Problembehebung bei Problemen mit der Interoperabilität des Wireless-Clients mit CUWN

Inhalt

Einleitung
Voraussetzungen
Anforderungen
Verwendete Komponenten
Hintergrundinformationen
I. Problemdefinition
II. WLC-Konfiguration und allgemeine Protokolle
Ausführungskonfiguration
WLC-Konfigurationsdatei
GUI
CLI
Syslogs vom WLC
III. Details und Informationen zu Clientgeräten
IV. Netzwerktopologie
V. Verfolgen Sie zusätzliche Details und Details.
VI. WLC - Befehle anzeigen und debuggen
WLC-Debug-Befehle
WLC Befehle anzeigen
VII. AP - Befehle anzeigen und debuggen
Cisco IOS® Access Points mit geringem Speicheraufkommen
AP Befehle anzeigen
AP-Debug-Befehle
AP-COS Access Points
AP-COS Befehle anzeigen
Serie 1800 | AP-COS-Debugbefehle
Serie 2800/3800 | AP-COS-Debugbefehle
VIII. Clientseitige Paketerfassung
IX. Over-the-Air (OTA)-Paketerfassung
802.11n-Erfassungen
802.11ac OTA-Erfassungen
X. Zusammenfassung
I. Problemdefinition
II. WLC-Konfiguration und Protokolle
III. Informationen zu Client-Geräten
IV. Diagramm der Netzwerktopologie
V. Erstellen Sie eine Tabelle, um alle Client-Probleme aufzuzeichnen.
VI. Befehle auf dem WLC anzeigen und debuggen
VII. Befehle auf dem Access Point anzeigen und debuggen

Leichte Cisco IOS® APs
AP-COS-APs
VIII. Kundenseitige Aufnahmen
IX. OTACaptures
802.11n-Erfassungen
802.11ac-Erfassungen
XI. Anhang A - Zusätzliche Tipps und Tricks
Windows
macOS (ehemals OS X)

Einleitung

In diesem Dokument werden Interoperabilitätsprobleme im Zusammenhang mit der Cisco Unified Wireless Network (CUWN)-Lösung beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Cisco Wireless APs
- Wireless LAN Controller (WLC)
- Zugehörige Netzwerkgeräte

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.

> **Hinweis**: Die Zielgruppe für dieses Dokument sind erfahrene Wireless-Netzwerktechniker und Administratoren, die bereits mit der Verwendung, Konfiguration und Fehlerbehebung dieser Themen vertraut sind.

Hintergrundinformationen

Es kann üblich sein, zu finden, dass angesichts der verschiedenen Client-Geräte, die sowohl existieren und weiter entwickelt werden. Es kann eine Vielzahl von Problemen auftreten, wenn es darum geht, die Verbindung zum Wireless-Netzwerk herzustellen, zu warten oder einfach nur das Beste aus ihnen herauszuholen und die Infrastruktur zu unterstützen.

Dies kann häufig auf ein einfaches Konfigurationsproblem seitens des Client-Geräts und/oder der Wireless-Infrastruktur selbst zurückzuführen sein. In einigen Fällen kann dies jedoch auf ein

Interoperabilitätsproblem in Bezug auf ein bestimmtes Client-Gerät und dessen unterstützende Komponenten (Supplicant, WLAN-Adapter, Wireless-Treiber,...) und/oder die betreffenden APs zurückgeführt werden. Als Wireless-Techniker bieten solche Interoperabilitätsprobleme eine Möglichkeit, potenziell komplexe Herausforderungen zu identifizieren, zu beheben und zu lösen.

In diesem Dokument wird detailliert beschrieben, welche Informationen zunächst erfasst werden müssen, um solche Probleme hinsichtlich der Wireless-Interoperabilität, die bei der Unified Wireless Network (CUWN)-Lösung von Cisco auftreten, effektiv zu untersuchen und zu beheben. Die Notwendigkeit eines solchen umfassenden Ansatzes wird mit der stetig wachsenden Zahl und Kombination von Wireless-Client-Geräten und Access Point-Funkgeräten immer wichtiger. Zusätzliche Informationen zu den in diesem Artikel beschriebenen Aspekten können von Fall zu Fall angefordert und gesammelt werden, da eine unbegrenzte Anzahl von Variablen diese Anforderungen bestimmen kann. Die hier aufgeführten Informationen stellen jedoch einen allgemeinen Leitfaden für die Behandlung potenzieller Probleme im Zusammenhang mit der Interoperabilität von Wireless-Clients dar.

I. Problemdefinition

Der erste Schritt, jedes Problem mit der Absicht, gelöst zu werden, effektiv anzugehen, besteht darin, das vorliegende Problem genau zu definieren. Zu diesem Zweck ist sicherzustellen, dass mindestens diese Fragen gestellt und ihre Antworten klar dokumentiert werden:

- Ist das Problem auf ein bestimmtes AP- und/oder Funkmodell (2,4 GHz gegenüber 5 GHz) beschränkt?
- Wird das Problem nur bei bestimmten Versionen der WLC-Software festgestellt?
- Tritt das Problem nur bei bestimmten Versionen von Clienttyp(en) und/oder Software auf (Betriebssystemversion, WLAN-Treiberversion,...)
- Gibt es andere Wireless-Geräte, bei denen dieses Problem nicht auftritt? Wenn ja, welche?
- Ist das Problem reproduzierbar, wenn der Client mit einer vereinfachten Wireless-Konfiguration wie einer offenen SSID mit einer Kanalbreite von 20 MHz verbunden und 802.11ac deaktiviert ist? (Tritt das Problem also nur im 802.11n-Modus und nicht nur im 802.11ac-Modus auf?)
- Wenn das Problem bei einer offenen SSID nicht reproduzierbar ist, welche Mindestsicherheitskonfiguration ist für das Problem erforderlich? (PSK oder 802.1X im WLAN).
- Wie lauteten die vorherigen zweifelsfrei funktionierenden Konfigurations- und Softwareversionen?

II. WLC-Konfiguration und allgemeine Protokolle

Ausführungskonfiguration

Ausnahmslos ist es unbedingt erforderlich, die WLC-Konfiguration zu erfassen, um eine detaillierte Überprüfung der vom Kunden verwendeten Funktionen, ihrer spezifischen Konfiguration und anderer solcher Details zu erhalten. Dazu müssen Sie eine Telnet/SSH-Sitzung mit den entsprechenden WLCs einrichten und die Ausgabe dieser CLI-Befehle in einer Textdatei speichern:

```
config paging disable

show run-config
```

Die vollständige Ausgabe von run-config wird immer bevorzugt, da sie detaillierte Informationen zu den verbundenen APs und den zugehörigen RF-Informationen enthält. Allerdings in einigen Fällen und Situationen, z. B. wenn Sie zu Beginn mit einem WLC mit einer großen Anzahl verbundener APs arbeiten (8510 WLC mit mehr als 2500 APs). Es könnte vorgezogen werden, zunächst nur die Konfiguration des WLC ohne solche AP-Informationen zu erfassen, um sie schnell zu überprüfen, da die vollständige Anzeige der Ausführungskonfiguration 30 Minuten oder länger dauern kann, bis die angegebene Anzahl von APs abgeschlossen ist. Es kann jedoch weiterhin erforderlich sein, die Ausgabe für die vollständige Run-Konfiguration zu einem späteren Zeitpunkt zu erfassen.

Dazu können Sie optional die Ausgabe dieser CLI-Befehle in eine Textdatei sammeln:

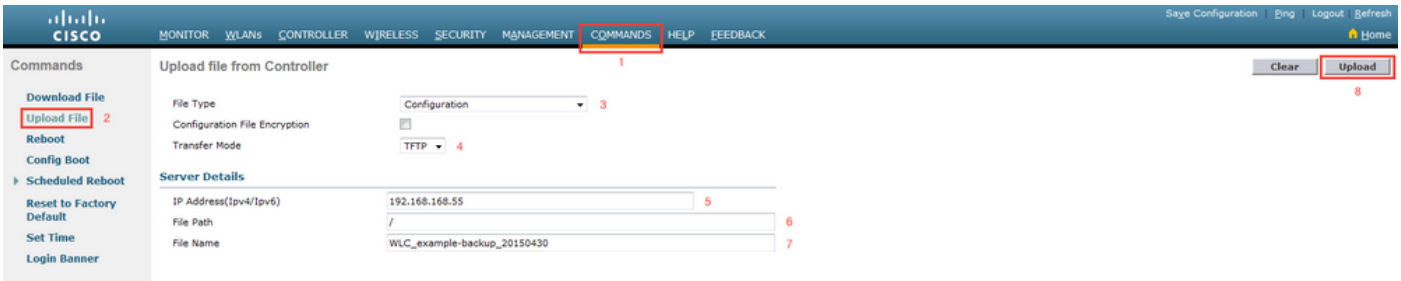
```
config paging disable

show run-config no-ap

show wlan apgroups
```

WLC-Konfigurationsdatei

Zusätzlich zur Ausgabe von **show run-config** oder **show run-config no-ap** wird auch empfohlen, ein vollständiges Backup der WLC-Konfiguration zu erstellen. Dies ist hilfreich, wenn ein Labor-Remix über TAC/HTTS und BU Eskalation durchgeführt werden muss, um das Problem in einer Cisco Laborumgebung zu reproduzieren. Ein Backup des WLC kann über die GUI oder die CLI des jeweiligen WLC gesammelt werden, wobei die Konfigurationsdatei über TFTP oder FTP auf dem externen TFTP/FTP-Server gespeichert wird. Dieses Beispiel zeigt die Verwendung der Benutzeroberfläche und der CLI zum Speichern eines Backups des WLC unter Verwendung von TFTP:

GUI

Befehle > Datei hochladen > Konfiguration > Hochladen wie im Bild dargestellt.



CLI

```
transfer upload datatype config

transfer upload mode tftp transfer upload serverip <TFTP-Server_IP-address> transfer upload path
/ transfer upload filename <desired-filename> transfer upload start
```

Syslogs vom WLC

Zu diesem Zeitpunkt möchten Sie bei Bedarf auch die aktuellen Protokolle vom WLC sammeln, um sie noch einmal überprüfen zu können. Im Idealfall sollten diese Protokolle unmittelbar nach dem Test mit einem Wireless-Client gesammelt werden, wodurch das gemeldete Problem reproduziert wird. Wenn der Kunde die WLC-Protokolle an einen externen Syslog-Server exportiert, möchten Sie sie von dort abrufen. Andernfalls können Sie das msglog und das Traplog, die derzeit lokal auf dem WLC gespeichert sind, speichern, indem Sie diese CLI-Sitzungsausgabe in einer anderen Textdatei speichern:

```
config paging disable

show msglog

show traplog
```

III. Details und Informationen zu Clientgeräten

Der nächste Schritt besteht darin, so viele Informationen und Details zu den verwendeten Client-Geräten zu sammeln, bei denen ein potenzielles Problem mit der Wireless-Interoperabilität auftritt. Diese Informationen müssen Folgendes umfassen, sind jedoch nicht unbedingt darauf beschränkt:

- Client-Typ (Tablet, Smartphone, Notebook, ...)
- Gerätehersteller und -modell
- Betriebssystemversion
- WLAN-Adaptermodell
- Treiberversion des WLAN-Adapters
- Verwendete Komponente (Windows Zero Config/Auto Config, Intel PROSet, ...)
- Für die Verwendung durch den Wireless-Client und das WLAN konfigurierte Sicherheit (offen, PSK, EAP-PEAP/MSCHAPv2,...)
- Beachten Sie alle Client-Parameter, die von den vom jeweiligen Anbieter bereitgestellten Standardeinstellungen abweichen (Ruhezustand, Roaming-Parameter, U-APSD,...).

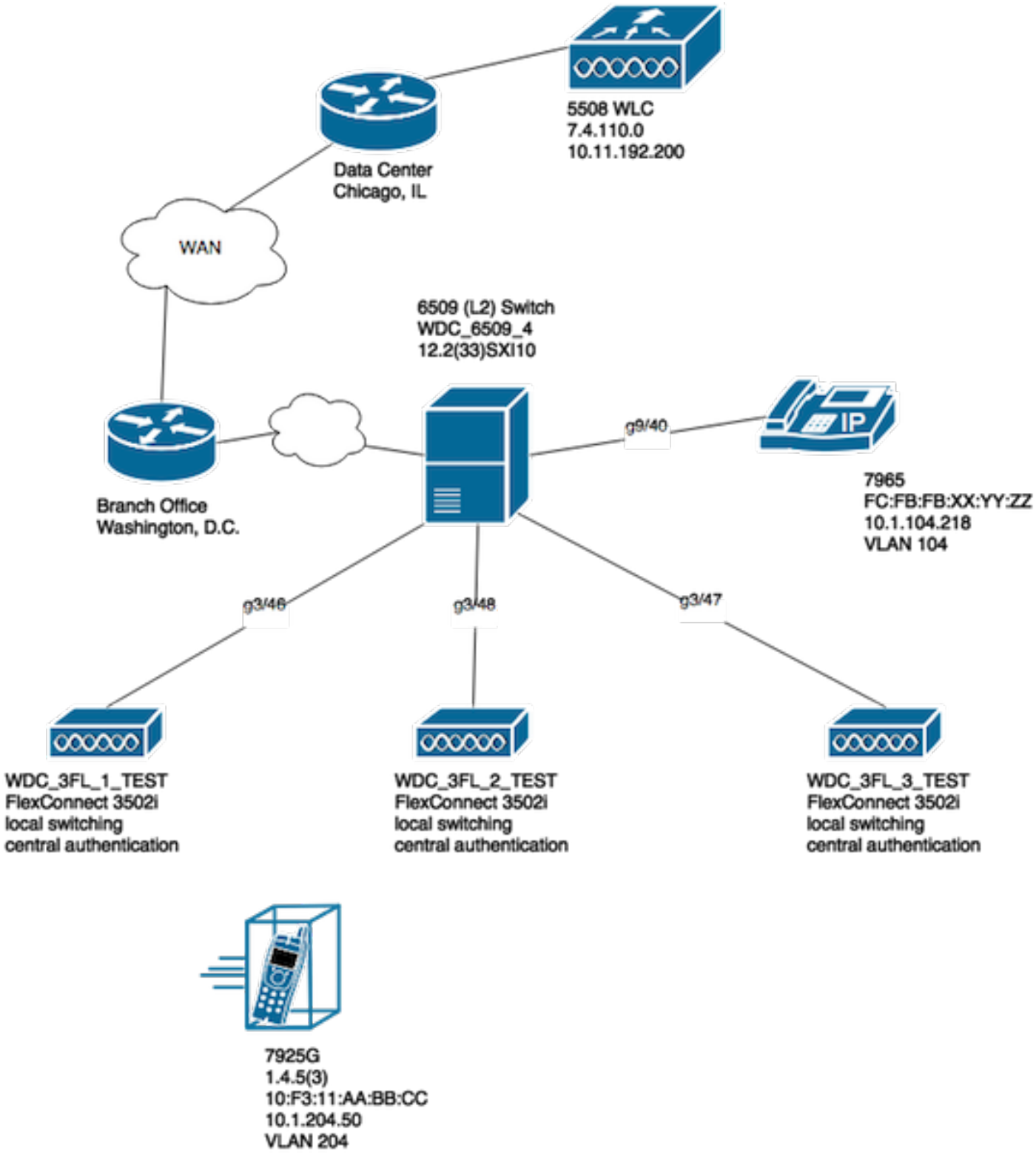
Hinweis: Zusätzliche Informationen oder Hinweise zu den Client-Geräten, einschließlich Screenshots der WLAN-bezogenen Konfiguration usw. müssen bei Bedarf ebenfalls bereitgestellt werden.

IV. Netzwerktopologie

Um die Fehlerbehebung und den Prozess der Ursachenanalyse (Root Cause Analysis, RCA) weiter zu beschleunigen, wird stets empfohlen, ein detailliertes und detailliertes Netzwerktopologiediagramm bereitzustellen. Das Netzwerktopologiediagramm muss nicht nur Details über das Netzwerk und die Wireless-Infrastruktur enthalten, sondern auch einen Einblick in die betreffenden Wireless-Geräte geben, die innerhalb des Netzwerks betrieben werden (Drucker/Scanner, welche Client-VLAN(s) genutzt werden,...) und deren Position(en) zueinander.

Eine Reihe von Tools (Microsoft Visio, draw.io,...) und eine Vielzahl von Stilen können verwendet werden, um ein solches Netzwerkdiagramm zu erstellen. Wichtig ist dabei lediglich, sicherzustellen, dass die richtigen Informationen in dem Diagramm, das von allen Beteiligten und Anbietern zur Prüfung bereitgestellt wird, klar und deutlich wiedergegeben werden. Eine Beispiel-Netzwerktopologie, die grundlegende, aber nützliche Informationen sowohl zur Infrastruktur als

auch zu den Client-Geräten erfasst, wie im Bild gezeigt.



V. Verfolgen Sie zusätzliche Details und Details.

Um sicherzustellen, dass bei jedem Test mit den Client-Geräten, bei denen Endbenutzer Probleme haben, die entsprechenden Informationen gesammelt werden. Es wird empfohlen, präventiv eine Tabelle oder Ähnliches zu erstellen, um alle Client-Probleme und die zugehörigen Details aufzuzeichnen, die zum Zeitpunkt des Tests beobachtet wurden, wie in diesem Beispiel:

MAC-Adresse	Benutzername	Beschreibung des gemeldeten	Zeitpunkt, zu dem der Endbenutzer	Ping für Standardgateway	WiFi-Signal (Verbunden

	Symptoms	das Symptom beobachtet hat	J/N		
xxyy.aabb.0011 Test_Benutzer1	Unterbrechungsfreie Verbindung zum Access Point	Netzwerkverbindung und Wireless-Verbindung vom AP3 unterbrochen.	N		Verbindung

Ziel dieser Übung ist es, ein gemeinsames Muster zu dokumentieren und zu ermitteln sowie ein genaues Bild der aktuellen Probleme zu erhalten. Sobald diese Tabelle für die Datenerfassung vorbereitet wurde, können Sie mit den Tests beginnen. Weitere, jedoch wichtige Überlegungen:

> **Hinweis**: Alle gesammelten Debug- und Paketerfassungen müssen mit demselben NTP-Server synchronisiert werden, um die Korrelation mit den Protokollen zu vereinfachen. Sie müssen für jeden Test gleichzeitig durchgeführt werden.

> **Hinweis**: Geben Sie einen genauen Zeitstempel an, wann das Problem festgestellt wurde und wann es sich zu erholen scheint (falls zutreffend).

> **Hinweis**: Sammeln Sie auf dem AP und dem WLC stets die nach der MAC-Adresse des Clients gefilterten Debugging-Meldungen.

> **Hinweis:** Führen Sie auf dem Access Point innerhalb derselben Telnet-/SSH-/Konsolensitzung keine Befehle zum Anzeigen und Debuggen aus. Diese werden entsprechend separat in einer anderen Sitzung ausgeführt.

> **Hinweis**: AP-Fehlerbehebungen werden bevorzugt bei Telnet/SSH und nicht bei der Konsole durchgeführt, da die Konsole in der Regel zu langsam ist, um effektiv zu sein.

VI. WLC - Befehle anzeigen und debuggen

Bei der Durchführung von Tests zur Reproduktion und Fehlerbehebung potenzieller Probleme mit der Interoperabilität von Wireless-Clients müssen in der verwendeten Wireless-Infrastruktur unbedingt Fehlerbehebungen und zusätzliche Protokolle erfasst werden. In diesen beiden Abschnitten werden die spezifischen Protokolle und die anfängliche Debugausgabe, die vom WLC bzw. den APs erfasst werden, ausführlich erläutert.

WLC-Debug-Befehle

```
config sessions timeout 0
debug client <MAC_address> debug dhcp message enable
```

In Bezug auf die Art des vorliegenden Problems können Sie diese WLC-Debugs auch von Fall zu Fall hinzufügen:

- **debug aaa detail enable** - Verwenden Sie diese Option, wenn Probleme mit der Authentifizierung beim AAA-Server auftreten.
- **debug aaa events enable** - Verwenden Sie diese Option, wenn Probleme mit der Authentifizierung beim AAA-Server auftreten.
- **debug aaa all enable** - Verwenden Sie diesen Parameter für Authentifizierungsprobleme. Die Ausgabe für diesen Debugger ist ausführlich, verwenden Sie ihn daher nur, wenn dies unbedingt erforderlich ist (bei AAA-Überschreibungsfällen...)
- **debug mobility handoff** - bei Roaming-Problemen zwischen WLCs verwenden

Sobald das Problem mit dem betreffenden Wireless-Client reproduziert wurde und alle in den vorherigen und folgenden Abschnitten beschriebenen Informationen gesammelt und dokumentiert wurden. Um diese CLI-Befehle auszuführen, müssen Sie die Debugging-Funktionen auf dem WLC deaktivieren.

```
debug disable-all
```

WLC Befehle anzeigen

```
config paging disable

show time

show client detail <MAC_address>

ping <client_IP-address> <repeat count [1-100]>
```

Stellen Sie wie bereits erwähnt sicher, dass die WLC-Debugging-Vorgänge in einer Telnet/SSH-Sitzung ausgeführt und die Ausgabe für diese Show-Befehle in einer anderen Telnet/SSH-Sitzung des WLC gesammelt wird. Sie müssen das Gleiche tun, um die AP-Debugs zu sammeln und die Ausgabe der Befehle anzuzeigen, die in diesem Abschnitt detailliert beschrieben sind.

VII. AP - Befehle anzeigen und debuggen

Leichte Cisco IOS® Access Points

Bevor Sie mit der Fehlerbehebung für die im Test verwendeten Lightweight Cisco IOS® APs (z. B. Access Points der Serien 2600, 2700, 3700 oder ältere Modelle von Cisco) beginnen, Sie müssen diese CLI-Befehle zunächst auf dem Access Point ausführen, um eine Zeitüberschreitung bei einer Telnet-/SSH-/Konsolensitzung mit den betreffenden Access Points zu vermeiden, wenn der Client Folgendes testet:

```
debug capwap console cli

config t

line vty 0 4

exec-timeout 0

session-timeout 0
```

Sie können diese Schritte auch ausführen, um die Konsolenverbindung zu verwenden und stattdessen die **Anweisung line vty 0 4** durch **line console 0** zu ersetzen, um die exec- und Session-Timeouts für eine serielle/Konsolenverbindung entsprechend zu deaktivieren.

- line console 0 - dient zum Ändern der Timeout-Parameter für serielle Sitzungen
- line vty 0 4 - zum Ändern der Timeout-Parameter für Telnet-/SSH-Sitzungen

AP Befehle anzeigen

Bevor Sie mit dem Test beginnen, müssen Sie zunächst ein Beispiel dieser Befehle zum Anzeigen des Access Points sammeln. Sammeln Sie die Ausgabe dieser show-Befehle mindestens zweimal für jeden Test, an dem der betreffende Wireless-Client beteiligt ist, sowohl vor als auch nach Abschluss des Tests.

```
term len 0

show clock

show tech

show capwap client mn

show int do1 dfs

show logging

more event.log

show trace dot11_rst display time format local

show trace dot11_rst

show trace dot11_bcn display time format local

show trace dot11_bcn
```

AP-Debug-Befehle

Nachdem Sie die erste Ausgabe der zuvor genannten show-Befehle gesammelt haben, können Sie die Debug-Vorgänge nun wie dargestellt auf demselben Access Point in einer separaten Telnet/SSH-Sitzung aktivieren. Stellen Sie sicher, dass die gesamte Ausgabe in einer Textdatei gespeichert wird.

```
debug dot11 {d0|d1} monitor addr <client_MAC-address>

debug dot11 {d0|d1} trace print clients mgmt keys rxev txev rcv xmt txfail ba

term mon
```

Flag	Beschreibung
d0	2,4-GHz-Funkmodul (Steckplatz 0)
D1	5-GHz-Funkmodul (Steckplatz 1)
Verwaltung	Trace-Verwaltungspakete
Ba	Trace-Block ACK-Informationen
Empf	Trace empfangener Pakete

Tasten	Trace-Set-Schlüssel
rxev	Trace empfangene Ereignisse
TXEV	Übertragene Ereignisse verfolgen
Txrad	Trace wird an Funk übertragen
xmt	Trace überträgt Pakete
txfail	Fehler bei Trace-Übertragung
Tarife	Änderungen der Trace-Rate

Wenn Sie die Fehlersuche am Access Point deaktivieren möchten, nachdem der Test- und Datensammlungsprozess abgeschlossen ist, können Sie den folgenden CLI-Befehl am Access Point ausführen:

```
u all
```

AP-COS Access Points

Für 802.11ac Wave 2-fähige Access Points und neuere Versionen, z. B. Access Points der Modelle 1800, 2800 und 3800. Diese neueren Access Point-Modelle führen ein völlig neues Betriebssystem für die Access Point-Plattformen ein, das als AP-COS bezeichnet wird. Daher gelten nach wie vor nicht alle Befehle, die zuvor für die herkömmlichen Lightweight Cisco IOS® Access Points verwendet wurden. Wenn bei der Fehlerbehebung ein Interoperabilitätsproblem mit verschiedenen Client-STA-Geräten und AP-COS-Modell-APs auftritt, müssen diese Informationen von den AP-COS-Access Points gesammelt werden, die an dem entsprechenden Test beteiligt sind.

Vor dem Starten von Debugs auf AP-COS-Modell-APs, die an dem Test beteiligt sind. Sie müssen zuerst diesen CLI-Befehl auf dem Access Point ausführen, um ein Timeout zum Zeitpunkt einer Telnet-/SSH-/Konsolensitzung mit den betreffenden Access Points zu vermeiden, wenn der Client Folgendes testet:

```
exec-timeout 0
```

AP-COS Befehle anzeigen

Bevor Sie mit dem Test beginnen, müssen Sie zunächst ein Beispiel dieser Befehle zum Anzeigen des Access Points sammeln. Sammeln Sie die Ausgabe dieser show-Befehle mindestens zweimal für jeden Test, an dem der betreffende Wireless-Client beteiligt ist, sowohl vor als auch nach Abschluss des Tests.

```
term len 0

show clock show tech

show client statistics <client_MAC-address>

show cont nss status

show cont nss stats

show log
```

Serie 1800 | AP-COS-Debugbefehle

Diese Fehlerbehebungen sind spezifisch für die Access Points der Serie 18xx. Dies ist darauf zurückzuführen, dass sich die für die Access Points der Serie 1800 verwendeten Chipsätze von denen der Access Points der Serien 2800/3800 unterscheiden. In diesem Szenario ist daher ein anderer Satz an Debugging-Vorgängen erforderlich. Die entsprechenden Fehlerbehebungsmaßnahmen für die Access Points der Serien 2800/3800 werden im nächsten Abschnitt behandelt.

Nachdem Sie die erste Ausgabe der zuvor genannten show-Befehle gesammelt haben, müssen Sie nun die Debug-Vorgänge auf denselben 1800 Access Points in einer separaten Telnet/SSH-Sitzung wie dargestellt aktivieren. Stellen Sie sicher, dass die gesamte Ausgabe in einer Textdatei gespeichert wird.

```
debug dot11 client level events addr <client_MAC-address>

debug dot11 client level errors addr <client_MAC-address>

debug dot11 client level critical addr <client_MAC-address>

debug dot11 client level info addr <client_MAC-address>

debug dot11 client datapath eapol addr <client_MAC-address>

debug dot11 client datapath dhcp addr <client_MAC-address>

debug dot11 client datapath arp addr <client_MAC-address>
```

In einigen Fällen müssen Sie möglicherweise auch die zusätzlichen Debugging-Funktionen auf dem 18xx AP aktivieren, um weitere Probleme mit der Client-Interoperabilität zu beheben. Dies sollte jedoch nur dann erfolgen, wenn/wie von einem Cisco TAC-Techniker für eine entsprechende Serviceanfrage/einen entsprechenden Fall angefordert.

Da zusätzliche Debugs nicht nur viel ausführlicher ausgegeben werden können, sondern auch eine zusätzliche Last für den Access Point verursachen können, benötigt es zusätzliche Zeit für die ordnungsgemäße Analyse. Dies kann unter bestimmten Bedingungen den Dienst möglicherweise unterbrechen, wenn viele Client-Geräte versuchen, unter Test oder ähnlichen Variablen eine Verbindung mit demselben Access Point herzustellen.

Um die Fehlersuche auf dem Access Point mit der Variante AP-COS zu deaktivieren (auf einem Access Point der Serien 1800 oder 2800/3800), können Sie nach Abschluss des Test- und Datensammlungsprozesses den folgenden CLI-Befehl auf dem Access Point ausführen:

```
config ap client-trace stop
```

Serie 2800/3800 | AP-COS-Debugbefehle

Nachdem Sie die anfängliche Ausgabe der oben genannten show-Befehle gesammelt haben, müssen Sie nun die Debug-Vorgänge auf denselben 2800/3800 Access Points wie dargestellt in einer separaten Telnet/SSH-Sitzung aktivieren. Stellen Sie sicher, dass die gesamte Ausgabe in einer Textdatei gespeichert wird.

```
config ap client-trace address add <client_MAC-address>
config ap client-trace filter all enable
config ap client-trace output console-log enable
```

```
config ap client-trace start
term mon
```

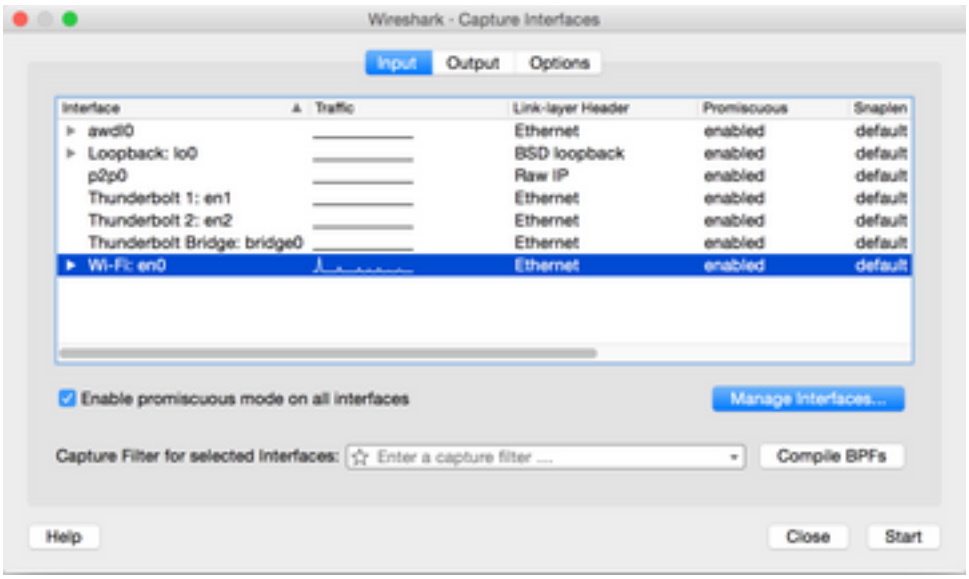
Um die Fehlersuche auf dem Access Point der Serien 1800/2800/3800 zu deaktivieren, nachdem der Test- und Datensammlungsprozess abgeschlossen ist, können Sie den folgenden CLI-Befehl auf dem Access Point ausführen:

```
config ap client-trace stop
```

VIII. Clientseitige Paketerfassung

Wenn es sich bei dem verwendeten Client-Gerät um einen Notebook-PC, ein MacBook oder Ähnliches handelt, müssen Sie die Paketerfassung im Promiscuous-Modus von der Wireless-Schnittstelle des Client-Geräts sammeln, mit dem das Problem reproduziert wurde. Allgemeine Dienstprogramme wie Netmon 3.4 (nur Windows) oder Wireshark können einfach heruntergeladen und verwendet werden, um diese Erfassung zu sammeln und sie in einer *.pcap-Datei zu speichern. Es hängt von dem Gerät ab, es kann auch Mittel geben, um einen tcpdump oder Ähnliches von dem betreffenden Client zu sammeln, so können Sie sich mit dem Hersteller des Client-Geräts für Unterstützung in dieser Hinsicht beraten müssen.

Hier ist ein Beispiel, um eine Wireshark-Aufzeichnung für die Wireless-Schnittstelle auf einem MacBook Pro zu konfigurieren:



Wie bei jeder Paketerfassung, unabhängig davon, welches Dienstprogramm verwendet wird, um sie zu sammeln, stellen Sie sicher, dass die Datei in einem pcap-Dateiformat (*.pcap, *.pcapng, *.pkt,...). So soll sichergestellt werden, dass nicht nur Cisco Techniker in allen Abteilungen die Paketerfassungsdateien mit Leichtigkeit anzeigen können, sondern auch Techniker von anderen Anbietern und Organisationen (Intel, Apple usw.). Dies ermöglicht einen nahtloseren Kooperations- und Kooperationsprozess, der die Zusammenarbeit zwischen Cisco und dem/den Clientgerätehersteller(n) bei der Untersuchung und Behebung potenzieller Interoperabilitätsprobleme weiter vereinfacht.

IX. Over-the-Air (OTA)-Paketerfassung

Um potenzielle oder bestehende Probleme mit der Wireless-Interoperabilität effizient beheben zu können, ist es wichtig, eine qualitativ hochwertige OTA-Paketerfassung des Problems zu erfassen. Dies ermöglicht die detaillierte Analyse der tatsächlichen 802.11-Wireless-Kommunikation

zwischen den betreffenden Wireless-Client- und Access Point-Funkmodulen und gibt darüber hinaus eine weitere Perspektive für die Client-Seite und die Protokolle und Fehlerbehebungen der Wireless-Infrastruktur. Dies ist ein wichtiger Schritt, der ausnahmslos für jeden Test eines potenziellen Problems mit der Wireless-Interoperabilität durchgeführt werden muss.

Häufig ist der Endkunde jedoch nicht angemessen ausgestattet oder bereit, OTA-Paketerfassungen zu sammeln. Wireless-Techniker stehen häufig vor einem solchen Hindernis und müssen mit dem Kunden zusammenarbeiten, um dieses Problem auf verschiedene Weise zu lösen. Dieser Artikel aus den Cisco Support-Foren kann als guter Ausgangspunkt dienen, um den Kunden entsprechend zu führen und zu schulen:

802.11 Wireless-Sniffing/Paketerfassung

Es ist von größter Wichtigkeit, dass die OTA-Paketerfassung(en) in einem pcap-Dateiformat (*.pcap, *.pcapng, *.pkt,...) erfasst wird und 802.11-Metadaten (RSSI, Kanal, Datenrate,...) umfasst. Der OTA-Sniffer muss außerdem während der Tests stets in unmittelbarer Nähe des betreffenden Client-Geräts aufbewahrt werden, um eine genaue Übersicht über den an das bzw. von dem getesteten Client-Gerät gesendeten und empfangenen Datenverkehr zu erhalten.

> **Hinweis**: Wenn die fraglichen Tests ein Client-Geräte-Roaming-Szenario beinhalten, bei dem mehr als ein 802.11-Kanal in einer aggregierten Paketerfassung überwacht werden muss. Dann ist es derzeit nicht empfehlenswert, AirMagnet WiFi Analyzer von Fluke Networks zu verwenden.

Der Grund dafür ist die Tatsache, dass aggregierte Paketerfassungen unter Verwendung dieses Dienstprogramms derzeit in einem proprietären Dateiformat gespeichert werden und nicht in einem pcap-Format, das in Wireshark oder anderen ähnlichen Dienstprogrammen problemlos angezeigt werden kann. Stellen Sie sicher, dass Ihre OTA-Paketerfassung in einem nicht proprietären Dateiformat vorliegt. Auf diese Weise wird sichergestellt, dass alle beteiligten Parteien und Anbieter jederzeit problemlos sämtliche Erfassungsdateien überprüfen können und letztendlich die Problembehebung beschleunigt wird.

in einem Format, das von aktuellem Wireshark gelesen werden kann und das 802.11-Metadaten (RSSI, Kanal, Datenrate) umfasst - Weitere Informationen finden Sie unter: https://supportforums.cisco.com/document/75331/80211-wireless-sniffing-packet-capture#sthash.Xhlx5LSS.dpuf
Es folgen einige gängige Methoden zum Sammeln einer OTA-Paketerfassung:

- AirPCAP mit Wireshark
- MacBook Pro
- OmniPeek Professional, OmniPeek Enterprise,...
- OmniPeek Remote Assistant (ORA)
- Cisco AP im Sniffer-Modus

802.11n-Erfassungen

Für OTA-Paketerfassungen, die 802.11n-Wireless-Clients umfassen, gibt es derzeit mehr Flexibilität und Benutzerfreundlichkeit. Dies ist auf eine größere Vielfalt von verfügbaren Wireless USB WLAN-Adaptern zurückzuführen, die problemlos mit einer Reihe von Tools wie OmniPeek und anderen verwendet werden können.

Beachten Sie, dass die Funktionen der spezifischen Wireless-Adapter, die für die Erfassung einer 802.11n-OTA verwendet werden, mit denen des tatsächlichen WLAN-Chipsatzes verglichen werden, der von den Client-Geräten verwendet wird, für die Sie eine Fehlerbehebung durchführen möchten. Beispiel: Das Client-Gerät weist ein potenzielles Problem mit der Wireless-Interoperabilität auf, bei der ein 802.11n-Chipsatz mit zwei räumlichen Streams (2SS) verwendet wird. In diesem Fall wird dringend empfohlen, sicherzustellen, dass der Wireless-Adapter, der für die Erfassung von OTA-Paketen verwendet wird, auch ein 2SS- oder besserer Adapter mit 802.11n- oder neueren Spezifikationen ist.

802.11ac OTA-Erfassungen

Für 3 802.11ac-Aufnahmen mit räumlichem Datenstrom (3SS) können Sie die nativen Sniffing-Funktionen eines 2014-Modells MacBook Pro oder höher mit Mac OS X 10.10.x oder höher verwenden. Wenn Sie ein 802.11ac-Client-Gerät mit zwei Signalströmen zur Fehlerbehebung verwenden, können Sie auch ein MacBook Air für 802.11ac-Aufnahmen verwenden. Das Air-Modell von MacBooks verwendet 2SS nur WLAN-Chipsätze derzeit zum Zeitpunkt dieser Veröffentlichung. Anweisungen zum Sammeln von OTA-Paketerfassungen unter Verwendung von Mac OS X finden Sie im folgenden Artikel in den Cisco Support-Foren. Hierbei stehen verschiedene Methoden zur Verfügung:

Wireless-Sniffing mit Mac OS X 10.6+

Sie können auch einen Access Point der Serien 2702/2802/3702/3802 oder einen ähnlichen Access Point im Sniffer-Modus verwenden, um eine ordnungsgemäße 802.11ac-Paketerfassung mit 3SS zu erfassen. Eine aktuelle Liste der verfügbaren 802.11ac Wireless-Adapter finden Sie in der aufgeführten Ressource. Einige davon können potenziell mit gängigen Tools wie OmniPeek und anderen verwendet werden, um eine 802.11ac-Paketerfassung zu erfassen (Chipsätze von Ralink, Atheros, ...):

https://wikidevi.com/wiki/List_of_802.11ac_Hardware#Wireless_adapters

Sie können auch einen Access Point der Serien 2702/2802/3702/3802 oder einen ähnlichen Access Point im Sniffer-Modus verwenden, um eine ordnungsgemäße 802.11ac-Paketerfassung mit 3SS zu erfassen. Schrittweise Anleitungen zur Konfiguration eines Cisco AP im Sniffer-Modus und zum Erfassen von OTA-Paketen finden Sie im folgenden Artikel in den Cisco Support-Foren:

Cisco AP im Sniffer-Modus

Bei der Fehlerbehebung von Roaming-Szenarien mit einem Wireless-Client-Gerät besteht die allgemeine Herausforderung darin, eine OTA-Paketerfassung über mehrere Kanäle effektiv zu erfassen. Diese Methode zur gleichzeitigen Überwachung mehrerer 802.11-Kanäle wird durch die Erfassung aggregierter OTA-Pakete erreicht. Es wird empfohlen, mehrere, kompatible 802.11ac-fähige USB-WLAN-Adapter mit einer kompatiblen Netzwerkanalysesoftware zu verwenden, um dieses Ziel zu erreichen. Zu den gängigen 802.11ac-fähigen USB-WLAN-Adaptern gehören der Savvius WiFI-Adapter für OmniPeek (802.11ac), Netgear A6210 oder Ähnliches.

X. Zusammenfassung

Im Folgenden finden Sie eine kurze Zusammenfassung der Informationen, die erfasst werden müssen, um ein potenzielles Problem der Interoperabilität von Wireless-Clients mit einem CUWN effektiv zu beheben. Dieser Abschnitt soll bei Bedarf als Kurzreferenz dienen.

I. Problemdefinition

- Ist das Problem auf ein bestimmtes Access Point- und/oder Funkmodell (2,4 GHz gegenüber 5 GHz) beschränkt?
- Wird das Problem nur bei bestimmten Versionen der Wireless LAN Controller (WLC)-Software festgestellt?
- Tritt das Problem nur bei bestimmten Versionen von Clienttyp(en) und/oder Software auf (Betriebssystemversion, WLAN-Treiberversion,...)
- Gibt es andere Wireless-Geräte, bei denen dieses Problem nicht auftritt? Wenn ja, welche?
- Ist das Problem reproduzierbar, wenn der Client mit einer offenen SSID verbunden ist, eine Kanalbreite von 20 MHz aufweist und 802.11ac deaktiviert ist? (Tritt das Problem nur im 11n-Modus und im 11ac-Modus auf?)
- Wenn das Problem bei einer offenen SSID nicht reproduzierbar ist, welche Mindestsicherheitskonfiguration ist für das Problem erforderlich? (PSK oder 802.1X im WLAN)
- Wie lauteten die vorherigen zweifelsfrei funktionierenden Konfigurations- und Softwareversionen?

II. WLC-Konfiguration und Protokolle

Wählen Sie dies aus der CLI der entsprechenden WLC:

- Konfiguration Paging deaktivieren
- show run-config

Alternativ können Sie auch nur diese Ausgaben nach Bedarf sammeln:

- Konfiguration Paging deaktivieren
- show run-config no-ap
- WLAN-Gruppen anzeigen

Sicherung der WLC-Konfiguration über TFTP, FTP,...(GUI: **Befehle > Datei hochladen > Konfiguration**)

Syslogs vom WLC

III. Informationen zu Client-Geräten

- Client-Typ (Tablet, Smartphone, Notebook, ...)
- Gerätehersteller und -modell
- Betriebssystemversion
- WLAN-Adaptermodell
- Treiberversion des WLAN-Adapters
- Verwendete Komponente (Windows Zero Config/Auto Config, Intel PROSet, ...)
- Für die Verwendung durch den Wireless-Client und das WLAN konfigurierte Sicherheit (offen, PSK, EAP-PEAP/MSCHAPv2,...)

  Hinweis: Client-Parameter, die sich gegenüber den vom jeweiligen Anbieter bereitgestellten Standardeinstellungen geändert haben. (Ruhezustand, Roaming-Parameter, U-APSD,...)

IV. Diagramm der Netzwerktopologie

Dies beinhaltet eine Darstellung und/oder Details bezüglich der drahtlosen Geräte im Netzwerk (Drucker/Scanner, WLCs,...)

V. Erstellen Sie eine Tabelle, um alle Client-Probleme aufzuzeichnen.

Beispiel:

MAC-Adresse	Benutzername	Beschreibung des gemeldeten Symptoms	Zeitpunkt, zu dem der Endbenutzer das Symptom beobachtet hat	Ping für Standardgateway J/N	WiFi-Signalstatus (Verbunden/Verbindungsvers

Ziel dieser Übung ist es, ein gemeinsames Muster zu identifizieren und ein genaueres Bild der aktuellen Probleme zu vermitteln.

VI. Befehle auf dem WLC anzeigen und debuggen

Erfassen Sie die folgenden WLC-Fehlerbehebungen über die CLI:

- **Konfigurationssitzungs-Timeout 0**
- **debug client <MAC_Adresse>**
- **debug dhcp message enable**

Fügen Sie die zusätzlichen Fehlerbehebungen auf Einzelfallbasis hinzu:

- **debug aaa detail enable** - Verwenden Sie diese Option, wenn Probleme mit der Authentifizierung beim AAA-Server auftreten.
- **debug aaa events enable** - Verwenden Sie diese Option, wenn Authentifizierungsprobleme mit dem AAA-Server auftreten
- **debug aaa all enable** - Verwenden Sie diese Einstellung für Authentifizierungsprobleme. Verwenden Sie sie daher nur bei Bedarf (bei AAA-Überschreibungsfällen und Ähnlichem).
- **debug mobility handoff** - Verwendung bei Roaming-Problemen zwischen WLCs

Erfassen Sie die Ausgabe für die WLC-Befehle show über die CLI:

- **Konfiguration Paging deaktivieren**
- **show time**
- **show client detail <MAC-Adresse des Clients>** (beachten Sie den Client-Status auf dem WLC)
- Pingen des Clients vom WLC

Wenn der Test abgeschlossen ist, beenden Sie mit diesem Befehl alle aktuellen Debugging-Vorgänge auf dem WLC:

- **debug disable-all**

VII. Befehle auf dem Access Point anzeigen und debuggen

Leichte Cisco IOS® APs

In diesem Abschnitt werden die für die Access Points der Serien 1700/2700/3700 oder frühere Modelle erforderlichen Fehlerbehebungen beschrieben.

Verwenden Sie die folgenden Befehle, um ein Zeitlimit für AP-Sitzungen während einer Telnet-/SSH-/Konsolensitzung zu vermeiden:

- debug capwap console cli
- config t
- line console 0 — zur Änderung der Timeout-Parameter für serielle Sitzungen
- line vty 0 4 — zum Ändern der Timeout-Parameter für Telnet-/SSH-Sitzungen
- exec-timeout 0
- Sitzungs-Timeout 0
- term len 0

Bevor Sie mit dem Test beginnen, sammeln Sie ein Beispiel dieser Befehle zum Anzeigen des Access Points. Erfassen Sie mindestens zwei Beispiele für diese Ausgabe, und zwar sowohl vor als auch nach Abschluss der Tests mithilfe der folgenden AP-show-Befehle über die CLI:

- term len 0
- Uhr anzeigen
- Showtech
- show capwap client mn
- show int do1 dfs
- show logging
- mehr event.log
- show trace dot11_rst Anzeigezeitformat lokal
- show trace dot11_rst
- show trace dot11_bcn Anzeigezeitformat lokal
- trace dot11_bcn anzeigen

Sammeln Sie diese AP-Debug-Meldungen über die CLI:

- debug dot11 { d0 | d1 } Monitoradresse <MAC_Adresse>
- debug dot11 { d0 | d1 } trace print clients mgmt keys rxev txev rcv xmt txfail ba
- Laufzeit

Wenn der Test abgeschlossen ist, können Sie die Fehlersuche mit dem folgenden Befehl deaktivieren:

- u all

AP-COS-APs

In diesem Abschnitt werden die für die Access Points der Serien 1800/2800/3800 erforderlichen Debugging-Aufgaben beschrieben.

Verwenden Sie die folgenden Befehle, um ein Zeitlimit für AP-Sitzungen während einer Telnet-/SSH-/Konsolensitzung zu vermeiden:

- exec-timeout 0

Bevor Sie mit dem Test beginnen, sammeln Sie ein Beispiel der Befehle zum Anzeigen des Access Points. Erfassen Sie mindestens zwei Beispiele für diese Ausgabe, und zwar sowohl vor

als auch nach Abschluss der Tests mithilfe der folgenden AP-show-Befehle über die CLI:

- **term len 0**
- **Uhr anzeigen**
- **Showtech**
- **Client-Statistiken anzeigen <client_MAC-address>**
- **NSS-Status anzeigen**
- **NSS-Statistiken anzeigen**
- **show log**

Erfassen Sie für Access Points der Serie 1800 die folgenden AP-Fehlerbehebungen über die CLI:

- **debug dot11, Ereignisadresse auf Clientebene <client_MAC-address>**
- **debug dot11 client level errors addr <client_MAC-address>**
- **debug dot11 client level critical addr <client_MAC-address>**
- **debug dot11 Info-Adresse auf Client-Ebene <client_MAC-address>**
- **debug dot11 client datapath eapol addr <client_MAC-address>**
- **debug dot11 client datapath dhcp addr <client_MAC-address>**
- **debug dot11 client datapath arp addr <client_MAC-address>**
- **Laufzeit**

Erfassen Sie für Access Points der Serien 2800/3800 die folgenden AP-Fehlerbehebungen über die CLI:

- **config ap client-trace address add <client_MAC-Adresse>**
- **config ap client-trace filter all enable**
- **config ap client-trace output console-log enable**
- **config ap client-trace start**
- **Laufzeit**

Wenn der Test abgeschlossen ist, können Sie die Fehlersuche mit dem folgenden Befehl deaktivieren:

- **config ap client-trace stop**

VIII. Kundenseitige Aufnahmen

Sammeln Sie entweder eine Promiscuous Netmon 3.4 (nur Windows XP oder 7)- oder Wireshark-Paketerfassung vom WLAN-Adapter des Client-Geräts.

IX. OTA-Erfassungen

802.11n-Erfassungen

- AirPCAP mit Wireshark
- MacBook Pro
- OmniPeek Professional, Enterprise, ...
- OmniPeek Remote Assistant (ORA)
- Cisco AP im Sniffer-Modus

802.11ac-Erfassungen

- Für 11ac 3SS-Aufnahmen können Sie ein 2014 Macbook Pro oder höher mit 10.10.x oder höher verwenden (verwenden Sie nicht MacBook Air für 11ac-Aufnahmen, wenn möglich, da es derzeit nur ein 2SS-Gerät ist).
- Sie können auch einen 2702, 3702 oder einen ähnlichen Cisco AP im Sniffer-Modus verwenden.
- Für Roaming-Szenarien und unter Verwendung professioneller Netzwerkanalysesoftware wie OmniPeek von Savvius. Es wird empfohlen, mehrere kompatible 802.11ac-fähige USB-WLAN-Adapter zu verwenden, z. B. den Savvius WiFI-Adapter für OmniPeek (802.11ac), Netgear A6210 oder Ähnliches.

XI. Anhang A - Zusätzliche Tipps und Tricks

Windows

Um einige zusätzliche Informationen in Bezug auf die aktuelle Wireless-Verbindung und andere verwandte Details direkt von einem Windows-PC zu sammeln. Sie können die folgenden netsh wlan-bezogenen Befehle in der Windows-Befehlszeile (CMD) verwenden:

```
C:\Users\engineer>netsh wlan show ?
These commands are available:
Commands in this context:
show all       - Shows complete wireless device and networks information.
show allowexplicitcreds - Shows the allow shared user credentials settings.
show autoconfig - Shows whether the auto configuration logic is enabled or
                  disabled.
show blockednetworks - Shows the blocked network display settings.
show createalluserprofile - Shows whether everyone is allowed to create all
                  user profiles.
show drivers   - Shows properties of the wireless LAN drivers on the system.
show filters   - Shows the allowed and blocked network list.
show hostednetwork - Show hosted network properties and status.
show interfaces - Shows a list of the wireless LAN interfaces on
                  the system.
show networks  - Shows a list of networks visible on the system.
show onlyUseGPProfilesforAllowedNetworks - Shows the only use GP profiles on GP
configured networks setting.
show profiles  - Shows a list of profiles configured on the system.
show settings  - Shows the global settings of wireless LAN.
show tracing   - Shows whether wireless LAN tracing is enabled or disabled.



C:\Users\engineer>netsh wlan show interfaces
There are 3 interfaces on the system:

    Name                   : Wireless Network Connection 8
    Description            : WildPackets Conceptronic Nano Wireless 150Mbps USB
Adapter #5
    GUID                   : 6beec9b0-9929-4bb4-aef8-0809ce01843e
    Physical address       : c8:d7:19:34:d5:85
    State                  : disconnected

    Name                   : Wireless Network Connection 4
    Description            : WildPackets Conceptronic Nano Wireless 150Mbps USB
Adapter
    GUID                   : 23aa09d4-c828-4184-965f-4e30f27ba359
    Physical address       : 48:f8:b3:b7:02:6e
    State                  : disconnected
```

```
    Name                   : Wireless Network Connection
    Description            : Intel(R) Centrino(R) Advanced-N 6200 AGN
    GUID                   : 8fa038f8-74e0-4167-98f9-de0943f0096c
    Physical address       : 58:94:6b:3e:a1:d0
    State                  : connected
    SSID                   : snowstorm
    BSSID                  : 00:3a:9a:e6:28:af
    Network type           : Infrastructure
    Radio type             : 802.11n
    Authentication         : WPA2-Enterprise
    Cipher                 : CCMP
    Connection mode        : Profile
    Channel                : 157
    Receive rate (Mbps)    : 300
    Transmit rate (Mbps)   : 300
    Signal                 : 80%
    Profile                : snowstorm

    Hosted network status  : Not started


C:\Users\engineer>netsh wlan show networks bssid | more

Interface name : Wireless Network Connection
There are 21 networks currently visible.

SSID 1 : snowstorm
    Network type            : Infrastructure
    Authentication          : WPA2-Enterprise
    Encryption              : CCMP
    BSSID 1                 : 00:3a:9a:e6:28:af
         Signal             : 99%
         Radio type         : 802.11n
         Channel            : 157
         Basic rates (Mbps) : 24 39 156
         Other rates (Mbps) : 18 19.5 36 48 54
    BSSID 2                 : 00:3a:9a:e6:28:a0
         Signal             : 91%
         Radio type         : 802.11n
         Channel            : 6
         Basic rates (Mbps) : 1 2
         Other rates (Mbps) : 5.5 6 9 11 12 18 24 36 48 54

-- More  --
```

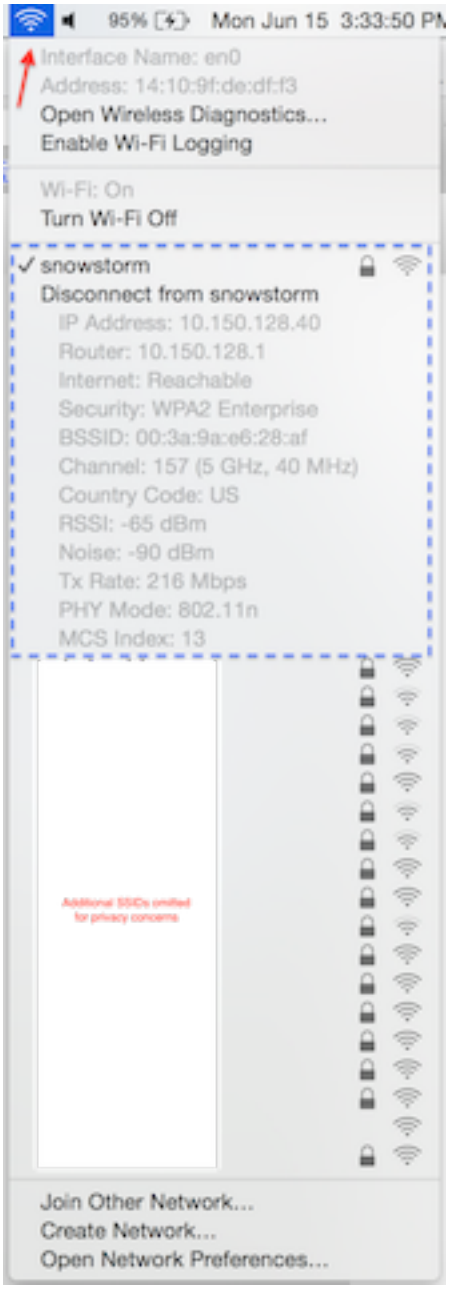
macOS (ehemals OS X)

Um die entsprechende Ausgabe als **ipconfig /all-**Befehl auf einem Windows-PC zu sammeln, können Sie stattdessen den gemeinsamen Linux/Unix-Befehl von **ifconfig** verwenden, um detaillierte Informationen zu allen Netzwerkschnittstellen auf einem Apple MacBook aufzulisten. Bei Bedarf können Sie auch festlegen, dass die Ausgabe nur für die native Wireless-Schnittstelle für ein bestimmtes MacBook (entweder en0 oder en1, es hängt vom Modell) zu empfangen. Beispiel:

```
bash-3.2$ ifconfig en0
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
ether 14:10:9f:de:df:f3
inet6 fe80::1610:9fff:fede:dff3%en0 prefixlen 64 scopeid 0x4
inet 10.150.128.40 netmask 0xffffe000 broadcast 10.150.159.255
nd6 options=1<PERFORMNUD>
```

```
media: autoselect
status: active
```

Um einige schnelle, aber detaillierte Informationen über die aktuelle Wireless-Verbindung auf einem MacBook zu erhalten. Sie können auch das WiFi-Symbol in der oberen rechten Ecke des Desktops auswählen, während Sie gleichzeitig die **Optionsschaltfläche** auf Ihrer Tastatur gedrückt halten, wie im Bild gezeigt.



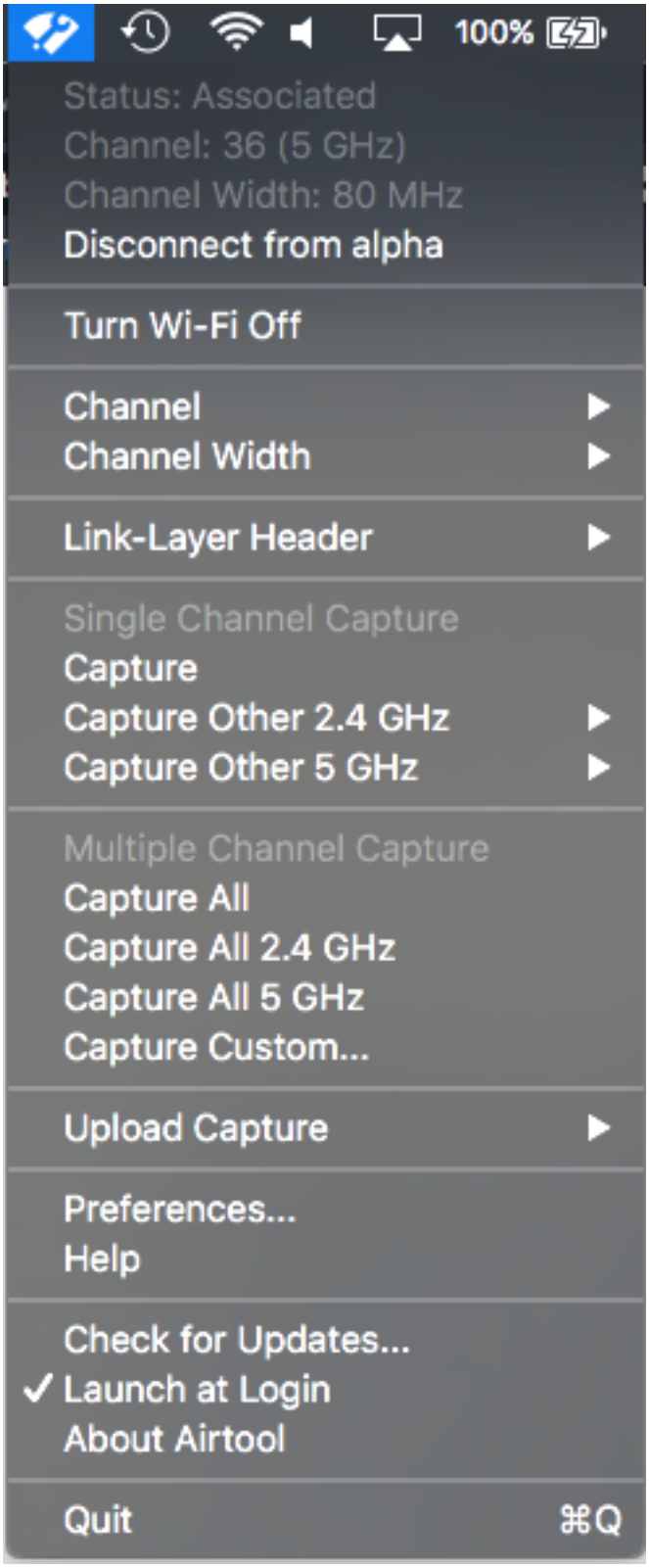
Eine weitere nützliche Option ist die Verwendung des versteckten Befehlszeilen-Dienstprogramms airport. Es wird dringend empfohlen, dieses nur mit Ihrem eigenen MacBook oder einem in einer Laborumgebung verwendeten MacBook zu verwenden. Da einige Netzwerkadministratoren möglicherweise keinen Zugriff auf dieses Dienstprogramm auf dem MacBook eines Endbenutzers gewähren möchten, sollten Sie entsprechend vorsichtig sein. Um fortzufahren, geben Sie dies in Terminal auf dem MacBook in Frage:

```
sudo ln -s
/System/Library/PrivateFrameworks/Apple80211.framework/Versions/Current/Resources/airport
/usr/local/bin/airport
```

Jetzt können Sie das CLI-Dienstprogramm des Flughafens ganz einfach aufrufen. Ein Beispiel hierfür ist:

```
bash-3.2$ airport -I
     agrCtlRSSI: -61
     agrExtRSSI: 0
    agrCtlNoise: -90
    agrExtNoise: 0
          state: running
        op mode: station
     lastTxRate: 216
        maxRate: 300
lastAssocStatus: 0
    802.11 auth: open
      link auth: wpa2
          BSSID: 0:3a:9a:e6:28:af
           SSID: snowstorm
            MCS: 13
        channel: 157,1
```

Um den Prozess weiter zu vereinfachen, um eine zuverlässige, einzelne 802.11-Kanal-OTA-Paketerfassung unter Verwendung der Funktionen eines MacBook Pro oder dergleichen zu sammeln. Sie können entweder die integrierten Funktionen in macOS mit der Wireless Diagnostics > Sniffer-Methode oder ähnlich wie zuvor beschrieben nutzen, aber optional können Sie auch ein Dienstprogramm eines Drittanbieters namens Airtool (OS X 10.8 und höher) verwenden. Der Vorteil ist eine einfache Schnittstelle, um schnell eine OTA-Paketerfassung zu sammeln, die direkt auf dem Desktop mit nur wenigen Klicks über die App-UI direkt von der oberen Menüleiste auf Ihrem Bildschirm gespeichert wird.



Weitere Informationen und Download-Links zu Airtool finden Sie unter folgender URL:

https://www.adriangranados.com/apps/airtool

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.