Fehlerbehebung bei AireOS Wireless LAN Controllern

Inhalt

Einleitung

In diesem Dokument wird die Verwendung der Befehle **debug** und **show** zur Fehlerbehebung bei Wireless LAN Controllern (WLCs) beschrieben.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps von Cisco zu Konventionen).

Probleme mit Controller-Komponenten

IDS-Signaturen

- debug wips sig enable

NAC

- debug nac events enable
- debug nac packets enable

OEAP

Controller Befehle anzeigen

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

AP-Seitenansicht/Fehlerbehebung

- show logging
- 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

Regelbasierte Klassifizierung von nicht autorisierten Benutzern

Zu sammelnde Debugs

- debug dot11 rogue rule enable

Aufnahmen

Nicht zutreffend.

Zu erfassende Ausgabe konfigurieren und anzeigen

- show rogue rule summary
- show rogue rule detail <Regel>
- show rogue ap detail <rogue-mac> (wenn ein bestimmtes unberechtigtes Gerät falsch klassifiziert wurde)

Blockierung nicht autorisierter APs

Stellen Sie sicher, dass im Netzwerk ein DHCP-Server konfiguriert ist, den der nicht autorisierte Access Point (AP) bei Verwendung der statischen IP-Adressierung verwenden kann.

Zu sammelnde Debugs

- debug dot11 rogue enable

Aufnahmen

Airopeek-Spur auf dem unberechtigten Kanal.

> **Anmerkung:** Achten Sie auf getrennte Frames.

Zu erfassende Ausgabe konfigurieren und anzeigen

- show rogue ap detailed <contained rogue-mac>
- show ap config 802.11b/a <Name aus dem vorherigen Befehl>

IDS-Signatur

Vergewissern Sie sich, dass ein DHCP-Server im Netzwerk konfiguriert ist, den der nicht autorisierte Access Point bei Verwendung der statischen IP-Adressierung verwenden kann.

Zu sammelnde Debugs

- debug wips sig enable

Aufnahmen

Airopeek-Erfassung an der Kanalsignatur erkannt.

Zu erfassende Ausgabe debuggen und anzeigen

In Software vor Version 5.2 kann LWAPP anstelle von CAPWAP für folgende Befehle verwendet werden:

- **show capwap ids sig dump** - Dumps Signaturen und Signaturerkennungs-Trefferzähler, die die MAC-Adresse mit den größten Treffern enthalten. Enthält außerdem den aktuellen Status der IDS-Paketverfolgung.
- **show capwap ids rogue containment <slot#> chan**- Zeigt die aktuelle Liste der Anforderungen an die Eindämmung nicht autorisierter APs an. Containment-Anforderungen werden nach Kanal gruppiert.
- **show capwap ids rogue containment <slot#> rad**- Zeigt die aktuelle Liste der Anforderungen an die Eindämmung nicht autorisierter APs an. Diese Liste entspricht der Liste der vom Controller empfangenen Anforderungen.

- **debug capwap ids sig**- Aktiviert Debugging für IDS Signature and Containment Detection.

- **test capwap ids trace match <Nachrichtentyp-Name>**- Verfolgt alle Pakete, die vom IDS-Signaturerkennungsmodul von Nachrichtentyp=<Nachrichtentyp-Name> empfangen wurden; <Nachrichtentyp-Name> = FF zum Verfolgen aller Nachrichtentypen. Signature Debugs in Abschnitt 8.2.1 müssen aktiviert werden, damit die verfolgten Pakete angezeigt werden.
- **test capwap ids trace rcv <type-name>**- Ablaufverfolgungen für alle Pakete, die mit den derzeit installierten Signaturen für das IDS-Signaturerkennungsmodul von message type=<message type-name> übereinstimmen; <Nachrichtentyp-Name> = FF, um alle Nachrichtentypen zu verfolgen, die mit einer Signatur übereinstimmen. Signature Debugs in Abschnitt 8.2.1 müssen aktiviert werden, damit die verfolgten Pakete angezeigt werden.

RLDP

Zu sammelnde Debugs

Auf dem WLC:

- debug dot11 rldp enable

Auf dem AP:

- debug lwapp client mgmt

Aufnahmen

Airopeek-Erfassung auf dem unberechtigten Kanal.

Zu erfassende Ausgabe konfigurieren und anzeigen

- config rogue ap rldp initiieren <rogue-mac>

Diagnosekanal

Zu sammelnde Debugs

- debug client <client mac>

- debug ccxdiag all enable

Aufnahmen

Airopeek-Erfassung auf dem Kanal, von dem der AP festgelegt wird. Es wird empfohlen, die Filterung zu vermeiden, da Beacon- und Probe-REQ/REP-Pakete verpasst werden können.

Zu erfassende Ausgabe konfigurieren und anzeigen

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

Client-Details

- Client-Hardware
- Zusätzliche Softwaredetails wie Softwareversion, Softwarename (z. B. Aironet Desktop Utility [ADU] oder Odyssey) und Treiberversion bei ADU
- Client-Betriebssystem

Inter-Controller-Mobilität

Zu sammelnde Debugs

- debug client <client mac> auf beiden WLCs
- debug mobility handoff enabled on both WLCs (Remember the order and always enable the debug client first.)
- Debug pem state enable

- Wenn der Mobility Control-Pfad oder die Daten aktiv sind, aktivieren Sie "debug mobility keepalive enable" auf beiden Switches (erinnern Sie sich an die Softwareversion auf beiden Controllern).
- Wenn das Address Resolution Protocol (ARP) nicht funktioniert, aktivieren Sie die Option "debug arp all enable" auf beiden Switches.
- Wenn DHCP nicht funktioniert, aktivieren Sie auf beiden Switches "debug dhcp message enable" und "debug dhcp packet enable".
- Wenn IPSec beteiligt ist: debug pm sa-export enable, debug pm sa-import enable.
- Wenn der Client nach einer Weile eine Verbindung herstellt, wie lange es gedauert hat.

Aufnahmen

Erfassung durch den Roaming-Typ, z. B. CCKM, PMKID oder TGR.

Zu erfassende Ausgabe konfigurieren und anzeigen

Identisch mit dem Problem mit der Client-Verbindung und mit den folgenden:

- show pmk-cache <Client-Mac> (auf dem Ziel-Controller)
- show client details <client mac> (when client is connected on old AP)
- Mobilitätsübersicht anzeigen (auf beiden WLCs)

Client-Details

Identisch mit einem bestimmten Roaming-Typ, z. B. CCKM, PMKID oder TGR

Honeypot

Zu sammelnde Debugs

Nicht zutreffend.

Aufnahmen

Erfassen Sie die Airopeek-Spur auf dem Kanal, auf dem die Trap empfangen wird, um zu bestätigen, dass das unberechtigte Gerät die Cisco SSID verwendet.

Zu erfassende Ausgabe konfigurieren und anzeigen

- show traplog

AirMagnet-Integration

Zu sammelnde Debugs

Auf dem WLC bei NMSP-bezogenen Problemen:

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

Bei CAPWAP-bezogenen Problemen:

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

Informationen zu fehlerhaften Alarmen/Geräteberichten:

- debug wips all enable

Auf dem AP:

- debug capwap am event
- debug capwap am error

Aufnahmen

- Airopeek-Erfassung des Angriffs

- Ethereal-Erfassung der Berichte (als Datenpaket gesendet)

Zu erfassende Ausgabe konfigurieren und anzeigen

Auf dem AP:

- show capwap am stats
- show capwap am buffer [einige Male ausführen]
- show capwap am policy [alarm-id]
- show capwap am alarm [alarm-id]

Lokale Authentifizierung

Vor dem Protokollieren eines Fehlers zu überprüfende Elemente

Stellen Sie sicher, dass der Client eine Verbindung zum WLAN herstellen kann. Wenn der Client dies nicht kann, liegt das Problem auf der dot1x-Ebene. Wenn Zertifikate verwendet werden, stellen Sie sicher, dass Geräte und Zertifizierungsstellenzertifikate auf dem WLC installiert sind. Stellen Sie außerdem sicher, dass Sie in der Konfiguration für die lokale Authentifizierung den richtigen Zertifikataussteller ausgewählt haben, um den richtigen Zertifikatsatz auf dem WLC auszuwählen.

Wenn die lokale Datenbank für Benutzeranmeldeinformationen verwendet wird, überprüfen Sie, ob der Benutzername in der Datenbank vorhanden ist. Wenn das Lightweight Directory Access Protocol (LDAP) verwendet wird, finden Sie weitere Informationen zum Debuggen im Abschnitt LDAP debugging.

Zu sammelnde Debugs

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

Zu erfassende Ausgabe konfigurieren und anzeigen

- show local-auth config
- show local-auth statistics
- show local-auth Certificates (wenn eine Extensible Authentication Protocol [EAP]-Methode mit Zertifikaten verwendet wird)

Client-Details

Der Clienttyp und die EAP-Konfigurationsdetails zeigen, welche Methode ausgewählt ist und welche Parameter für diese Methode auf dem Client festgelegt sind. Auch der Text einer Fehlermeldung, die auf dem Client angezeigt wird.

Controller-Fehlersuche

- debug pm pki enable: Details zur Zertifikatsvalidierung.
- debug aaa events enable - Diese Option ist hilfreich, wenn Autorisierungslistenprobleme auftreten.
- show certificate lsc summary: Für jede LSC-bezogene Zusammenfassung

Allgemeine AAA-Authentifizierung

Diese Debugging-Optionen sind hilfreich beim Debuggen von RADIUS-Authentifizierungs-, Autorisierungs- oder Kontoproblemen:

Zu sammelnde Debugs

- debug client <client mac>: Zeigt an, wie bürokratiebezogene Attribute wie session-timeout und action-type angewendet werden.
- debug aaa events enable - Hilft bei der Fehlerbehebung, wie unterschiedliche AAA-Server für Authentifizierung, Autorisierung und Konto verwendet werden.
- debug aaa packet enable: Hilft bei der Fehlerbehebung, wenn verschiedene AAA-Attribute empfangen und angewendet werden.

Aufnahmen

Eine kabelgebundene Erfassung kann zwischen dem Controller und dem RADIUS-Server erfasst werden, wenn die früheren Fehlerbehebungen das Problem nicht erkennen lassen.

Zu erfassende Ausgabe konfigurieren und anzeigen

Identisch mit dem Problem der Clientverbindung und mit:

- show radius summary

Client-Details

Identisch mit Problem mit der Clientverbindung.

TACACS+

Zu sammelnde Debugs

- debug aaa tacacs enable (bei WLC Protokoll auf dem ACS-/RADIUS-Server für Konto sammeln)
- debug aaa events
- debug aaa detail
- debug dot11 mobile
- debug dot11 state
- debug pem events
- debug pem state

Aufnahmen

- Eine kabelgebundene Erfassung kann zwischen dem Controller und dem RADIUS-Server erfasst werden, wenn die früheren Fehlerbehebungen das Problem nicht erkennen lassen.

Zu erfassende Ausgabe konfigurieren und anzeigen

- show tacacs summary
- Problem mit Autorisierungsänderung (CoA) und Verbindungspaket (PD) - RFC 3576
- show radius summary

LDAP

Vor dem Protokollieren eines Fehlers zu überprüfende Elemente

Stellen Sie sicher, dass der LDAP-Server vom WLC aus einen Ping-Befehl empfangen kann.

Wenn Sie die Active Directory- und die lokale EAP-Authentifizierung verwenden, werden diese EAP-Methoden nicht unterstützt:

- SPRUNG
- EAP-FAST MSCHAPv2
- PEAP MSCHAPv2

Dies liegt daran, dass Active Directory kein unverschlüsseltes Kennwort zurückgeben kann, das für die MSCHAPv2-Authentifizierung verwendet werden kann.

Zu sammelnde Debugs

- debug aaa ldap enable

Wenn das Problem auftritt, wenn Sie LDAP mit lokaler Authentifizierung verwenden, finden Sie weitere Debugging-Informationen im Abschnitt Lokale Authentifizierung.

Zu erfassende Ausgabe konfigurieren und anzeigen

- show ldap summary
- show ldap <Server-Nr.>
- show ldap statistics
- Zeigt Statistiken zur lokalen Authentifizierung (wenn das Problem auftritt, wenn es mit LDAP mit lokaler EAP-Authentifizierung verwendet wird)

Client Management Frame Protection (MFP)

Für alle Probleme

- debug wps mfp client
- show wps mfp summary

Zu erfassende Ausgabe konfigurieren und anzeigen

- show wps mfp statistics

Konfigurationsprobleme

Controller-Debugging:

- debug wps mfp lwapp

- debug lwapp mfp (auf Aironet APs)

Kunde verbindet nicht

Controller-Debugging:

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

Ausgabe für Erfassung konfigurieren und anzeigen:

- show msglog
- show client detail

Zusätzliche 1130/1240 AP-Fehlermeldungen, wenn der Client keine Verbindung herstellt

- debug dot11 mgmt msg
- debug dot11 aaa manager all (for H-REAP standalone mode)

Aironet AP debuggt, wenn Client im H-REAP-Standalone-Modus keine Verbindung herstellt

- 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

Mobilität

Controller-Debugs

- debug wps mfp mm enable
- debug mobility directory

Zu erfassende Ausgabe konfigurieren und anzeigen

- show mobility summary
- show mobility statistics

Berichtsprobleme

Controller-Debugs

- debug wps mfp report

Zu erfassende Ausgabe konfigurieren und anzeigen

- show wps mfp statistics

  Anmerkung: Dieser muss unmittelbar nach der Fehlergenerierung aufgerufen werden.

FIPS-bezogene Probleme

Wird der Controller in den FIPS-Modus (Federal Information Processing Standard) versetzt, können nur zugelassene Verschlüsselungsfunktionen verwendet werden. Daher müssen Sie das SSL sperren, um den TLS_RSA-Authentifizierungsalgorithmus mit AES-Verschlüsselung zu verwenden.

Startmenü kann nicht geöffnet werden

Dies ist eine Funktion für FIPS. Die Funktion wird mit dem folgenden Befehl aktiviert:

- config switchconfig boot-break disable

Neues Image kann nicht heruntergeladen werden

- Dies ist eine Funktion für FIPS. Die Übertragung ist deaktiviert, wenn die Unterbrechung des Bootvorgangs deaktiviert ist.

Wireless-Client verwendet Local Authenticator mit EAP-TLS, EAP-FAST und PEAP

Zu sammelnde Debugs

Je nach Kommunikationsschwierigkeiten können die folgenden Debug-Funktionen aktiviert werden:

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

Aufnahmen

Sniffer-Trace zwischen dem WLC und dem Gerät mit dem Problem.

> **Anmerkung:** Der WLC kann mit der Kommunikation beginnen, sobald der entsprechende Service startet. Es wird empfohlen, den Sniffer zu starten, bevor der WLC hochgefahren wird.

Zu erfassende Ausgabe konfigurieren und anzeigen

- show switchconfig

512 WLANs/AP-Gruppen

512 WLANs

Ein 512-WLAN-Fehler tritt auf, wenn der Client eine Verbindung zu einem Access Point der Standardgruppe herstellen kann, aber keine Verbindung zu einem Access Point herstellen kann, der auf eine benutzerdefinierte Access Point-Gruppe festgelegt ist.

Ausgabe anzeigen, die auf dem Controller gesammelt werden soll:

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

Ausgabe anzeigen, die am AP gesammelt werden soll:

- show controller
- show capwap client mn
- show log

Zu sammelnde Debugs:

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

  Anmerkung: Diese oder andere Debug-Programme müssen nach Verwendung des Befehls **debug client<client mac>** eingeschaltet werden. Mit diesem Befehl werden alle früheren Debugs deaktiviert.

Zu erfassende Spur:

- Wireless-Trace

AP-Gruppen

Probleme im Zusammenhang mit dem Hinzufügen oder Löschen der AP-Gruppe oder dem Hinzufügen einer Schnittstelle zur AP-Gruppe.

Zu erfassende Ausgabe anzeigen:

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

Zu sammelnde Debugs:

- debug group enable

ACLs, Pre-Auth ACLs und CPU ACLs

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

DHCP

Debuggen von DHCP In-Band

- debug dhcp message enable
- debug dhcp packet enable

Debug DHCP für den aktivierten Service-Port

- debug dhcp service-port enable

Probleme mit dem Gastzugriff

Gast-WLAN

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

Bei DHCP-Problemen:

- debug dhcp packet enable
- debug dhcp message enable

Bei Problemen mit Mobilverbindungen:

- debug dot11 events enable
- debug dot11 mobile enable

Bei RADIUS-/AAA-Problemen:

- debug dot1x aaa enable

Probleme mit hoher Verfügbarkeit des WLC

AP-Failover

Konfigurationsproblem

Sammeln und prüfen Sie die folgenden Konfigurationsdateien:

- Alle zugehörigen WLC-Konfigurationsdateien: show run-config und show running-config.
- Ist die AP-Failover-Priorität konfiguriert?
- Primärer WLC pro AP ("Primärer Cisco Switch", Name | IP-Adresse]" unter "AP-Konfiguration")
- Sekundärer WLC pro AP ("Sekundärer Cisco Switch") [Name | IP-Adresse]" unter "AP-Konfiguration")
- Tertiärer Cisco Switch [Name | IP-Adresse]" unter "AP-Konfiguration")
- Die entsprechenden AP-Konfigurationsparameter im WLC - show ap config <AP-Name>.
- Der einzige unterstützte AP-Modus für Fast-Heartbeat ist lokal und h-reap ("AP Mode"-Feld).
- Die entsprechenden AP-Konfigurationsparameter im AP zeigen die Konfiguration des Capwap-Clients.

Failover auf unerwarteten WLC

- show sysinfo: Die maximale Anzahl von APs, die vom erwarteten WLC unterstützt werden.
- show ap summary - APs, die dem erwarteten WLC beigetreten sind.

- show capwap client ha - Wenn Fast-Heartbeat aktiviert ist, überprüfen Sie die Backup-Liste im AP.

Transportproblem

Wenn DHCP für die AP-Ethernet-Schnittstelle aktiviert ist, wurde dann eine IP-Adresse abgerufen? Verwenden Sie show interface FastEthernet0.

- ping <IP-Adresse> - Legt fest, ob der AP und der WLC einander pingen können.

CAPWAP-Protokolle

Allgemeine WLC- und AP-Debugbefehle:

- Debuggen von CAPWAP-Ereignissen und -Status - Aktivieren/Deaktivieren von CAPWAP-Ereignissen beim Debuggen
- CAPWAP-Fehler debuggen - Aktivieren/Deaktivieren von CAPWAP-Fehlern
- CAPWAP-Details debuggen - Aktivieren/Deaktivieren von CAPWAP-Details
- CAPWAP-Info debuggen - Aktivieren/Deaktivieren der CAPWAP-Info-Meldung
- Debug CAPWAP payload - debuggen capwap payload aktivieren/deaktivieren
- Debug CAPWAP hexdump - debug capwap hexdump enable/disable

AP-Fast-Heartbeat-spezifischer Debug-Befehl:

- Debug Fast-Heartbeat: show capwap client ha

  Anmerkung: Manchmal benötigen Sie die Ausgabe des Netzwerkanalysetools (z. B. Wireshark).

AP-Priorität

- Entscheiden Sie, ob die AP-Priorität aktiviert ist - show run-conf ("AP Join Priority" unter "Network Information")
- Bestimmen Sie die maximale Anzahl der vom WLC unterstützten APs - show sysinfo ("Maximale Anzahl unterstützter APs").
- Entscheiden Sie, wie viele APs dem WLC beigetreten sind: Übersicht anzeigen
- Prüfen der Join-Priorität jedes AP - Übersicht anzeigen (letzte Spalte)

Probleme mit Transporter und CAPWAP

Siehe die entsprechenden Sitzungen im Abschnitt AP-Failover.

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

Probleme im Zusammenhang mit H-REAP

H-REAP

Controller-Debugging:

- debug client <mac>

AP-Debugger:

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

H-REAP CCKM-Probleme

Controller-Debugging:

- debug cckm
- debug hreap cckm

AP-Show/-Debugs:

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

H-REAP Lokaler RADIUS

Controller-Debugging:

- debug hreap group
- debug hreap aaa

AP/Show Debugs:

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

Medien-Stream

- debug media-stream
- Admission (Zulassung): Das Debuggen von Client-Zulassungen ist beim Debuggen von Problemen mit Client-Verweigerung/Löschung hilfreich.
- Event (Ereignis) - Gibt IGMP-/Media Direct-Client-Updates aus.
- RRC - RRC State Machine updates.

debug bcast

- igmp: Client IGMP-Beitrittsanfrage-/Berichtsmeldungen.

Standortbezogene Probleme

```
>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.
```

Systemspeicher, Probleme mit nicht genügend Arbeitsspeicher

Zu erfassende Ausgabe konfigurieren und anzeigen

- show memory stat
- show buffers
- show process memory

Anmerkung: Wenn das Flag "config memory monitor errors" (Speicherüberwachungsfehler konfigurieren) auf "disable" gesetzt ist, können die Details zur Speicherbeschädigung mit den folgenden Befehlen hochgeladen werden:

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

Mesh-bezogene Probleme

Es gibt mehrere Fehlerpunkte (oder Fehlerpräsenz):

- Controller
- Mesh-APs
- GUI/WLC

Allgemeine Richtlinien

- Finden Sie den Fehlerpunkt, und isolieren Sie die fehlerhafte Komponente.
- Korrelation der Ablaufverfolgungen des Controllers, der Mesh-APs sowie der visuellen Ausgabe auf der CLI/GUI/WLC, um den Fehlerpunkt zu ermitteln
- Sammeln Sie bei paketbezogenen Problemen Airopeek- oder ätherische Spuren, um die vorläufige Analyse zu bestätigen.
- Analysieren Sie die Ursache des Fehlers und wie das Problem reproduziert werden kann.
- Konfiguration
- Trigger-Aktion

Allgemeine Richtlinien

In diesem Abschnitt sollen genügend Hinweise zum Debuggen eines Mesh-Fehlers und zum Sammeln relevanter Informationen bereitgestellt werden, damit die DEs den Fehler besser verstehen können. Da es unmöglich sein kann, einen Fehler auf den ersten Blick festzuhalten, ist dieses Dokument eine Reihe von Vorschlägen für das DT und kein Regelwerk. Die DT nutzt Diskretion, um relevante Fehlerberichte anzuhängen, um effizient zu studieren und den Fehler so schnell wie möglich zu beheben.

Fehlende verdächtige Pakete

Sammle ätherische und airopäische Spuren.

Debuggen von Befehlssätzen

Dabei handelt es sich um einen Satz generischer **Debugbefehle**, mit denen Informationen über das System abgerufen werden können.

CLI für allgemeine Anzeige:

- show version
- show capwap client rcb
- show mesh status
- show mesh module adjacency
- show mesh channel [current]

Test Mesh-CLI:

- Test Mesh-Adjacency - für Mesh-Adjacency-Testbefehle
- Mesh-Astools testen - für MESH Anti-Strang-Werkzeuge
- test mesh awpp - für Mesh-AWPP-Testbefehle
- test mesh disable: Deaktivieren einer Funktion
- Test Mesh aktivieren - um eine Funktion zu aktivieren
- Test Mesh Forwarding - für Mesh Forwarding-Testbefehle
- Mesh-Verbindungstest — für den Test der Mesh-Verbindung
- Mesh mperf - für MESH BW Prüfwerkzeug

Spezifische Probleme

- jedes Verbindungsproblem
- Debug-Mesh-Verbindung
- show mesh adjacency (child/parent/all)

Funk:

- show controller d0, d1, ... (für alle funkbezogenen Probleme)
- Spuren aus der Luft (zwischen den betroffenen Knoten)

Schnittstellenprobleme (in Bezug auf Datenverkehr):

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

Ethernet-Traces zwischen Controller und Roof-Top Access Point (RAP)

Forwarding:

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

IP-Adresse/DHCP:

- debug ip address
- show ip int bri
- show int bvi1
- show run int bvi 1
- show mesh forwarding port-state
- test mesh deaktiviert Port-Filter und pings router

IP-Datenverkehr und DHCP:

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

Ausschlussliste:

- debug mesh adjacency exclude - Überwacht Ereignisse, die Eltern ausschließen.
- test mesh adjacency exclude clear - Löscht die Zähler für die aktuelle Ausschlussliste und startet neu.

Adjacency-Status-Computer:

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

Kommunikation über Nachbarschaft:

- debug mesh adjacency packet
- debug mesh adjacency message

Probleme mit Adjazenzverknüpfungen:

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

Änderung des Signal-Rausch-Verhältnisses (SNR):

- debug mesh adjacency snr

Dynamische Frequenzwahl (Dynamic Frequency Selection, DFS):

- debug mesh adjacency dfs

Workgroup Bridge (WGB) verbindet nicht:

- Sammeln von Client-Debugging-Meldungen auf dem Controller und dem Access Point
- Sammeln Airopeek Sniffer-Traces zwischen dem WGB und dem übergeordneten Mesh AP.
- Der kabelgebundene Client hinter dem WGB kann keinen Datenverkehr weiterleiten.
- Abrufen des Status des übergeordneten WGB auf dem Controller
- Sammeln Sie Debug-Meldungen auf dem Controller, Mesh AP und WGB.
- Sammeln Sie ätherische Spuren zwischen dem übergeordneten Mesh-AP und dem Controller.

AP KANN NICHT VERBUNDEN WERDEN:

- Sammeln der Debugmeldung auf dem Controller:
- debug capwap errors enable
- debug capwap events enable

Sammeln der Debugmeldung am AP:

- debug capwap client event
- debug capwap client error

Weitere Informationen finden Sie in den folgenden zusätzlichen Debugs:

Controller-Debugging:

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

AP-Debugger:

- 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

ShowCommands:

- show capwap client rcb - zeigt die Konfiguration des Funksteuerungsblocks
- show capwap client config - zeigt die Funkkonfiguration aus nvram

Testbefehle:

- 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

Anti-Stranding Tools:

AP-Befehle

```
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-Adresse> - Die b/g-Funk-MAC-Adresse des isolierten AP.

Befehle anzeigen

- show mesh astools config - aktuelle Konfiguration
- show mesh astools stranded-ap-list - Druckliste der erkannten Stranded

APs - Keine Beacons gehört

- Stellen Sie sicher, dass mindestens ein benachbarter AP mit dem Controller verbunden ist

und den isolierten AP überwachen kann.
- Zeigen Sie cont d0 an, um den aktuellen Kanal von 11b-Funkmodulen zu bestimmen, der funktioniert.
- Sammeln Sie alle möglichen relevanten Debug-Meldungen.

Mperf Bandbreitenmesswerkzeug:

- Befehle anzeigen
```
show mesh mperf ?
globals --- Print configuration used to spawn objects
print [all/id] --- Print active connections
```
- Debugbefehle
```
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
```

Probleme mit dem NTP-Client und der Zeitkonfiguration auf dem Controller

- debug ntp packet enable
- debug ntp low enable
- debug ntp detail enable
- show time
- Ethereal-Erfassung am Controller-Management-Port

Probleme mit RF-Komponenten für die WLCs

```
>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
```

SNMP-Komponente für WLCs

```
>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.
```

- Schließen Sie den fehlgeschlagenen SNMP-Befehl (Simple Network Management Protocol) an.
- Wenn das WCS einen SNMP-Fehler meldet, versuchen Sie, den Befehl "SNMP set/get" von MG-soft oder einem anderen SNMP-Manager auszuführen.
- Überprüfen Sie, ob dies über die Benutzeroberfläche oder die CLI des Controllers möglich ist.
- Fügen Sie einen Screenshot der CLI/Controller-Benutzeroberfläche an.
- Bei Speicherlecks oder CPU-Problemen geben Sie an, wie lange das System bereits aktiv ist.
- Sehen Sie sich die SNMP-Debugs an, um festzustellen, ob etwas offensichtlich ist.debug snmp mibs enable o debug snmp agent enabledebug snmp traps enable.
- Von den früheren Debugs anfügen.

Probleme mit dem TFTP-Upload/-Download, einschließlich Upgrade/Downgrade

```
>debug transfer tftp ?

disable        Disables debug.
enable         Enables debug.
```

Web-GUI-Komponente für WLCs

- Geben Sie an, welches Browserproblem aufgetreten ist.
- Überprüfen Sie, ob Java-Skriptprobleme vorliegen. Wenn Firefox verwendet wird, überprüfen Sie die Fehlerkonsole. Fügen Sie einen Screenshot des Java-Skriptfehlers an. Internet Explorer zeigt ein Popup-Fenster an. Bei Firefox schließen Sie das Fehlerkonsolenfenster an.
- Wenn die Konfiguration fehlschlägt, wenden Sie sich an die CLI. Schließen Sie die CLI-Ausgabe an.
- Screenshot an den Bug anhängen.
- Erwähnen Sie den Controller und die AP-Plattform.
- Wenn es einen Absturz in emweb task gibt, dann schauen Sie sich die Absturzstapel-Ablaufverfolgung an. Wenn die Stapelüberwachung CLI anzeigt, verwenden Sie diese Komponente nicht.

Probleme mit Webauthentifizierung und Konfiguration

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

WLC-Webauth-Vorlage

Grundlegende Informationen

Bestimmen Sie die Topologie des Netzwerks zum Zeitpunkt der Webauthentifizierung.

- Handelt es sich um eine Gasteinrichtung oder eine normale Zuordnung an einem einzelnen WLC oder nachdem die Roam-Webauthentifizierung durchgeführt wurde?
- Welche Webauthentifizierung ist konfiguriert (intern, extern, angepasst oder Web-Passthrough)?
- Welche Anmeldeseite wird verwendet?

- Laden Sie das Webauth-Paket herunter, und stellen Sie es bereit.
- Haben Sie Secure-Web aktiviert? Wenn ja, deaktivieren Sie die Option, und prüfen Sie, ob Webauth funktioniert.

Befehle anzeigen:

- Client-Details anzeigen <mac>
- show wlan <wlanid>
- show rules show custom-web

Fehlersuche

- debug emweb server enable
- debug pm ssh-tcp enable
- debug pm ssh-engine enable packet <>
- debug pm ssh-appgw enable

debug client <mac>

> **Anmerkung:** Führen Sie dieses Debugging aus, wenn die Seite nicht angezeigt wird. Stellen Sie sicher, dass Sie dieses Debugging separat sammeln.

- debug mobility handoff enable

> **Anmerkung:** Führen Sie diesen Fehler aus, wenn Webauth nach dem Roaming nicht funktioniert.

Sniffer

- WLC DS-Port - Dies ist bei einem RADIUS-Authentifizierungsproblem hilfreich.WLC AP-Port - wenn HTTP-Pakete zwischen WLC und AP verworfen werdenPer Funk, wenn der WAP Pakete verwirft

Probleme und Erweiterungen im Zusammenhang mit der Controller-XML-Konfiguration

XML-Validierung

- XML-Validierungsfehlermeldungen, z. B. `Validation für den Knoten ptr_apfCfgData.apfVAPIDData.apfVapSecurity.<any configuration data>`, werden beim Systemstart beobachtet.
- die gesamte XML-Validierungsfehlermeldung
- Das CLI- oder GUI-Verfahren zum Konfigurieren der WLANs vor dem Systemstart
- die CLI- oder XML-Konfigurationsdatei, die vor dem Systemstart generiert und auf TFTP gespeichert wird
- Ungültige Konfiguration anzeigen

Diagnosekanal

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

Dynamische Kanalzuweisung

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

TACACS+

- debug aaa tacacs enable
- show tacacs summary

WLC-Multicast-Leitfaden

Grundlegende Informationen

- Netzwerktopologie
- Stellen Sie sicher, dass die Adresse des Multicast-Streams nicht die IANA-reservierte Adresse für die verwendete Anwendung ist.
- Verwendete Multicast-Adressen
- Multicast-Streamrate und Paketgröße
- Stellen Sie sicher, dass die konfigurierte Multicast-Adresse der AP-Gruppe nicht mit der Adresse des Multicast-Streams übereinstimmt.
- Das WLC-Modell (2106, 4404, 4402, WiSM...)
- Das AP-Modell (1131, 1232, 1242, 1250...)
- Vom Client verwendetes Radio
- MAC-Adresse des Clients

WLC-Informationen (alle Aromen)

Dumps von:

- show interface summarydebug bcast * enable
- show network summary
- show network multicast mgid summary
- show network multicast mgid detail <mgid>
- Für Version G und höher: WLAN-Gruppen anzeigen
- Für TALWAR/2106 mit neuem FP-Code:Wenn IGMP-Snooping aktiviert ist, debuggen Sie fastpath cfgtool —mcast4db.dump debuggen fastpath cfgtool —mcast2db.dumpWenn IGMP-Snooping deaktiviert ist, debuggen Sie fastpath cfgtool —mcast2db.dumpWenn Multicast-Unicast aktiviert ist, debuggen Sie fastpath cfgtool —mcastrgdb.dump

AP-Informationen (alle Varianten)

Dumps von:

- show lwapp mcastshow lwapp mcast mgid allshow lwapp mcast mgid id <mgid>show lwapp client traffic-four times with 1 minute interval

Radio Debugs:

1. Ethernet-Überlaufrate
2. Die Funkübertragungsrate

3. Die Funkabwurfrate
4. Energiesparmodus des Basis-Servicesets
5. Die gesamte Ethernet-RX-Rate
6. Ethernet-Multicast-RX-Rate

Führen Sie für #1 **die Show int g0 aus. | inc** overruncommand regelmäßig.

Führen Sie für #2, #3 und #4 **die Show weiter (Fortsetzung) d0 | beg** queuesregelmäßig. Überprüfen Sie die Sende-/Verwerfungszahlen für jede Warteschlange.

Führen Sie außerdem für #3 **die Show int d0 aus. | inc output** dropcommand regelmäßig.

Führen Sie für #5 **die Show cont g0 aus. | inc RX** Zählerbefehl periodisch.

Führen Sie für #6 **die Show cont g0 aus. | inc** multicastcommand regelmäßig. In der ersten Zeile wird RX-Multicast/-Broadcast angezeigt.

Um die Paketraten zu erhalten, führen Sie alle 10 Sekunden einen Befehl aus, und teilen Sie die Differenz durch 10. Wenn viele Pakete in der Multicast-Warteschlange (für einen BSS) gesendet werden, befindet sich der BSS im Energiesparmodus. Die maximale Multicast-Paketrate für einen Energiesparmodus ist relativ niedrig. Dies ist ein bekanntes Problem.

Switch-Informationen

Überprüfen Sie die Switch-Version mit dem Befehl **show** version. Der Switch kann die "advance ip base"-Version verwenden (z. B. Cisco IOS Software, C3750 Software [C3750-ADVIPSERVICESK9-M], Version 12.2(40)SE, RELEASE SOFTWARE (fc3)). [Abbild: c3750-advipservicesk9-mz.122-40.SE.bin]). Bei der Version "ip base" liegt ein Problem beim Routing des Multicast-Datenverkehrs zwischen VLANs vor.

Einige Fehlerbehebungen:

- Überprüfen Sie, ob Multicast-Routing aktiviert ist. ("show run" kann "ip multicast routing distributed" enthalten)
- Überprüfen Sie, ob die Konfiguration "ip pim sparse-dense-mode" zum konfigurierten VLAN hinzugefügt wurde.
- ip igmp-Gruppe anzeigen

Sniffer erfasst

- DS-Schnittstelle des WLAN
- Verwaltungsschnittstelle des WLC
- AP-Mgr, mit dem der AP verbunden ist (nur erforderlich, wenn mcast src drahtlos ist)
- Eth-Schnittstelle des AP
- Auf Sendung

Analyse von Sniffer-Aufnahmen

Multicast-Quelle ist kabelgebunden

- Überprüfen Sie, ob die Pakete den WLC an der DS-Schnittstelle erreichen.
- Überprüfen Sie, ob das LWAPP-gekapselte Multicast-Paket an die Verwaltungsschnittstelle gesendet wird. Das Paket muss Folgendes aufweisen:outer ip dst addr = konfigurierte

Multicast-Adresse einer AP-Gruppeudp dst port = 12224
- Überprüfen Sie, ob das in "b" angezeigte Paket am eth intf des AP erkannt wird.
- Überprüfen Sie, ob das Multicast-Stream-Paket auf Sendung empfangen wird.

Multicast-Quelle ist Wireless-seitig

- Überprüfen Sie, ob die LWAPP-gekapselten Pakete unter ap-mgr intf empfangen werden. Hier ist LWAPP Unicast.
- Überprüfen Sie, ob ein Multicast-Paket von der DS-intf gesendet wurde.
- Überprüfen Sie, ob das LWAPP-gekapselte Multicast-Paket an die Verwaltungsschnittstelle gesendet wird. Das Paket muss Folgendes aufweisen:outer ip dst addr = konfigurierte Multicast-Adresse einer AP-Gruppeudp dst port = 12224
- Überprüfen Sie, ob das in "b" angezeigte Paket am eth intf des AP erkannt wird.
- Überprüfen Sie, ob das Multicast-Stream-Paket auf Sendung empfangen wird.

Switch-Konfigurationsprüfung für WiSM

- Wenn Sie ein Wireless Services Module (WiSM) verwenden, überprüfen Sie, ob Sie dasselbe Problem erhalten, das im folgenden Abschnitt erwähnt wird.
- Cisco Bug-ID CSCsj48453 - CAT6k leitet Multicast-Datenverkehr im L3-Modus nicht an WISM weiter.
- Symptom - Multicast-Datenverkehr fließt nicht von einem kabelgebundenen Host zu einem Wireless-Host über die WiSM-Karte im L3-Modus, wenn sich beispielsweise beide Hosts in unterschiedlichen VLANs befinden. Nur das erste Paket wird erfolgreich erreicht. Danach hält der Verkehr an.
- Bedingungen - Der Datenverkehr wird nur gestoppt, wenn der Multicast-Replikationsmodus "Egress" ist.
- Problemumgehung - Eine Problemumgehung besteht darin, den Multicast-Replikationsmodus in den Eingangsmodus des Befehls **ip multicast Replication-mode** ingresszu ändern. Der Datenverkehr fließt im Eingangsmodus ordnungsgemäß. Vergewissern Sie sich, dass der Befehl **mls ip multicast** Capability den gleichenBefehl verwendet.

Weitere Problembeschreibung - Das Problem zeigt sich bei CAT6k und einem WiSM. Der Multicast-Datenverkehr vom Wireless-Host zum kabelgebundenen Host funktioniert auch in L3 einwandfrei. Außerdem funktioniert der Multicast-Datenverkehr, der vom kabelgebundenen Host zum Wireless-Host über die WiSM-Karte fließt, im L2-Modus einwandfrei.

WLC-QoS-Leitfaden

Mindestanzahl an Debugs

- Laden Sie "show run-config" von allen Switches in der Mobilitätsgruppe herunter.
- Wenn das Problem auftritt, erfassen Sie die folgenden Debugs:debug aaa all enabledebug pem state enabledebug pem events enabledebug mobility handoff enabledebug dot11 mobile enabledebug dot11 state enable
- Holen Sie sich eine Airopeek- oder AirMagnet-Spur in der Nähe des problematischen AP/Telefons/Hörers.
- Erfassen Sie den DS-Port des Switches, den Upstream-Switch des AP und die SpectraLink Voice Priorities (SVPs) mit Ethereal oder Etherpeek.

CallControl-Debuggen (SIP-Klassifizierung)

Fragen

- Handelt es sich um einen SIP-Client (Session Initiation Protocol)?
- Welche IP-Telefonanlage\sip wird verwendet?
- Zeigt es an, dass es auf diesem SIP-Server registriert ist?
- Funktioniert der 7921 wie erwartet, und nur die SIP-Clients haben ein Problem?

WLC-Informationen

- show wlan summary [WLAN-Nummer]
- Debuggen der Anrufsteuerung all
- Debuggen von Anrufsteuerungsereignissen
- Anrufsteuerungsfehler anzeigen
- Anrufe zur Anrufsteuerung anzeigen

AP-Informationen

- Details zu dot11 cc debuggen
- Fehler bei dot11 cc debuggen
- Debuggen von dot11 cc-Ereignissen
- lwapp client call-info mac (MAC-Adresse des betreffenden Clients) anzeigen

Lastbasierte Zugangskontrolle und Sprachkennzahlen

Zu beantwortende Fragen

- Tritt dies bei den beiden Funkmodulen "a" und "b" auf?
- Welchen Wert hat die Kanalnutzung, wenn der Anruf abgelehnt wird?
- Ist dies nur bei 7921-Telefonen oder auch bei anderen Telefonen der Fall? Wenn ja, welche Telefone gibt es? Wenn nicht, kann dies mit einem anderen TSPEC-Telefon versucht werden?
- Handelt es sich um 11n- oder reguläre APs?
- Nutzen Sie die Inter-Controller-Mobilität?
- Ist das TSPEC-Telefon geeignet?
- Ist es die UAPSD?
- Ist dies auf den Plattformen 2006 oder 4100 reproduzierbar?
- Handelt es sich um eine abgeschirmte Raumumgebung?
- Gab es eine besondere Bedingung, für die der Anruf abgelehnt wurde?

Debug- und Show-Befehle auf WLC für 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>

Debuggen des AP für LBCAC

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

Sprachmetriken

- Over-the-Air- und Wire-Sniffer-Aufnahmen
- Überprüfen Sie, ob UP6-Datenverkehr kontinuierlich generiert wird.
- Vergewissern Sie sich, dass das WLAN über das richtige QoS-Profil und die Wi-Fi Multimedia (WMM)-Richtlinie verfügt.
- Die meisten Fragen, die im Zusammenhang mit LBCAC gestellt werden, gelten für Sprachkennzahlen.

Debuggt Sprachkennzahlen und zeigt Befehle im WLC:

- 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>

Fehlerbehebung am AP für Sprachkennzahlen:

- debug dot11 tsm
- debug lwapp client voice-metrics

WLC-Lizenzhandbuch

Auf Controller zu sammelnde Debugs

- Konsolenausgabe
- Nachrichtenlog

ARP-Probleme

Auf Controller zu sammelnde Debugs

- debug arp all enable

Netzwerkprobleme

Auf Controller zu sammelnde Debugs

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

Sonstige

Auf Controller zu sammelnde Debugs

- dump-low-level-debugs
- Nachrichtenlog

Access Point-Probleme

IAPP

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

Probleme mit der WGB-Zuordnung

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

WGB oder kabelgebundener Client erhält keine DHCP-Adresse

- debug dhcp packet enable
- debug dhcp message enable

Der WGB- oder kabelgebundene Client verwendet eine statische IP-Adresse, die jedoch auf dem Controller nicht angezeigt wird.

- debug dot11 mobile enable
- debug dot11 state enable

AP-Benutzername Kennwort

Debuggen zum Sammeln auf AP

- debug lwapp client config

Aufnahmen

- Nicht zutreffend.

Zu erfassende Ausgabe konfigurieren und anzeigen

- config ap mgmtuser

Probleme mit der Clientverbindung

Client-Fehlersuche

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

Dem Controller gefällt die Zuordnungsanfrage nicht

Paketerfassung

- Airopeek-Erfassung auf dem Kanal, von dem der AP festgelegt wird. Es wird empfohlen, die Filterung zu vermeiden, da die Pakete für Beacon und Probe Req/resp verpasst werden können. Stellen Sie sicher, dass Sie das Ereignis erfassen, wenn die Verbindung beendet wird.
- Falls der Client keine Verbindung herstellt, erfassen Sie das gesamte Ereignis von der Probeanforderung bis zum Ende der Sitzung (z. B. wird der Fehler gesendet und die Zuordnungsantwort mit dem Statuscode ist nicht 0).
- Geben Sie die Client- und AP-MAC-Adressen an.

Anmerkung: Die AP MACi ist die Basis-MAC- + WLAN-ID des Funkmoduls.

Konfigurieren und Anzeigen der auf dem Controller zu erfassenden Ausgabe

- show sysinfo - Details zur WLC-Version
- show wlan x - auf WLC für das betroffene WLAN
- show run-config - von WLC
- show debug
- show msglog
- show tech-support - von WLC (gut zu haben, aber nicht notwendig)

Client-Details

- Client-Hardware - Supplicant-Software-Details wie Version und Software-Name (z. B. ADU oder Odyssey)
- Client-Betriebssystem - Wenn es sich um Windows handelt, geben Sie die Client-Systemkonfiguration an, und wählen Sie **Programme > Zubehör > Systemprogramme > Systeminformationen**.

Details zum RADIUS-Server

Geben Sie den RADIUS-Servertyp (SBR, Cisco ACS, Linux usw.) und ggf. die Konfiguration an.

Client reagiert nicht auf EAP-Anforderungen

Siehe Abschnitt "Controller does not Like the Association Request".

Die EAP-Authentifizierung wird nicht durchgeführt.

Siehe Abschnitt "Controller does not Like the Association Request".

DHCP-Anfrage vom Client fehlgeschlagen

Siehe Abschnitt "Controller does not Like the Association Request".

EAPOL Exchange wird nicht durchgeführt

Siehe Abschnitt "Controller does not Like the Association Request".

CCKM-Roaming schlägt fehl

Zu sammelnde Debugs

Die meisten Debugs entsprechen dem vorherigen Abschnitt, dem Problem mit der Clientverbindung. Diese neuen Fehlerbehebungen helfen jedoch besser beim CCKM-Debugging. Dieser Debug-Befehl ist ab Version 5.0 verfügbar:

- debug cckm enable
- show pmk-cache <Client-Mac> - auf dem Ziel-Controller
- show client details <client mac> - when client is connected on the old AP
- debug cckm enable

Anmerkung: Diese oder alle anderen Debug-Programme müssen eingeschaltet werden, nachdem Sie **debug client<client mac>** ausgegeben haben. Dies liegt daran, dass der **Debug-Client<mac>**-Befehl alle früheren Debugs deaktiviert.

Aufnahmen

Stellen Sie sicher, dass Sie den Kanal erfassen, in dem sich der Ziel-AP befindet. Sie möchten beispielsweise alle Managementpakete zwischen dem Client und dem Ziel-AP erfassen. Weitere Informationen finden Sie im Abschnitt Controller does not Like the Association Request (Controller-Anforderungen mögen keine Zuordnungen).

Konfigurieren und Anzeigen der Ausgabe für die Erfassung auf dem Controller

Lesen Sie den Abschnitt Controller Does Not Like the Association Request und geben Sie die folgenden Befehle ein:

- show pmk-cache <Client-Mac> - auf dem Ziel-Controller
- show client details <client mac> - when client is connected on the old AP

Client-Details

Siehe Abschnitt "Controller does not Like the Association Request".

PMKID-Caching schlägt fehl

Überprüfen Sie, ob der Client den opportunistischen Schlüssel-Cache (OKC) unterstützt.

Anmerkung: OKC entspricht nicht dem in 802.11I angegebenen proaktiven Schlüssel-Cache (PKC). Der WLC unterstützt nur OKC.

Zu sammelnde Debugs

Siehe Abschnitt "Controller does not Like the Association Request".

Aufnahmen

Stellen Sie sicher, dass Sie den Kanal erfassen, in dem sich der Ziel-AP befindet. Sie möchten beispielsweise alle Managementpakete zwischen dem Client und dem Ziel-AP erfassen.

Siehe Abschnitt "Controller does not Like the Association Request".

Konfigurieren und Anzeigen der Ausgabe für die Erfassung auf dem Controller

Lesen Sie den Abschnitt Controller Does Not Like the Association Request und geben Sie die folgenden Befehle ein:

- show pmk-cache <Client-Mac> - auf dem Ziel-Controller
- show client details <client mac> - when client is connected on the old AP

Client-Details

Siehe Abschnitt "Controller does not Like the Association Request".

Authentifizierungsprobleme

Zu sammelnde Debugs

Siehe Abschnitt "Controller does not Like the Association Request".

Aufnahmen

Nicht zutreffend.

Konfigurieren und Anzeigen der Ausgabe für die Erfassung auf dem Controller

Lesen Sie den Abschnitt Controller Does Not Like the Association Request und geben Sie die folgenden Befehle ein:

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

Client-Details

Siehe Abschnitt "Controller does not Like the Association Request".

802.11r (Fast Transition) Roaming funktioniert nicht

Zu sammelnde Debugs

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

> **Anmerkung:** Diese oder alle anderen Debug-Programme müssen eingeschaltet werden, nachdem Sie **debug client<client mac>** ausgegeben haben. Dies liegt daran, dass der **Debug-Client<mac>**-Befehl alle früheren Debugs deaktiviert.

Aufnahmen

Wenn Sie über die Luft wandern, sammeln Sie Airopeek capture auf dem Kanal, auf dem sich der Ziel-AP befindet. Sie möchten z. B. alle 802.11-Authentifizierungs-FT-Anforderungs-/Resp-Frames und alle Neuzuordnungs-Anforderungs-/Resp-Frames erfassen.

Wenn Sie über den DS laufen, sammeln Sie Airopeek capture auf dem Kanal, auf dem sich der

Quell-AP befindet. Wenn Sie z. B. Frames für Zuordnungsanforderungen bzw. Frames erfassen möchten. Sie möchten auch die FT-Anforderungen/resp. des Action-Frames auf dem Kanal des Quell-AP erfassen.

> **Anmerkung:** Es wird empfohlen, die Quell- und Ziel-APs im gleichen Kanal zu halten, um das 802.11R-Roaming-Problem zu beheben. Auf diese Weise können Sie FT req/resp und Ressoziation req/resp in einer einzigen Erfassungsdatei erfassen.

Konfigurieren und Anzeigen der Ausgabe für die Erfassung auf dem Controller

Lesen Sie den Abschnitt Controller Does Not Like the Association Request und geben Sie die folgenden Befehle ein:

- show pmk-cache <Client-Mac> - auf dem Ziel- und Quell-Controller
- show client details <client mac> - when client is connected on the old AP
- show mobility summary: die Mobilitätsdomänen-ID

Client-Details

Derzeit ist nur der WGB der bekannte 802.11R-Client. Weitere Informationen finden Sie im Abschnitt Controller does not Like the Association Request (Controller-Probleme mit Zuordnungsanforderungen).

Inter-Controller-Mobilität

Zu sammelnde Debugs

- debug client <client mac> - auf beiden WLCs
- debug mobility handoff enable - auf beiden WLCs (Reihenfolge speichern: Debug-Client immer zuerst aktivieren.)
- Debug pem state enable
- Eping <IP>
- Mping <IP>

Wenn der Mobility Control-Pfad oder die Daten aktiv sind, aktivieren Sie "debug mobility keepalive enable" auf beiden Switches (notieren Sie sich die Softwareversion auf beiden Controllern).

Wenn ARP nicht funktioniert, aktivieren Sie auf beiden Switches die Option "debug arp all enable".

Wenn DHCP nicht funktioniert, aktivieren Sie auf beiden Switches "debug dhcp message enable" und "debug dhcp packet enable".

Wenn IPSec beteiligt ist: debug pm sa-export enable, debug pm sa-import enable.

Wenn der Client nach einer Weile eine Verbindung herstellt, zeigen Sie, wie lange es gedauert hat.

Aufnahmen

Erfassung durch den Roaming-Typ, z. B. CCKM, PMKID oder TGR.

Zu erfassende Ausgabe konfigurieren und anzeigen

Lesen Sie den Abschnitt Controller Does Not Like the Association Request und geben Sie die folgenden Befehle ein:

- show pmk-cache <Client-Mac> - auf dem Ziel-Controller
- show client details <client mac> - when client is connected on the old AP
- show mobility summary - auf beiden WLCs

Client-Details

Siehe Roaming-Typ, z. B. CCKM, PMKID oder TGR.

Deaktivieren von Debuggen

Um alle Debugmeldungen zu deaktivieren, verwenden Sie den Befehl **debug disable-all**.

Alternativ können Sie bestimmte Debugging-Vorgänge mit dem Befehl debugund dem Schlüsselwort disable deaktivieren:

```
debug capwap events disable
```

Zugehörige Informationen

- Technischer Support und Dokumentation
- Wireless-Fehlerbehebungen und Protokollierung auf Catalyst 9800 Wireless LAN Controllern

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.