Risoluzione dei problemi dei controller LAN wireless AireOS

Sommario

Introduzione

In questo documento viene descritto come usare i comandi **debug** e **show** per risolvere i problemi dei controller WLC.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

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.

Problemi dei componenti dei controller

Firme IDS

- debug wips sig enable

NAC

- debug nac events enable
- debug nac packets enable

OEAP

Comandi show del controller

- show ap join stats detail <ap mac add>
- show h-reap summary
- show h-reap latency
- show ap link-encryption
- show ap data-plane

Show/debug lato AP

- show logging (visualizza registri)
- show lwapp/capwap client rcb
- show lwapp/capwap client config
- test lwapp/capwap iapp-data-echo
- debug lwapp/capwap iapp-data-echo
- show lwapp/capwap reap
- show controller

Classificazione di elementi non autorizzati basata su regole

Debug da raccogliere

- debug dot11 rogue rule enable

Acquisizioni da effettuare

Non applicabile.

Output di config e show da raccogliere

- show rogue rule summary
- show rogue rule detailed <rule>
- show rogue ap detailed <rogue-mac> (se un particolare elemento non autorizzato è classificato erroneamente)

Controllo di elementi non autorizzati

Verificare che nella rete sia configurato un server DHCP per il punto di accesso non autorizzato da utilizzare se si utilizza l'indirizzamento IP statico.

Debug da raccogliere

- debug dot11 rogue enable

Acquisizioni da effettuare

Traccia Airopeek sul canale non autorizzato.

> **Nota:** Prestare attenzione ai fotogrammi non associati.

Output di config e show da raccogliere

- show rogue ap detailed <contained rogue-mac>
- show ap config 802.11b/a <nome-ap del comando precedente>

Firma IDS

Assicurarsi che ci sia un server DHCP configurato sulla rete per l'access point non autorizzato da utilizzare se si ricorre all'indirizzamento IP statico.

Debug da raccogliere

- debug wips sig enable

Acquisizioni da effettuare

Acquisizione Airopeek sulla firma del canale rilevata.

Output di debug e show da raccogliere

Nel software precedente alla versione 5.2, è possibile usare LWAPP al posto di CAPWAP per questi comandi:

- **show capwap ids sig dump**- Esegue il dump delle firme e dei conteggi delle visite di rilevamento delle firme che includono l'indirizzo MAC con le visite più grandi. Include anche lo stato corrente della traccia del pacchetto IDS.
- **show capwap ids rogue containment <slot#> chan**: mostra l'elenco corrente delle richieste di controllo degli elementi non autorizzati in corrispondenza di questo AP. Le richieste di controllo sono raggruppate per canale.
- **show capwap ids rogue containment <slot#> rad**: mostra l'elenco corrente delle richieste di controllo degli elementi non autorizzati in corrispondenza di questo AP. Questo elenco corrisponde all'elenco di richieste ricevute a partire dal controller.

- **debug capwap ids sig**: attiva i debug per la firma IDS e il rilevamento del controllo.

- **test capwap ids trace match <nome-tipo-messaggio>**- Traccia tutti i pacchetti ricevuti dal modulo IDS Signature Detection del tipo di messaggio=<nome-tipo-messaggio>; <message type-name> = FF per tracciare tutti i tipi di messaggio. I debug delle firme nella sezione 8.2.1 devono essere attivati per visualizzare i pacchetti tracciati.
- **test capwap ids trace rcv <nome-tipo>**- Traccia per tutti i pacchetti che corrispondono a qualsiasi firma attualmente installata per il modulo di rilevamento firma IDS del tipo di messaggio=<nome-tipo-messaggio>; <message type-name> = FF per tracciare tutti i tipi di messaggio corrispondenti a una firma. I debug delle firme nella sezione 8.2.1 devono essere attivati per visualizzare i pacchetti tracciati.

RLDP

Debug da raccogliere

Sul WLC:

- debug dot11 rldp enable

Sull'AP:

- debug lwapp client mgmt

Acquisizioni da effettuare

Acquisizione Airopeek sul canale non autorizzato.

Output di config e show da raccogliere

- config rogue ap rldp initiate <rogue-mac>

Canale di diagnostica

Debug da raccogliere

- debug client <client mac>

- debug ccxdiag all enable

Acquisizioni da effettuare

Acquisizione Airopeek sul canale da cui è impostato l'AP. Si consiglia di evitare l'applicazione di filtri perché i pacchetti beacon e di richiesta/risposta possono non essere rilevati.

Output di config e show da raccogliere

- show sysinfo
- show wlan x
- show run-config
- show tech-support
- show debug
- show msglog
- show client summary
- show client detail <client mac>

Dettagli client

- Hardware client
- Dettagli del software supplicant come la relativa versione, il relativo nome (ad esempio, Aironet Desktop Utility [ADU] o Odyssey) e la versione del driver nel caso di ADU
- Sistema operativo client

Mobilità tra controller

Debug da raccogliere

- debug client <client mac> su entrambi i WLC
- l'handoff della mobilità di debug viene abilitato su entrambi i WLC (ricordare l'ordine e abilitare sempre prima il client di debug).
- debug pem state enable

- Se il percorso di controllo della mobilità o i dati sono inattivi, attivare il comando "debug mobility keepalive enable" su entrambi gli switch (ricordare la versione software su entrambi i controller).
- Se il protocollo ARP (Address Resolution Protocol) non funziona, attivare il comando "debug arp all enable" su entrambi gli switch.
- Se il protocollo DHCP non funziona, attivare le opzioni "debug dhcp message enable" e "debug dhcp packet enable" su entrambi gli switch.
- Se è coinvolto IPSec: debug pm sa-export enable, debug pm sa-import enable.
- Se il client si connette dopo un po', mostra quanto tempo ci è voluto.

Acquisizioni da effettuare

Acquisizione tramite roaming, ad esempio CCKM, PMKID o TGR.

Output di config e show da raccogliere

Uguale a quanto indicato in Problema di connessione del client, oltre a:

- show pmk-cache <client mac> (sul controller di destinazione)
- show client details <client mac> (quando il client è connesso a un AP obsoleto)
- show mobility summary (su entrambi i WLC)

Dettagli client

Uguale a quanto indicato per il tipo di roaming specifico, ad esempio CCKM, PMKID o TGR.

AP honeypot

Debug da raccogliere

Non applicabile.

Acquisizioni da effettuare

Acquisire la traccia di Airopeek sul canale su cui viene ricevuta la trap per confermare che il router utilizza il SSID Cisco.

Output di config e show da raccogliere

- show traplog

Integrazione di AirMagnet

Debug da raccogliere

Sul WLC per problemi relativi a NMSP:

- debug wips nmsp enable
- debug wips event enable
- debug wips error enable

Per problemi relativi a CAPWAP:

- debug wips event enable
- debug wips error enable
- debug iapp error enable
- debug iapp event enable

Per informazioni sulla segnalazione di avvisi/dispositivi compromessi:

- debug wips all enable

Sull'AP:

- debug capwap am event
- debug capwap am error

Acquisizioni da effettuare

- Acquisizione Airopeek dell'attacco

- Acquisizione Ethereal dei report (inviati come pacchetto di dati)

Output di config e show da raccogliere

Sull'AP:

- show capwap am stats
- show capwap am buffer [run it few times]
- show capwap am policy [alarm-id]
- show capwap am alarm [alarm-id]

Autenticazione locale

Aspetti da controllare prima di registrare un bug

Accertarsi che il client possa essere associato alla WLAN. In caso contrario, il problema è al livello dot1x. Se si utilizzano i certificati, verificare che nel WLC siano installati dispositivi e certificati CA. Inoltre, accertarsi di aver selezionato l'autorità di certificazione corretta nella configurazione di autenticazione locale per selezionare il set di certificati corretto sul WLC.

Se per le credenziali utente viene utilizzato il database locale, verificare che il nome utente esista nel database. Se si utilizza il protocollo LDAP (Lightweight Directory Access Protocol), vedere la sezione relativa al debug di LDAP per ulteriori informazioni sul debug.

Debug da raccogliere

WLC:

- debug aaa local-auth eap framework errors enable
- debug aaa local-auth eap method errors enable
- debug aaa local-auth eap method events enable
- debug aaa local-auth eap method sm enable
- debug aaa local-auth db enable
- debug aaa local-auth shim enable

Output di config e show da raccogliere

- show local-auth config
- show local-auth statistics
- show local-auth certificates (quando si utilizza un metodo EAP (Extensible Authentication Protocol) con certificati)

Dettagli client

Il tipo di client, più i dettagli di configurazione EAP che mostrano quale metodo è selezionato e quali parametri sono impostati per tale metodo sul client. Inoltre, il testo di qualsiasi messaggio di errore visualizzato sul client.

Debug del controller

- debug pm pki enable: mostra i dettagli sulla convalida dei certificati.
- debug aaa events enable: è utile se si riscontrano problemi correlati agli elenchi di

autorizzazioni.
- show certificate lsc summary: per qualsiasi riepilogo correlato a LSC.

Autenticazione generale AAA

Questi debug sono utili per il debug di problemi relativi all'autenticazione, all'autorizzazione o all'account RADIUS:

Debug da raccogliere

- debug client <client mac>: fornisce informazioni su come vengono applicati gli attributi correlati alla riautenticazione, come session-timeout e action-type.
- debug aaa events enable: aiuta a risolvere i problemi relativi all'utilizzo dei diversi server AAA per l'autenticazione, l'autorizzazione e l'account.
- debug aaa packet enable: consente di risolvere i problemi relativi ai diversi attributi AAA ricevuti e applicati.

Acquisizioni da effettuare

Se i debug precedenti non indicano il problema, è possibile raccogliere un'acquisizione cablata tra il controller e il server RADIUS.

Output di config e show da raccogliere

Uguale a quanto indicato in Problema di connessione del client, oltre a:

- show radius summary

Dettagli client

Uguale a quanto indicato in Problema di connessione del client.

TACACS+

Debug da raccogliere

- debug aaa tacacs enable (sul WLC); raccolta del log sul server ACS/RADIUS per l'account)
- debug aaa events
- debug aaa detail
- debug dot11 mobile
- debug dot11 state
- debug pem events
- debug pem state

Acquisizioni da effettuare

- Se i debug precedenti non indicano il problema, è possibile raccogliere un'acquisizione cablata tra il controller e il server RADIUS.

Output di config e show da raccogliere

- show tacacs summary

- Problema relativo a Change of Authorization (CoA) e Packet of Disconnect (PD): RFC 3576
- show radius summary

LDAP

Aspetti da controllare prima di registrare un bug

Assicurarsi che il server LDAP sia controllabile mediante ping dal WLC.

Se si utilizza l'autenticazione EAP locale e di Active Directory, questi metodi EAP non sono supportati:

- LEAP
- EAP-FAST MSCHAPv2
- PEAP MSCHAPv2

Active Directory non è in grado di restituire una password non crittografata utilizzabile per l'autenticazione MSCHAPv2.

Debug da raccogliere

- debug aaa ldap enable

Se il problema si verifica quando si utilizza LDAP con l'autenticazione locale, vedere la sezione Autenticazione locale per ulteriori debug.

Output di config e show da raccogliere

- show ldap summary
- show ldap <server no.>
- show ldap statistics
- mostra statistiche di autenticazione locale (se il problema si verifica quando viene utilizzato con LDAP con l'autenticazione EAP locale)

Protezione dei frame di gestione (MFP) del client

Per tutti i problemi

- debug wps mfp client
- show wps mfp summary

Output di config e show da raccogliere

- show wps mfp statistics

Problemi di configurazione

Debug del controller:

- debug wps mfp lwapp
- debug lwapp mfp (su AP Aironet)

Il client non si associa

Debug del controller:

- debug wps mfp client
- debug wps mfp detail
- debug pem state
- debug pem events
- debug dot1x events

Output di config e show da raccogliere:

- show msglog
- show client detail

Debug aggiuntivi per AP 1130/1240 quando il client non si associa

- debug dot11 mgmt msg
- debug dot11 aaa manager all (per la modalità indipendente H-REAP)

Debug per AP Aironet quando il client non si associa in modalità indipendente H-REAP

- debug dot11 mfp client
- debug dot11 mgmt msg
- debug dot11 mgmt interface
- debug dot11 mgmt station
- debug dot11 supp-sm-dot1x
- debug dot11 aaa manager all
- debug dot11 wpa-cckm-km-dot1x

Mobilità

Debug del controller

- debug wps mfp mm enable
- debug mobility directory

Output di config e show da raccogliere

- show mobility summary
- show mobility statistics

Segnalazione dei problemi

Debug del controller

- debug wps mfp report

Output di config e show da raccogliere

- show wps mfp statistics

  Nota: Questo deve essere richiamato immediatamente dopo la generazione degli errori.

Problemi relativi a FIPS

Quando il controller è in modalità FIPS (Federal Information Processing Standard), è possibile utilizzare solo funzioni crittografiche approvate. Di conseguenza, è necessario bloccare SSL per utilizzare l'algoritmo di autenticazione TLS_RSA con crittografia AES.

Impossibile accedere al menu di avvio

Questa è una funzione per FIPS. La funzionalità è abilitata con questo comando:

- config switchconfig boot-break disable

Impossibile scaricare una nuova immagine

- Questa è una funzione per FIPS. Il trasferimento è disabilitato quando l'interruzione dell'avvio è disabilitata.

Wireless Client utilizza l'autenticatore locale con EAP-TLS, EAP-FAST e PEAP

Debug da raccogliere

A seconda dei problemi di comunicazione, è possibile abilitare i seguenti debug:

- debug wps cids enable
- debug locp event enable
- debug emweb server enable
- debug aaa local-auth eap method events enable

Acquisizioni da effettuare

Traccia dello sniffer tra il WLC e il dispositivo con il problema.

> **Nota:** Il WLC può avviare la comunicazione non appena il servizio corrispondente viene avviato. Si consiglia di avviare lo sniffer prima dell'accensione del WLC.

Output di config e show da raccogliere

- show switchconfig

512 WLAN/gruppi di AP

512 WLAN

Il bug della licenza 512 WLAN si verifica se il client può connettersi a un access point 'default-group' ma non a un access point impostato su un gruppo di access point personalizzato.

Output di show da raccogliere sul controller:

- show sysinfo
- show running-config
- show wlan summary
- show wlan apgroup
- show msglog

Output di show da raccogliere sull'AP:

- show controller
- show capwap client mn
- show log

Debug da raccogliere:

- debug client xx:xx:xx:xx:xx:xx
- debug group enable
- debug capwap event

> **Nota:** Dopo aver usato il comando **debug client<mac client>, i** debug o qualsiasi altro comando di debug devono essere attivati. Con questo comando vengono disabilitati tutti i debug precedenti.

Traccia da raccogliere:

- wireless trace

Gruppi di AP

Qualsiasi problema relativo all'aggiunta o all'eliminazione del gruppo AP o all'aggiunta di un'interfaccia al gruppo AP.

Output di show da raccogliere:

- show sysinfo
- show running-config
- show wlan summary
- show wlan apgroup
- show msglog

Debug da raccogliere:

- debug group enable

ACL, ACL pre-autenticazione e ACL CPU

```
>show acl ?
summary        Display a summary of the Access Control Lists.
detailed       Display detailed Access Control List information.
cpu            Display CPU Acl Information
```

DHCP

Debug DHCP in banda

- debug dhcp message enable
- debug dhcp packet enable

Debug DHCP per l'attivazione di porte di servizio

- debug dhcp service-port enable

Problemi relativi all'accesso guest

WLAN guest

- debug mobility handoff enable
- debug pem events enable
- debug pem state enable

Per problemi relativi a DHCP:

- debug dhcp packet enable
- debug dhcp message enable

Per problemi di connessione mobile:

- debug dot11 events enable
- debug dot11 mobile enable

Per problemi relativi a RADIUS/AAA:

- debug dot1x aaa enable

Problemi relativi all'alta affidabilità del WLC

Failover dell'AP

Problema di configurazione

Raccogliere ed esaminare i seguenti file di configurazioni:

- Tutti i file di configurazioni WLC correlati: show run-config e show running-config.
- La priorità di failover dell'AP è configurata?
- Per il WLC principale per AP (campo "Primary Cisco Switch [Name | IP Address]" in "AP Config")
- Per il WLC secondario per AP (campo "Secondary Cisco Switch [Name | IP Address]" in "AP Config")
- Per il WLC terziario per AP (campo "Tertiary Cisco Switch [Name | IP Address]" in "AP Config")
- I parametri di configurazione dell'AP corrispondente nel WLC: show ap config <AP name>.
- Le uniche modalità AP supportate per l'heartbeat veloce sono locale e h-reap (campo "Modalità AP").
- I parametri di configurazione dell'AP corrispondente nell'AP: show capwap client config.

Failover su WLC non previsto

- show sysinfo: il numero massimo di AP supportati dal WLC previsto.
- show ap summary: AP collegati al WLC previsto.
- show capwap client ha: se fast-heartbeat è abilitato, esaminare l'elenco di backup nell'AP.

Problema di trasporto

Se DHCP è abilitato per l'interfaccia AP Ethernet, ha recuperato un indirizzo IP? Utilizzare show interface FastEthernet0.

- ping <indirizzo IP> - Decide se l'AP e il WLC possono comunicare tra loro.

Protocolli CAPWAP

Comandi comuni di debug per AP e WLC:

- Debug per eventi e stato CAPWAP: debug capwap events enable/disable
- Debug per errori CAPWAP: debug capwap errors enable/disable
- Debug per dettagli CAPWAP: debug capwap detail enable/disable
- Debug per informazioni CAPWAP: debug capwap info message enable/disable
- Debug per payload CAPWAP: debug capwap payload enable/disable
- Debug per hexdump CAPWAP: debug capwap hexdump enable/disable

Comando di debug specifico per fast-heartbeat dell'AP:

- Debug per fast-heartbeat: show capwap client ha

  Nota: A volte è necessario l'output dell'analizzatore di rete, ad esempio wireshark.

Priorità degli AP

- Decidere se la priorità AP è abilitata—show run-conf (campo "AP Join Priority" in "Network Information")
- Decidere il numero massimo di access point supportati dal WLC—show sysinfo ("Numero massimo di access point supportati")
- Decidere il numero di access point che sono stati aggiunti al WLC: mostra riepilogo access point
- Esaminare la priorità di collegamento di ciascun AP: show ap summary (ultima colonna)

Problemi relativi a Transporter e CAPWAP

Consultare le sessioni corrispondenti nella sezione Failover dell'AP.

- show tech-support
- show run-config
- show running-config
- show ap config general <AP name>
- show capwap client config

Problemi relativi al controller H-REAP

H-REAP

Debug del controller:

- debug client <mac>

Debug dell'AP:

- debug lwapp reap mgmt
- debug dot11 mgmt msg
- debug dot11 mgmt int

Problemi relativi a CCKM per H-REAP

Debug del controller:

- debug cckm
- debug hreap cckm

Show/debug per AP:

- debug lwapp reap mgmt
- debug dot11 aaa manager key
- debug lwapp reap cckm
- debug dot11 mgmt msg
- show lwapp reap cckm

RADIUS locale per H-REAP

Debug del controller:

- debug hreap group
- debug hreap aaa

Show/debug per AP:

- debug lwapp reap
- debug lwapp client config
- show run

Media-Stream

- debug media-stream
- Ammissione: debug di ammissione dei client utili per il debug di problemi di negazione/eliminazione dei client.
- Evento: scarica gli aggiornamenti del client diretto IGMP/multimediale.
- RRC: aggiornamenti dei computer nello stato RRC.

debug bcast

- igmp: messaggi di richiesta/segnalazione di collegamento del client IGMP

Problemi relativi alla posizione

```
>show location ?

ap-detect      Display devices detected by specified AP
detail         Display detailed location information.
plm            Display Location's Path Loss Measurement(CCX S60) Configuration
statistics     Display Location Based System statistics.
summary        Display Location Based System summary information.
```

Problemi relativi alla memoria di sistema/memoria esaurita

Output di config e show da raccogliere

- show memory stat
- show buffers

- show process memory

  Nota: Se il flag "config memory monitor errors" è impostato su "disable", i dettagli relativi al danneggiamento della memoria possono essere caricati con i seguenti comandi:

- transfer upload datatype errorlog
- transfer upload filename memerrors.txt
- transfer upload start

Problemi relativi alla magliata

Esistono diversi punti di vulnerabilità (o presenza di bug):

- Controller
- AP in modalità magliata
- GUI/WLC

Indicazioni generali

- Individuate il punto di errore e isolate il componente fallito.
- Correlazione delle tracce dal controller, dai Mesh AP e anche dall'output visivo sulla CLI/GUI/WLC per trovare il punto di errore.
- In caso di problemi relativi ai pacchetti, raccogliere tracce Airopeek o Ethereal per confermare l'analisi preliminare.
- Analizzare il motivo dell'errore e il modo in cui il problema può essere riprodotto.
- Configurazione
- Attivare l'azione

Linee guida generali

Questa sezione ha lo scopo di fornire un numero sufficiente di puntatori per eseguire il debug di un bug correlato alla magliata e raccogliere informazioni pertinenti e utili per aiutare i sistemi di difesa a comprendere il bug in modo più efficiente. Dato che può essere impossibile individuare un bug a prima vista, questo documento è una serie di suggerimenti per il DT, non un libro di regole. Il DT ricorre alla discrezione per allegare i relativi debug in modo da contribuire allo studio efficiente e risolvere il bug il più rapidamente possibile.

Pacchetti sospetti mancanti

Raccogliere tracce Ethereal e Airopeek.

Serie di comandi debug

Questo è un insieme di comandi debug generici che possono essere utilizzati per ottenere informazioni sul sistema.

CLI show generale:

- show version
- show capwap client rcb
- show mesh status
- show mesh module adjacency

- show mesh channel [current]

CLI test mesh:

- test mesh adjacency: per comandi di test di adiacenza della magliata
- test mesh astools: per gli strumenti anti-blocco della magliata
- test mesh awpp: per comandi di test AWPP della magliata
- test mesh disattivato (test mesh disable) - per disattivare una feature
- attiva mesh test (test mesh enable) - per attivare una feature
- test mesh forwarding: per comandi di test di inoltro della magliata
- test mesh linktest: per test di collegamento della magliata
- test mesh mperf: per lo strumento di test della larghezza di banda della magliata

Problemi specifici

- Qualsiasi problema di connessione del collegamento
- debug mesh link
- show mesh adjacency (secondari/principali/tutti)

Radio:

- show controller d0, d1, ... (per tutti i problemi relativi alla radio)
- Tracce dall'aria (tra i nodi interessati)

Problemi relativi all'interfaccia (correlati al traffico dei dati):

- show int d0, d1, G0, G1, ...

Tracce Ethernet tra il controller e il Roof-top Access Point (RAP)

Inoltro:

- show mesh forwarding table
- debug mesh forwarding [table/packet]
- show mesh forwarding links
- show mesh forwarding port-state
- debug mesh forwarding port-filter

Indirizzo IP/DHCP:

- debug ip address
- show ip int bri
- show int bvi1
- show run int bvi 1
- show mesh forwarding port-state
- test mesh: disabilita il filtro porte e il router ping

Traffico IP e DHCP:

- debug ip udp
- debug ip icmp
- debug dhcp [detail]

Elenchi di esclusione:

- debug mesh adiacency exclusion - Osserva gli eventi che escludono gli elementi padre.

- test mesh adjacency exclusion clear: per azzerare i contatori degli elenchi di esclusione correnti e riniziare da capo.

Computer con stato di adiacenza:

- debug mesh adjacency event
- debug mesh adjacency state
- debug mesh adjacency timer

Comunicazione di adiacenza:

- debug mesh adjacency packet
- debug mesh adjacency message

Problemi relativi al collegamento di adiacenza:

- debug mesh adjacency channel
- debug mesh adjacency neighbor
- debug mesh adjacency parent

Modifiche al rapporto segnale-rumore (SNR):

- debug mesh adjacency snr

Dynamic Frequency Selection (DFS):

- debug mesh adjacency dfs

Mancata associazione del workgroup bridge (WGB):

- Raccogliere i debug dei client sul controller e sull'AP.
- Raccogliere le tracce dello sniffer Airopeek tra il WGB e l'AP principale in modalità magliata.
- Il client cablato dietro il WGB non può trasmettere il traffico.
- Ottenere lo stato del WGB principale sul controller.
- Raccogliere i debug sul controller, sull'AP in modalità magliata e su WGB.
- Raccogliere le tracce Ethereal tra l'AP principale in modalità magliata e il controller.

L'AP non può essere COLLEGATO:

- Raccogliere il messaggio di debug sul controller:
- debug capwap errors enable
- debug capwap events enable

Raccogliere il messaggio di debug sull'AP:

- debug capwap client event
- debug capwap client error

Per ulteriori informazioni, utilizzare questi debug aggiuntivi:

Debug del controller:

- debug capwap detail enable
- debug capwap info enable
- debug capwap payload enable
- debug capwap hexdump enable

Debug dell'AP:

- debug capwap client config
- debug capwap client detail
- debug capwap client fwd
- debug capwap client hexdump
- debug capwap client info
- debug capwap client payload
- debug capwap client reassembly

MostraComandi:

- show capwap client rcb: mostra la configurazione del blocco di controllo radio
- show capwap client config: mostra la configurazione radio da nvram

Comandi test:

- test mesh lwapp restart
- test mesh mode bridge/local
- test mesh role rap/map
- test mesh bgn xxxx
- test lwapp console cli
- test lwapp controller ip

Strumenti anti-blocco:

Comandi AP

```
debug mesh astools
event -- Event debugs
level -- Level of detail in debugs
packet -- packet related debugs
timer -- timer debugs
```

Controller

- debug mesh astools troubleshoot <MAC addr>: il MAC address su radio b/g dell'AP bloccato

Comandi show

- show mesh astools config: configurazione corrente
- show mesh astools stranded-ap-list: per stampare l'elenco degli AP bloccati rilevati

AP: nessun beacon ascoltato

- Accertarsi che almeno un access point adiacente sia collegato al controller e in grado di ascoltare l'access point bloccato.
- Mostrare cont d0 per determinare il canale corrente delle radio 11b in funzione.
- Raccogliere tutti i possibili debug pertinenti.

Strumento di misurazione della larghezza di banda Mperf:

- Comandi show
  ```
  show mesh mperf ?
  globals --- Print configuration used to spawn objects
  print [all/id] --- Print active connections
  ```
- Comandi debug
  ```
  debug mesh mperf ?
  bwreport -- Bandwidth output reports
  ```

```
fds -- Multiple connection state machine multiplexing
general -- All general debugs
jitter -- Jitter calculations
sockdata -- Socket data RX and TX
timer -- Timer related
```

Problemi con il client NTP e la configurazione temporale sul controller

- debug ntp packet enable
- debug ntp low enable
- debug ntp detail enable
- show time
- Acquisizione Ethereal sulla porta di gestione del controller

Problemi relativi ai componenti RF per i WLC

```
>debug airewave-director ?

all             Configures debug of all Airewave Director logs
channel         Configures debug of Airewave Director channel assignment protocol
error           Configures debug of Airewave Director error logs
detail          Configures debug of Airewave Director detail logs
group           Configures debug of Airewave Director grouping protocol
manager         Configures debug of Airewave Director manager
message         Configures debug of Airewave Director messages
packet          Configures debug of Airewave Director packets
power           Configures debug of Airewave Director power assignment protocol
radar           Configures debug of Airewave Director radar detection/avoidance protocol
plm             Configures debug of CCX S60 Power Measurement Loss messages
rf-change       Configures logging of Airewave Director rf changes
profile         Configures logging of Airewave Director profile events
```

Componente SNMP per WLC

```
>debug snmp ?

all             Configures debug of all SNMP messages.
agent           Configures debug of SNMP agent.
mib             Configures debug of SNMP MIB.
trap            Configures debug of SNMP traps.
engine          Configures debug of SNMP engine.
```

- Includere il comando del Protocollo SNMP (Simple Network Management Protocol) non riuscito.
- Se il WCS indica che SNMP non è riuscito, provare a eseguire il comando SNMP set/get da MG-soft o da qualsiasi altro gestore SNMP.
- Verificare se funziona dall'interfaccia utente o dalla CLI del controller.
- Allegare una schermata dell'interfaccia utente/CLI del controller.
- In caso di perdite di memoria o problemi della CPU, indicare da quanto tempo il sistema è attivo.
- Esaminare i debug SNMP per vedere se risulta qualcosa con evidenza.debug snmp mibs enable o debug snmp agent enabledebug snmp traps enable
- Eseguire la connessione dai debug precedenti.

Problemi di caricamento/download TFTP che includono upgrade/downgrade

```
>debug transfer tftp ?

disable        Disables debug.
enable         Enables debug.
```

Componente GUI Web per WLC

- Indicare il problema rilevato relativo al browser.
- Controllare se sono presenti problemi relativi a script Java. Se si usa Firefox, controllare la console degli errori. Allegare una schermata dell'errore di script Java. In Internet Explorer viene visualizzata una finestra popup. Per Firefox, allegare la finestra della console degli errori.
- Se la configurazione ha esito negativo, verificare con la CLI. Includere l'output della CLI.
- Allegare la schermata al bug.
- Indicare il controller e la piattaforma AP.
- Se si verifica un arresto anomalo nell'attività emweb, osservare la traccia dello stack di arresto anomalo. Se la traccia dello stack indica la CLI, non utilizzare questo componente.

Problemi relativi alla configurazione dell'autenticazione Web e all'autenticazione

- debug pm ssh-appgw enable
- debug pm ssh-tcp enable

WLC-Webauth-Template

Informazioni di base

Determinare la topologia della rete al momento dell'esecuzione dell'autenticazione Web.

- Èuna configurazione guest o un'associazione normale in un singolo WLC oppure avviene dopo l'esecuzione dell'autenticazione Web in roaming?
- Che tipo di autenticazione Web è configurata (interna, esterna, personalizzata o web-passthru)?
- Qual è la pagina di accesso utilizzata?
- Scaricare il pacchetto dell'autenticazione Web e fornirlo.
- Secure-web è abilitato? In caso affermativo, disabilitarlo e vedere se l'autenticazione Web funziona.

Comandi show:

- show client details <mac>
- show wlan <wlanid>
- show rules show custom-web

Debug

- debug emweb server enable
- debug pm ssh-tcp enable

- debug pm ssh-engine enable packet <>
- debug pm ssh-appgw enable

debug client <mac>

> **Nota:** Eseguire questo debug se la pagina non è visualizzata. Accertarsi di raccogliere questo debug separatamente.

- debug mobility handoff enable

> **Nota:** Eseguire questo debug se webauth non funziona dopo il roaming.

Sniffer

- Porta WLC DS: utile per un problema di autenticazione RADIUS.Porta WLC AP: utile se i pacchetti http vengono eliminati tra il WLC e l'APVia etere, se il punto di accesso scarta i pacchetti

Problemi e miglioramenti relativi alla configurazione XML del controller

Convalida XML

- I messaggi di errore di convalida XML, ad esempio `Validation per il nodo ptr_apfCfgData.apfVAPIDData.apfVapSecurity.<qualsiasi dato di configurazione>`, vengono osservati durante l'avvio del sistema.
- L'intero messaggio di errore di convalida XML
- la procedura CLI o GUI per configurare le WLAN prima dell'avvio del sistema
- il file di configurazione CLI o XML generato e salvato in TFTP prima dell'avvio del sistema
- show invalid-config

Canale di diagnostica

- debug client <client mac>
- debug ccxdiag all enable

Allocazione dinamica del canale

- debug airwave-director channel enable
- debug airwave-director radar enable

TACACS+

- debug aaa tacacs enable
- show tacacs summary

WLC-Multicast-Guide

Informazioni di base

- Topologia della rete
- Assicurarsi che l'indirizzo del flusso multicast non sia l'indirizzo riservato IANA per l'applicazione in uso.
- Indirizzi multicast utilizzati
- La velocità di flusso multicast e la dimensione del pacchetto
- Assicurarsi che l'indirizzo multicast del gruppo di AP configurato non sia uguale all'indirizzo del flusso multicast.
- Il modello WLC (2106, 4404, 4402, WiSM...)
- Il modello AP (1131, 1232, 1242, 1250...)
- Radio utilizzata dal client
- MAC address del client

Informazioni sul WLC (tutte le varianti)

Dump di:

- show interface summarydebug bcast * enable
- show network summary
- show network multicast mgid summary
- show network multicast mgid detail <mgid>
- Per la versione G e versioni successive: show wlan apgroups
- Per TALWAR/2106 con il nuovo codice FP:Se lo snooping IGMP è abilitato, eseguire debug fastpath cfgtool --mcast4db.dump debug fastpath cfgtool --mcast2db.dumpSe lo snooping IGMP è disabilitato, eseguire debug fastpath cfgtool --mcast2db.dumpSe Multicast-Unicast è abilitato, eseguire debug fastpath cfgtool --mcastrgdb.dump

Informazioni sull'AP (tutte le varianti)

Dump di:

- show lwapp mcastshow lwapp mcast mgid allshow lwapp mcast mgid id <mgid>show lwapp client traffic: quattro volte con un intervallo di un minuto tra ognuna

Debug radio:

1. La velocità di overrun Ethernet
2. La velocità di trasmissione radio
3. La velocità di eliminazione radio
4. Modalità di risparmio energia del set di servizi di base (BSS)
5. La velocità di ricezione Ethernet totale
6. La velocità di ricezione multicast Ethernet

Per #1, eseguire **il comando show int g0 | inc** overruncommand periodicamente.

Per #2, #3 e #4, eseguire **il show cont d0 |** accodare periodicamente il comando. Osservare i conteggi di invio/eliminazione per ogni coda.

Inoltre, per #3, eseguire **il comando show int d0 | inc output** dropcommand periodicamente.

Per #5, eseguire **il comando show cont g0 | incl. comando** conteggio **RX** periodicamente.

Per #6, eseguire **il comando show cont g0 | inc** multicast comando periodicamente. La prima riga mostra il multicast di ricezione/la trasmissione.

Per ottenere le velocità dei pacchetti, eseguire un comando ogni 10 secondi e dividere la differenza per 10. Se molti pacchetti vengono inviati alla coda Mcast (per un BSS), il BSS è in modalità di risparmio energetico. La velocità massima dei pacchetti multicast per un BSS in risparmio energetico è relativamente bassa. Questo è un problema noto.

Informazioni sullo switch

Controllare la versione dello switch con **il** comando **show** version. Lo switch può avere la versione "base ip avanzata" (ad esempio, software Cisco IOS, software C3750 [C3750-ADVIPSERVICESK9-M], versione 12.2(40)SE, SOFTWARE RELEASE (fc3)). [immagine: c3750-advipservicesk9-mz.122-40.SE.bin]). La versione "ip base" presenta un problema di routing del traffico multicast tra VLAN

Alcuni debug:

- Controllare se il routing multicast è abilitato. ("show run" può includere "ip multicast-routing distribuito")
- Controllare se la configurazione "ip pim sparse-dense-mode" è stata aggiunta alla VLAN configurata.
- show ip igmp group

Acquisizioni di sniffer

- Interfaccia DS della WLAN
- Interfaccia Mgmt del WLC
- Ap-Mgr a cui è connesso l'AP (richiesto solo quando mcast src è wireless)
- Interfaccia Eth dell'AP
- In diretta

Analisi delle acquisizioni di sniffer

L'origine multicast è su lato cablato

- Controllare se i pacchetti raggiungono il WLC nell'interfaccia DS.
- Controllare se il pacchetto multicast incapsulato LWAPP viene inviato sull'interfaccia mgmt. Il pacchetto deve avere:outer ip dst addr = indirizzo multicast del gruppo di AP configuratoudp dst port = 12224
- Controllare se il pacchetto visualizzato in "b" è visibile nell'interfaccia eth dell'AP.
- Controllare se il pacchetto del flusso mcast è visibile in diretta.

L'origine multicast è su lato wireless

- Controllare se i pacchetti incapsulati LWAPP vengono ricevuti nell'interfaccia ap-mgr. In questo caso, LWAPP è unicast.
- Controllare se un pacchetto multicast viene inviato dall'interfaccia DS.
- Controllare se il pacchetto multicast incapsulato LWAPP viene inviato sull'interfaccia mgmt. Il pacchetto deve avere:outer ip dst addr = indirizzo multicast del gruppo di AP configuratoudp dst port = 12224
- Controllare se il pacchetto visualizzato in "b" è visibile nell'interfaccia eth dell'AP.
- Controllare se il pacchetto del flusso mcast è visibile in diretta.

Verifica della configurazione dello switch per WiSM

- Quando si utilizza un modulo di servizi wireless (WiSM), verificare se si verifica lo stesso problema indicato nella sezione successiva a questo.
- ID bug Cisco CSCsj48453 - CAT6k non inoltra il traffico multicast a WISM in modalità L3.
- Sintomo: il traffico multicast non scorre da un host cablato a un host wireless attraverso la scheda WiSM in modalità L3, ad esempio, quando entrambi gli host si trovano in VLAN diverse. Solo il primo pacchetto viene inviato correttamente. In seguito, il traffico si arresta.
- Condizioni: il traffico si arresta solo quando la modalità di replica multicast è in uscita.
- Soluzione. Per ovviare al problema, è possibile modificare la modalità di replica multicast in entrata con il comando **themls ip ip multicast replication-mode** in entrata. Il traffico fluisce correttamente nella modalità di ingresso. Verificare che venga utilizzato lo **stesso comando mls ip multicast** capabilities.

Ulteriore descrizione del problema: il problema si verifica con CAT6k e un WiSM. Il traffico multicast che passa dall'host wireless all'host cablato funziona correttamente, anche in L3. Inoltre, il traffico multicast che passa dall'host cablato all'host wireless attraverso la scheda WiSM funziona correttamente in modalità L2.

WLC-QoS-Guide

Debug minimi

- Ottenere il comando "show run-config" da tutti gli switch nel gruppo di mobilità.
- Quando si verifica il problema, acquisire questi debug:debug aaa all enabledebug pem state enabledebug pem events enabledebug mobility handoff enabledebug dot11 mobile enabledebug dot11 state enable
- Ottenere una traccia Airopeek o AirMagnet vicino all'access point, al telefono o al ricevitore problematico.
- Ottenere un'acquisizione Ethereal o Etherpeek della porta DS dello switch, dello switch a monte dell'AP e delle priorità vocali SpectraLink (SVP).

Debug del controllo delle chiamate (classificazione SIP)

Domanda

- Si tratta di un client SIP (Session Initiation Protocol)?
- Quale server IP PBX\sip viene utilizzato?
- Dimostra che è registrato su quel dato server SIP?
- Lo switch 7921 funziona come previsto e solo i client SIP hanno un problema?

Informazioni sul WLC

- show wlan summary [wlan #]
- debug call-control all
- debug call-control events
- show call-control errors
- show call-control calls

Informazioni sull'AP

- debug dot11 cc details
- debug dot11 cc errors

- debug dot11 cc events
- show lwapp client call-info mac (MAC address del client in questione)

Controllo di ammissione basato sul caricamento e metriche relative alla voce

Domande a cui rispondere

- Il problema si verifica con entrambe le radio "a" e "b"?
- Qual è il valore di utilizzo del canale quando la chiamata viene rifiutata?
- Si verifica solo con telefoni 7921 o anche con altri telefoni? In caso affermativo, quali sono gli altri telefoni? In caso contrario, è possibile provare su un altro telefono TSPEC?
- Si verifica con AP 11n o AP standard?
- Utilizzate la mobilità tra controller?
- Il telefono TSPEC è in grado di effettuarla?
- Fa la UAPSD?
- Èriproducibile su piattaforme 2006 o 4100?
- Èun ambiente protetto?
- Si è verificata una condizione speciale per cui la chiamata è stata rifiutata?

Comandi debug e show su WLC per LBCAC

- debug cac all enable
- show 802.11a/b/g
- show wlan <wlan id>
- show ap stats 802.11a/b/g <ap-name>
- show ap auto-rf 802.11a/b/g <ap-name>

Eseguire il debug dell'AP per LBCAC

- debug dot11 cac unit
- debug dot11 cac metrics
- debug dot11 cac events

Metriche relative alla voce

- Acquisizioni over-the-air e di sniffer cablato
- Verificare se il traffico UP6 viene generato in modo continuo.
- Accertarsi che la WLAN disponga del profilo QoS e della policy Wi-Fi Multimedia (WMM) giusti.
- La maggior parte delle domande poste per LBCAC sono valide anche per le metriche relative alla voce.

Comandi debug e show sul WLC per le metriche relative alla voce:

- show 802.11a/b/g o show wlan <wlan id>
- show ap stats 802.11a/b/g <ap-name>
- show ap stats 802.11a/b/g <ap-name> tsm
- show client tsm 802.11a/b/g <client-mac> <AP mac>
- debug iapp packet enable o debug iapp error enable
- debug iapp all enable o debug client <client mac>

Debug sull'AP per le metriche relative alla voce:

- debug dot11 tsm
- debug lwapp client voice-metrics

WLC-License-Guide

Debug da raccogliere sul controller

- Output della console
- msglog

Problemi del protocollo ARP

Debug da raccogliere sul controller

- debug arp all enable

Problemi di rete

Debug da raccogliere sul controller

- debug packet logging enable
- dump-low-level-debugs

Altri

Debug da raccogliere sul controller

- dump-low-level-debugs
- msglog

Problemi relativi agli access point

IAPP

- show wgb summary
- show wgb detail <wgb mac>

Problemi di associazione WGB

- debug dot11 mobile enable
- debug dot11 state enable
- debug pem events enable
- debug pem state enable
- debug iapp all enable

WGB o il client cablato non riceve l'indirizzo DHCP

- debug dhcp packet enable
- debug dhcp message enable

WGB o il client cablato utilizza l'indirizzo IP statico ma l'indirizzo IP non viene visualizzato sul controller

- debug dot11 mobile enable
- debug dot11 state enable

Nome utente e password dell'AP

Debug da raccogliere sull'AP

- debug lwapp client config

Acquisizioni da effettuare

- Non applicabile.

Output di config e show da raccogliere

- config ap mgmtuser

Problemi di connessione del client

Debug del client

- debug client xx.xx.xx.xx.xx.xx

Il controller non accetta la richiesta di associazione

Acquisizione pacchetti

- Acquisizione Airopeek sul canale da cui è impostato l'AP. Si consiglia di evitare l'applicazione di filtri perché i pacchetti beacon e di richiesta/risposta possono non essere rilevati. Assicurarsi di acquisire l'evento quando la connessione è terminata.
- Nel caso in cui il client non si connetta, acquisire l'intero evento dalla richiesta di prob fino al termine della sessione (ad esempio, viene inviata la risposta predefinita e la risposta di associazione con il codice di stato diverso da 0).
- Fornire il client e i MAC address dell'AP.

  Nota: Il MACi AP è un Radio MAC di base + WLAN-ID.

Output di config e show da raccogliere sul controller

- show sysinfo: i dettagli della versione del WLC
- show wlan x: su WLC per la WLAN interessata
- show run-config: del WLC
- show debug
- show msglog

- show tech-support: del WLC (utile, ma non necessario)

Dettagli client

- Hardware client: dettagli del software supplicant come relativi versione e nome (ad esempio, ADU o Odyssey)
- Sistema operativo client: se si tratta di Windows, fornire la configurazione del sistema client, selezionare **Programmi > Accessori > Utilità di sistema > System Information** (Informazioni di sistema).

Dettagli server RADIUS

Specificare il tipo di server RADIUS (SBR, Cisco ACS, Linux e così via) e la configurazione, se applicabile.

Il client non risponde alle richieste EAP

Consultare la sezione Il controller non accetta la richiesta di associazione.

L'autenticazione EAP non viene portata a termine

Consultare la sezione Il controller non accetta la richiesta di associazione.

Richiesta DHCP dal client non riuscita

Consultare la sezione Il controller non accetta la richiesta di associazione.

EAPOL Exchange non passa

Consultare la sezione Il controller non accetta la richiesta di associazione.

Roaming CCKM non riuscito

Debug da raccogliere

La maggior parte dei debug è uguale alla sezione precedente, Problema di connessione del client. Tuttavia, questi nuovi debug consentono di eseguire in modo più efficace il debug CCKM. Questo comando debug è disponibile a partire dalla versione 5.0:

- debug cckm enable
- show pmk-cache <client mac>: sul controller di destinazione
- show client details <client mac>: quando il client è connesso a un AP obsoleto
- debug cckm enable

> **Nota:** Dopo aver eseguito il comando **debug client<mac client>**, i debug o qualsiasi altro comando di debug devono essere attivati. Infatti, il comando **debug client<mac>**disabilita tutti i debug precedenti.

Acquisizioni da effettuare

Assicurarsi di effettuare l'acquisizione sul canale in cui si trova l'AP di destinazione. Ad esempio, se si desidera acquisire tutti i pacchetti di gestione tra il client e l'AP di destinazione. Per ulteriori

informazioni, vedere la sezione Il controller non ama la richiesta di associazione.

Output di config e show da raccogliere sul controller

Consultare la sezione Il controller non accetta la richiesta di associazione ed eseguire questi comandi:

- show pmk-cache <client mac>: sul controller di destinazione
- show client details <client mac>: quando il client è connesso a un AP obsoleto

Dettagli client

Consultare la sezione Il controller non accetta la richiesta di associazione.

Memorizzazione nella cache PMKID non riuscita

Controllare se il client supporta OKC (Opportunistic Key Caching).

> **Nota:** OKC non è uguale a PKC (Proactive Key Cache) come specificato in 802.11I. Il WLC supporta solo OKC.

Debug da raccogliere

Consultare la sezione Il controller non accetta la richiesta di associazione.

Acquisizioni da effettuare

Assicurarsi di effettuare l'acquisizione sul canale in cui si trova l'AP di destinazione. Ad esempio, se si desidera acquisire tutti i pacchetti di gestione tra il client e l'AP di destinazione.

Consultare la sezione Il controller non accetta la richiesta di associazione.

Output di config e show da raccogliere sul controller

Vedere la sezione Il controller non ama la richiesta di associazione ed eseguire questi comandi:

- show pmk-cache <client mac>: sul controller di destinazione
- show client details <client mac>: quando il client è connesso a un AP obsoleto

Dettagli client

Consultare la sezione Il controller non accetta la richiesta di associazione.

Problemi di riautenticazione

Debug da raccogliere

Consultare la sezione Il controller non accetta la richiesta di associazione.

Acquisizioni da effettuare

Non applicabile.

Output di config e show da raccogliere sul controller

Consultare la sezione Il controller non accetta la richiesta di associazione ed eseguire questi comandi:

- show radius summary
- show client details <client mac>
- show pmk-cache <client mac>

Dettagli client

Consultare la sezione Il controller non accetta la richiesta di associazione.

Il roaming 802.11R (Fast Transition) non funziona

Debug da raccogliere

- debug client <client mac>
- debug ft events enable
- debug ft keys enable

> **Nota:** Dopo aver eseguito il comando **debug client<mac client>**, i debug o qualsiasi altro comando di debug devono essere attivati. Infatti, il comando **debug client<mac>**disabilita tutti i debug precedenti.

Acquisizioni da effettuare

Quando si viaggia in aereo, raccogliere la cattura di Airopeek sul canale in cui si trova il punto di accesso di destinazione. Ad esempio, se si desidera acquisire tutti i frame di richiesta/risposta FT di autenticazione 802.11 e la richiesta/risposta di riassociazione.

Quando si effettua il roaming sul DS, raccogliere l'acquisizione di Airopeek sul canale in cui si trova l'access point di origine. Ad esempio, se si desidera acquisire i frame di richiesta/risposta di riassociazione. Si desidera anche acquisire la richiesta/risposta FT del frame di azione sul canale dell'AP di origine.

> **Nota:** Si consiglia di mantenere gli access point di origine e destinazione nello stesso canale per eseguire il debug del problema di roaming 802.11R. Ciò consente di acquisire la richiesta/risposta FT e la richiesta/risposta di riassociazione in un singolo file di acquisizione.

Output di config e show da raccogliere sul controller

Consultare la sezione Il controller non accetta la richiesta di associazione ed eseguire questi comandi:

- show pmk-cache <client mac>: sul controller di destinazione e di origine
- show client details <client mac>: quando il client è connesso a un AP obsoleto
- show mobility summary: per ottenere l'ID dominio di mobilità

Dettagli client

Attualmente, solo il WGB è il client 802.11R noto. Per ulteriori informazioni, consultare la sezione

Il controller non accetta la richiesta di associazione.

Mobilità tra controller

Debug da raccogliere

- debug client <client mac>: su entrambi i WLC
- debug mobility handoff enable: su entrambi i WLC (ricordarsi l'ordine: abilitare sempre prima il debug client.)
- debug pem state enable
- Eping <ip>
- Mping <ip>

Se il percorso di controllo della mobilità o i dati sono inattivi, attivare il comando "debug mobility keepalive enable" su entrambi gli switch (annotare la versione software su entrambi i controller).

Se ARP non funziona, attivare il comando "debug arp all enable" su entrambi gli switch.

Se il protocollo DHCP non funziona, attivare le opzioni "debug dhcp message enable" e "debug dhcp packet enable" su entrambi gli switch.

Se è coinvolto IPSec: debug pm sa-export enable, debug pm sa-import enable.

Se il client si connette dopo un certo periodo di tempo, mostrare il tempo impiegato.

Acquisizioni da effettuare

Acquisizione tramite roaming, ad esempio CCKM, PMKID o TGR.

Output di config e show da raccogliere

Consultare la sezione Il controller non accetta la richiesta di associazione ed eseguire questi comandi:

- show pmk-cache <client mac>: sul controller di destinazione
- show client details <client mac>: quando il client è connesso a un AP obsoleto
- show mobility summary: su entrambi i WLC

Dettagli client

Verificare il tipo di roaming specifico, come CCKM, PMKID o TGR.

Disabilita debug

Per disabilitare tutti i messaggi di debug, usare **il comando debug disable-all**.

In alternativa, è possibile disabilitare i debug specifici con il comando debugcommand e la parola chiave disable:

```
debug capwap events disable
```

Informazioni correlate

- Documentazione e supporto tecnico
- Informazioni sui debug wireless e sulla raccolta di registri sui controller LAN wireless 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).