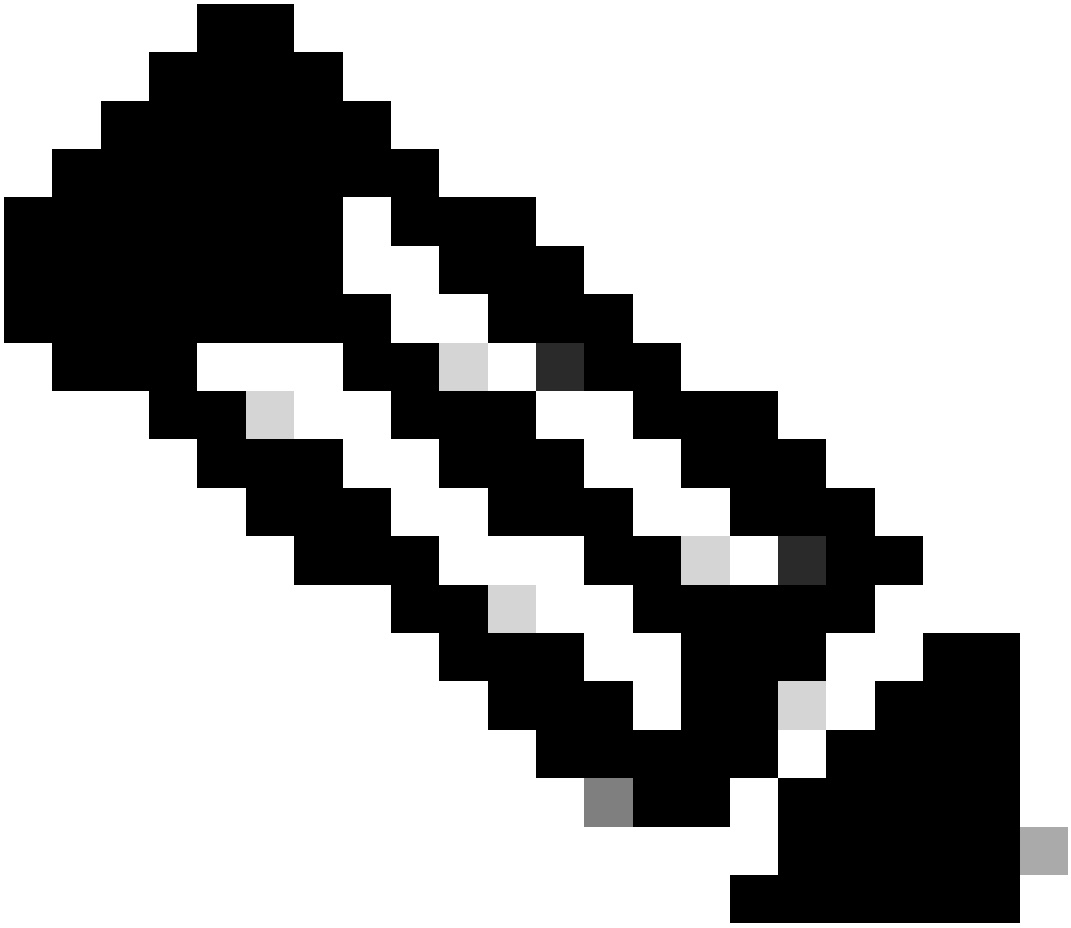
```
Authorize APs against AAA ..... enabled
Allow APs with Self-signed Certificate (SSC) .... disabled
```

Per aggiungere un LAP all'elenco delle autorizzazioni dei punti di accesso, usare il config auth-list add mic <AP MAC Address> comando. Per ulteriori informazioni su come configurare l'autorizzazione del LAP, fare riferimento alla configurazione di esempio dell'autorizzazione del Lightweight Access Point (LAP) in una Cisco Unified Wireless Network.

Problema 4: certificato o chiave pubblica danneggiata nell'access point

Il LAP non può collegarsi al controller a causa di un problema nel certificato.

Eseguire i debug capwap errors enable comandi e **debug pm pki enable** . Vengono visualizzati dei messaggi che indicano le chiavi o i certificati danneggiati.



Nota: a causa dei limiti di spazio, in alcuni punti l'output è stato suddiviso su due righe.

<#root>

```
Tue Aug 12 17:36:09 2008: 00:0f:24:a9:52:e0
 CAPWAP
```

Join Request does not include valid certificate in CERTIFICATE_PAYLOAD
from AP 00:0f:24:a9:52:e0

```
.
Tue Aug 12 17:36:09 2008: 00:0f:24:a9:52:e0
 Deleting and removing AP 00:0f:24:a9:52:e0 from fast path
Tue Aug 12 17:36:09 2008: 00:0f:24:a9:52:e0 Unable to free public key for AP
```

Per risolvere il problema, usare una di queste due opzioni:

- MIC AP - Richiesta di autorizzazione restituzione materiali (RMA).
- AP LSC - Effettuare nuovamente il provisioning del certificato LSC.

Problema 5: il controller riceve il messaggio di individuazione AP su una VLAN errata (viene visualizzato il messaggio di individuazione debug, ma non la risposta)

Questo messaggio viene visualizzato nell'output deldebug capwap events enable comando:

<#root>

Received a Discovery Request with subnet broadcast with wrong AP IP address (A.B.C.D)!

Questo messaggio indica che il controller ha ricevuto una richiesta di individuazione da parte di un indirizzo IP di trasmissione con un indirizzo IP di origine che non si trova in alcuna subnet configurata sul controller. Ciò significa anche che il controller è quello che scarta il pacchetto.

Il problema è che l'access point non è quello che ha inviato la richiesta di rilevamento all'indirizzo IP di gestione. Il controller segnala una richiesta di rilevamento broadcast da una VLAN non configurata sul controller. Questo si verifica in genere quando i trunk permettono le VLAN e non le restringono alle VLAN wireless.

Completare questa procedura per risolvere il problema:

- Se il controller si trova su un'altra subnet, gli access point devono essere **avviati** per l'indirizzo IP del controller oppure devono

ricevere l'indirizzo IP dei controller con l'utilizzo di uno dei metodi di rilevamento.

- Lo switch è configurato in modo da consentire alcune VLAN non sul controller. Limitare le VLAN autorizzate sui trunk.

Problema 6: il punto di accesso non è in grado di collegarsi al WLC, il firewall blocca le porte necessarie

Se nella rete aziendale viene utilizzato un firewall, verificare che queste porte siano abilitate sul firewall in modo che il LAP si colleghi e comunichi con il controller.

È necessario abilitare queste porte:

- Abilitare queste porte UDP per il traffico CAPWAP:
  - Dati - 5247
  - Controllo - 5246
- Abilitare queste porte UDP per il traffico di mobilità:
  - 16666 - 16666
  - 16667 - 16667

- Abilitare le porte UDP 5246 e 5247 per il traffico CAPWAP.

- TCP 161 e 162 per SNMP (per Wireless Control System [WCS])

Queste porte sono facoltative (a seconda dei requisiti):

- 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 per l'accesso CLI

Problema 7: indirizzo IP duplicato nella rete

Si tratta di un altro problema comune che si verifica quando l'AP tenta di unirsi al WLC. È possibile visualizzare questo messaggio di errore quando l'access point tenta di collegarsi al controller.

<#root>

No more AP manager IP addresses remain

Uno dei motivi di questo messaggio di errore è la presenza di un indirizzo IP duplicato sulla rete che corrisponde all'indirizzo IP dell'AP-manager. In questo caso, il LAP mantiene le avviazioni del ciclo di alimentazione e non può unirsi al controller.

I debug mostrano che il WLC riceve le richieste di rilevamento LWAPP dagli access point e trasmette una risposta di rilevamento LWAPP agli access point.

Tuttavia, i WLC non ricevono le richieste di collegamento LWAPP dagli access point.

Per risolvere questo problema, eseguire il ping del gestore AP da un host cablato sulla stessa subnet IP dell'AP-manager. Quindi, controllare la cache ARP. Se viene rilevato un indirizzo IP duplicato, rimuovere il dispositivo con l'indirizzo IP duplicato o modificare l'indirizzo IP sul dispositivo in modo che abbia un indirizzo IP univoco sulla rete.

L'access point potrà quindi collegarsi al WLC.

Problema 8: i LAP con immagine Mesh non sono in grado di unirsi al WLC

Il Lightweight Access Point non si registra sul WLC. Il registro visualizza il seguente messaggio di errore:

```
AAA Authentication Failure for UserName:5475xxx8bf9c User
     Type: WLAN USER
```

Ciò può accadere se il Lightweight Access Point è stato fornito con un'immagine mesh ed è in modalità bridge. Se il LAP è stato ordinato con un software mesh, è necessario aggiungerlo all'elenco degli access point autorizzati. Selezionare Security > AP Policies (Sicurezza > Policy AP) e aggiungere l'access point all'elenco degli access point autorizzati. L'access point deve quindi unirsi, scaricare l'immagine dal controller, quindi registrare il WLC in modalità bridge. Infine, è necessario selezionare la modalità locale sull'access point. Il LAP scarica l'immagine, si riavvia e si registra nuovamente sul controller in modalità locale.

Problema 9: indirizzo errato di DHCP Microsoft

I punti di accesso possono rinnovare rapidamente i propri indirizzi IP quando viene effettuato un tentativo di connessione a un WLC, il che può causare ai server DHCP Windows di contrassegnare questi IP come BAD_ADDRESS che potrebbe rapidamente ridurre il pool DHCP. Per ulteriori informazioni, consultare il capitolo Client Roaming della guida alla configurazione di Cisco Wireless Controller, versione 8.2.

Informazioni correlate

- **Supporto tecnico Cisco e download**

- **Processo di unione dell'access point con Catalyst 9800**

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).