# Problemen met draadloze clientinteroperabiliteit met CUWN oplossen

## Inhoud

# Inleiding

Dit document beschrijft interoperabiliteitsproblemen wanneer deze zich voordoen met de Cisco Unified Wireless Network (CUWN)-oplossing.

# Voorwaarden

## Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco draadloze AP's
- Draadloze LAN-controllers (WLC)
- Verwante netwerkapparaten

## Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

> **Opmerking**: de doelgroep voor dit document zijn ervaren draadloze netwerkengineers en beheerders die al bekend zijn met het gebruik, de configuratie en de probleemoplossing van deze onderwerpen.

# Achtergrondinformatie

Het kan algemeen zijn om te vinden dat gegeven de verschillende client-apparaten die zowel bestaan als verder worden ontwikkeld. Een verscheidenheid van kwesties kan zich voordoen met betrekking tot het vestigen, handhaven, of eenvoudig om het meeste uit hun verbinding aan het draadloze netwerk en infrastructuur te krijgen te steunen.

Dit kan vaak neerkomen op een eenvoudige configuratiekwestie van de kant van het clientapparaat en/of de draadloze infrastructuur zelf. In sommige gevallen kan dit echter worden

toegeschreven aan een interoperabiliteitsprobleem met betrekking tot een specifiek clientapparaat en componenten die dit ondersteunen (supplicant, WLAN-adapter, draadloos stuurprogramma,...) en/of de betreffende AP's. Als draadloze engineers vormen zulke interoperabiliteitsproblemen een kans om potentieel complexe uitdagingen te identificeren, op te lossen en op te lossen.

Dit document beschrijft in detail welke informatie aanvankelijk moet worden verzameld om dergelijke draadloze interoperabiliteitsproblemen effectief te onderzoeken en op te lossen wanneer ze zich voordoen met de Unified Wireless Network (CUWN)-oplossing (Cisco Unified Wireless Network). De behoefte aan een dergelijke uitgebreide benadering wordt steeds belangrijker met de steeds grotere aantallen en combinaties van draadloze clientapparaten en access point (AP)-radio's.Aanvullende informatie over wat in dit artikel wordt geschetst, kan worden gevraagd en moet per geval worden verzameld, gezien het onbeperkte aantal variabelen dat dergelijke vereisten zou kunnen dicteren. De hier gedetailleerde informatie is echter een generieke richtlijn voor het aanpakken van eventuele problemen met de interoperabiliteit van draadloze clients.

# I. Probleemdefinitie

De eerste stap om elk probleem effectief aan te pakken met de bedoeling om vastberaden te worden, is het nauwkeurig definiëren van de kwestie in kwestie. Om dit te doen, moet u ervoor zorgen dat ten minste deze vragen worden gesteld en dat hun antwoorden duidelijk worden gedocumenteerd:

- Is de kwestie beperkt tot een specifiek model van AP's en/of radiotype (2,4 GHz versus 5 GHz)?
- Wordt de kwestie alleen waargenomen bij specifieke versie(s) van WLC-software?
- Is het probleem ondervonden met alleen specifieke versie(s) van clienttype(s) en/of software (OS-versie, WLAN-driver-versie,...)
- Zijn er nog andere draadloze apparaten die dit probleem niet ervaren? Zo ja, welke?
- Is het probleem reproduceerbaar terwijl de client is verbonden met een vereenvoudigde draadloze installatie zoals een open SSID, met een kanaalbreedte van 20 MHz en 802.11ac uitgeschakeld? (d.w.z. vindt het probleem alleen plaats in de 802.11n-modus versus de 802.11ac-modus?).
- Als de kwestie niet reproduceerbaar met open SSID is, bij welke minimumveiligheidsconfiguratie wordt de kwestie gezien? (PSK of 802.1X op het WLAN).
- Wat waren de vorige best bekende configuratie- en softwareversies?

# II. WLC-configuratie en algemene logbestanden

## Run-Config

Zonder uitzondering is het absoluut noodzakelijk om de WLC-configuratie te verzamelen voor een gedetailleerd overzicht van de functies die door de klant worden gebruikt, hun specifieke setup en andere dergelijke details. Om dit te doen, moet u een Telnet/SSH-sessie instellen voor de WLC(s) in kwestie en de uitvoer van deze CLI-opdrachten opslaan in een tekstbestand:

```
config paging disable

show run-config
```

De volledige run-config uitvoer heeft altijd de voorkeur, aangezien het gedetailleerde informatie met betrekking tot aangesloten APs en bijbehorende RF informatie omvat. In sommige gevallen en situaties, zoals wanneer u aanvankelijk met een WLC met een groot aantal APs werkt aangesloten bij (8510 WLC met 2500+ APs). Het kan de voorkeur hebben om in eerste instantie alleen de configuratie van de WLC te verzamelen zonder dergelijke AP-informatie voor een snelle beoordeling, aangezien de volledige show run-config 30 minuten of meer zou kunnen duren om het gegeven aantal AP's te voltooien. Het kan echter nog nodig zijn om de volledige run-config uitvoer op een later tijdstip te verzamelen.

Hiervoor kunt u de uitvoer van deze CLI-opdrachten naar een tekstbestand optioneel verzamelen:

```
config paging disable

show run-config no-ap

show wlan apgroups
```

## WLC-configuratiebestand

Naast de **show run-config** of **show run-config no-ap** output, is het ook aanbevolen om een volledige back-up van de WLC-configuratie te verzamelen. Dit is een hulpmiddel wanneer een lab opnieuw moet worden uitgevoerd door zowel TAC/HTTS als BU Escalation, om het probleem te proberen en te reproduceren in een Cisco lab-omgeving. Een back-up van de WLC kan worden verzameld via de GUI of de CLI van de WLC in kwestie, met het gebruik van ofwel TFTP of FTP om het configuratiebestand op te slaan naar de externe TFTP/FTP server. Dit voorbeeld toont het gebruik van zowel de GUI als CLI om een back-up van de WLC op te slaan, met behulp van TFTP:

### GUI

**Opdrachten > Bestand uploaden > Configuratie > Upload** zoals in de afbeelding.


### 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 van WLC

Op dit moment, wilt u ook de huidige logboeken van de WLC verzamelen voor extra review zoals nodig. Idealiter verzamelt u deze logbestanden direct na uw test met een draadloze client waarbij het gemelde probleem wordt gereproduceerd. Als de klant de WLC-logbestanden exporteert naar

een externe syslog-server, dan wilt u ze daar ophalen. Anders kunt u de msglog en traplog die momenteel lokaal op de WLC zijn opgeslagen opslaan door deze CLI-sessie-uitvoer naar een ander tekstbestand op te slaan:

```
config paging disable

show msglog

show traplog
```

# III. Apparaatgegevens en -informatie van client

De volgende stap is om zoveel informatie en specificaties te verzamelen met betrekking tot de gebruikte client(s) die een potentieel draadloos interoperabiliteitsprobleem ervaren. Deze informatie omvat, maar is niet noodzakelijkerwijs beperkt tot:

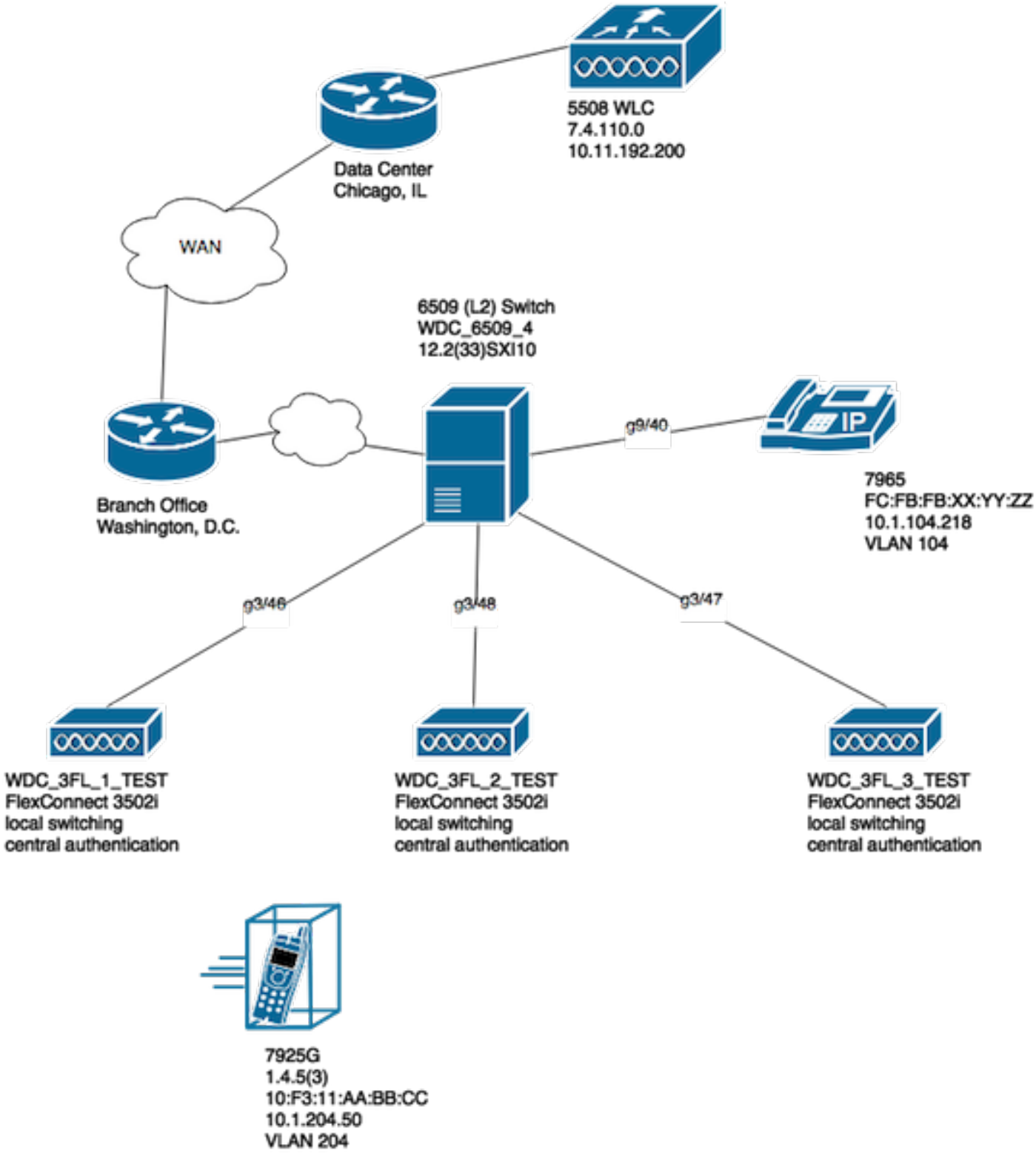
- Clienttype (tablet, smartphone, notebook-pc,...)
- Merk en model apparaat
- Versie besturingssysteem
- WLAN-adaptermodel
- Versie WLAN-adapterstuurprogramma
- Gebruikte supervisor (Windows Zero Config / Auto Config, Intel PROSet,...)
- Beveiliging geconfigureerd voor gebruik door de draadloze client en WLAN (Open, PSK, EAP-PEAP/MSCHAPv2,...)
- Noteer de clientparameters die zijn gewijzigd ten opzichte van de standaardinstellingen die door de betreffende verkoper zijn opgegeven (slaapstand, roaming-parameters, U-APSD,...).

Opmerking: alle aanvullende informatie of opmerkingen met betrekking tot het clientapparaat of de clientapparaten tot welke screenshots van de WLAN-gerelateerde configuratie(s) bevat, enzovoort, moeten ook worden opgenomen als dat nodig is.

# IV. Netwerktopologie

Om het oplossen van problemen en het proces van de Analyse van de Oorzaak van de Wortel verder te bespoedigen (RCA), wordt het altijd geadviseerd om een gedetailleerd en grondig diagram van de netwerktopologie te verstrekken. Het diagram van de netwerktopologie moet niet alleen gegevens over het netwerk en de draadloze infrastructuur bevatten, maar ook inzicht bieden in het (de) draadloze apparaat(apparaten) in kwestie dat (die) binnen het netwerk (printers/scanners) werkt (werken), welke client-VLAN’s in gebruik zijn,...) en hun locatie(s) ten opzichte van elkaar.

Een aantal gereedschappen (Microsoft Visio, trekking.io,...) en een verscheidenheid aan stijlen kunnen worden gebruikt om zo'n netwerkdiagram te maken. Belangrijk is alleen dat de juiste informatie duidelijk wordt weergegeven in het schema dat door alle betrokken partijen en verkopers wordt gecontroleerd. Een voorbeeldnetwerktopologie die basisinformatie, maar nuttige informatie met betrekking tot zowel de infrastructuur als de clientapparaten zoals in de afbeelding weergeeft.




## V. Aanvullende gegevens en de specificaties volgen

Om ervoor te zorgen dat de juiste informatie wordt verzameld op het moment van een test met de clientapparatuur(en) waarmee eindgebruikers problemen ondervinden. Het wordt aanbevolen om vooraf een spreadsheet of vergelijkbaar te maken om alle cliëntproblemen en gerelateerde details die op het moment van de test zijn waargenomen, zoals in dit voorbeeld, te registreren:

| MAC-adres | Username | Beschrijving van het gemelde symptoom | Waargenomen symptoom door eindgebruiker | Standaard gateway Y/N pingen | WiFi-signaalstatus (verbonden/proberen verbinding te maken) | Reco equiv |
|---|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| xxyy.abb.0011 test_gebruiker1 | Maakt af en toe de verbinding met het toegangspunt los. | Verloren netwerkconnectiviteit en draadloze associatie van AP3. | N | Proberen verbinding te maken | ifcon<br>en0: f<br>BRO/<br>SIMP<br>1500<br>eth<br>inet<br>fe80:8<br>prefix<br>0x4<br>inet<br>0xffff(<br>192.1<br>nd6<br>DAD><br>me<br>stat |

Het doel van deze oefening is om te helpen bij het documenteren en bepalen van een gemeenschappelijk belangenpatroon, en om een accuraat beeld te krijgen van de kwestie(n) in kwestie. Zodra deze spreadsheet is voorbereid om te worden gebruikt voor het verzamelen van gegevens, bent u nu klaar om te beginnen met uw tests. Enkele aanvullende, maar belangrijke overwegingen zijn:

**Opmerking**: alle debugs- en pakketopnamen moeten gesynchroniseerd worden naar dezelfde NTP-server voor een eenvoudiger correlatie met de logbestanden en moeten op hetzelfde moment genomen worden voor een bepaalde test.

**Opmerking**: Geef een nauwkeurige tijdstempel van wanneer de uitgifte is waargenomen en wanneer de uitgifte lijkt te herstellen (indien van toepassing).

**Opmerking**: verzamel altijd debugs gefilterd per client MAC-adres op zowel de AP als WLC.

**Opmerking**: voer de opdrachten tonen en debuggen op het toegangspunt niet uit binnen dezelfde Telnet/SSH/console-sessie, deze worden afzonderlijk in een andere sessie uitgevoerd.

**Opmerking**: AP-debugs worden bij voorkeur genomen op Telnet/SSH versus Console, omdat de console meestal te langzaam is om effectief te zijn.

# VI. WLC - Opdrachten weergeven en debuggen

Wanneer tests worden uitgevoerd om potentiële problemen met de interoperabiliteit van draadloze clients te reproduceren en op te lossen, is het noodzakelijk dat debugs en extra logbestanden worden verzameld van de draadloze infrastructuur die in gebruik is. Deze twee secties kunnen de specifieke logbestanden in detail uitleggen en de eerste debug-uitvoer die respectievelijk van de WLC en de AP(s) wordt verzameld.

### WLC-debugopdrachten

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

Met betrekking tot de aard van het probleem in kwestie, kunt u deze WLC debugs ook op een case-by-case basis toevoegen:

- **debug aaa detail enable** - gebruik dit als er authenticatie gerelateerde problemen zijn met de AAA server
- **debug aaa events enabled** - gebruik dit als er authenticatie gerelateerde problemen zijn met de AAA server
- **debug aaa all enable** - gebruik dit voor auth issues; de output voor deze debug is breedsprakig dus gebruik het alleen wanneer absoluut nodig (voor AAA override cases,...)
- **debug mobility handoff** - gebruik wanneer er roaming problemen zijn tussen WLC's

Zodra het probleem met de betreffende draadloze client is gereproduceerd en alle informatie die in de secties voor en na deze is beschreven, is verzameld en gedocumenteerd. Om deze CLI-opdrachten uit te voeren, moet u de debugs in de WLC uitschakelen.

```
debug disable-all
```

### WLC-opdrachten weergeven

```
config paging disable

show time

show client detail <MAC_address>

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

Zoals eerder vermeld, zorg ervoor dat de WLC debugs in één Telnet/SSH sessie uitvoert en verzamel de uitvoer voor deze showopdrachten in een ander Telnet/SSH naar de WLC. U moet hetzelfde doen om de debugs van het toegangspunt te verzamelen en de uitvoer van opdrachten in deze sectie te tonen.

## VII. AP - Toon en zuiver Bevelen

### Lichtgewicht Cisco IOS® access points

Voordat u debugs start op lichtgewicht Cisco IOS® AP(s) die bij de test betrokken zijn, zoals de 2600, 2700, 3700 of eerdere model Cisco access points. U moet deze CLI-opdrachten eerst op het toegangspunt uitvoeren om een time-out te voorkomen tijdens een Telnet-/SSH-/consolesessie met de betreffende toegangspunt(en) wanneer uw client-test(s) wordt (worden) uitgevoerd:

```
debug capwap console cli

config t

line vty 0 4
```

```
exec-timeout 0

session-timeout 0
```

U kunt deze stappen ook volgen om de consoleverbinding te gebruiken en de verklaring **vty 0 4** te vervangen met **lijnconsole 0** in plaats daarvan, om de exec- en sessietime-outs voor een seriële/consoleverbinding dienovereenkomstig uit te schakelen.

- lijnconsole 0 - gebruik om seriële sessietime-outparameters aan te passen
- line vty 0.4 - gebruiken om de Time-outparameters van Telnet/SSH-sessies aan te passen

### Opdrachten weergeven AP

Alvorens u met de test begint, moet u eerst een steekproef van deze showbevelen op AP verzamelen. Verzamel de output van deze showbevelen minstens tweemaal voor elke test die de draadloze cliënt in kwestie impliceert; zowel vóór als na de test is volledig.

```
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 Opdrachten

Zodra u de eerste uitvoer van de bovengenoemde showopdrachten hebt verzameld, kunt u de debugs op hetzelfde access point nu inschakelen in een afzonderlijke Telnet/SSH-sessie zoals getoond. Zorg ervoor dat de gehele uitvoer in een tekstbestand wordt opgeslagen.

```
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
```

| Vlag | Beschrijving |
|---|---|
| d0 | 2,4 GHz radio (sleuf 0) |
| d1 | 5 GHz radio (sleuf 1) |
| beheer | Trace-beheerpakketten |

| | |
|---|---|
| ba | Informatie over Trace Block ACK |
| rcv | Ontvangen pakketten overtrekken |
| sleutels | Toetsen voor overtrekken |
| rxev | Gebeurtenissen traceren |
| taxivrij | Transmissie-gebeurtenissen overtrekken |
| belastingtarief | Overbrengen naar radio overtrekken |
| XMT | Transmissiepakketten overtrekken |
| belastingnalaten | Fouten bij overbrengen overtrekken |
| tarieven | Veranderingen in de traceringssnelheid |

Om de debugs op AP uit te schakelen zodra de test en de gegevensverzameling proces is voltooid, kunt u deze CLI opdracht op AP uitvoeren:

```
u all
```

## AP-COS access points

Voor 802.11ac-golf 2 geschikte access points en hoger, zoals de 1800, 2800 en 3800 model access points. Deze nieuwere model AP's introduceren een volledig nieuw besturingssysteem voor de access point platforms die AP-COS worden genoemd. Als zodanig zijn niet alle opdrachten zoals eerder gebruikt op de traditionele lichtgewicht op Cisco IOS® gebaseerde access points zoals eerder gedetailleerd nog van toepassing. Als bij het oplossen van een probleem sprake is van interoperabiliteitsproblemen met verschillende client-STA-apparaten en AP-COS-model-AP's, dan moet deze informatie worden verzameld bij de AP-COS access point(en) die betrokken zijn bij de equivalente test.

Voordat u debugs start op een AP-COS model AP(s) betrokken bij de test. U moet deze CLI-opdracht eerst op het toegangspunt uitvoeren om een time-out te voorkomen tijdens een Telnet-/SSH-/consolesessie met de betreffende toegangspunt(en) wanneer uw client-test(s):

```
exec-timeout 0
```

### AP-COS Toon opdrachten

Alvorens u met de test begint, moet u eerst een steekproef van deze showbevelen op AP verzamelen. Verzamel de output van deze showbevelen minstens tweemaal voor elke test die de draadloze cliënt in kwestie impliceert; zowel vóór als na de test is volledig.

```
term len 0

show clock show tech

show client statistics <client_MAC-address>

show cont nss status

show cont nss stats

show log
```

### 1800 reeks | Opdrachten voor debuggen van AP-COS

Deze debugs zijn specifiek voor de 18xx-serie access points. Dit is te wijten aan het feit dat de

chipset(s) die gebruikt worden voor de 1800-serie van AP's verschillen van die welke gevonden worden in de 2800/3800-serie access points, en daarom is in dit scenario een andere set van debugs vereist door vergelijking. Het corresponderende debug voor de 2800/3800-serie AP's wordt behandeld in de volgende paragraaf.

Nadat u de eerste uitvoer van de bovengenoemde showopdrachten hebt verzameld, moet u de debugs op hetzelfde 1800 access point(en) nu in een afzonderlijke Telnet/SSH-sessie inschakelen zoals aangegeven op de afbeelding. Zorg ervoor dat de gehele uitvoer in een tekstbestand wordt opgeslagen.

```
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 sommige gevallen moet u ook de aanvullende debugs op de 18xx AP inschakelen om problemen met de interoperabiliteit van de client verder op te lossen. Dit dient echter alleen te worden gedaan als/zoals gevraagd door een Cisco TAC-engineer voor een corresponderend serviceverzoek/case.

Aangezien extra debugs niet alleen veel uitgebreider zijn in hun output, maar ook extra belasting op de AP kunnen introduceren, vereist het extra tijd voor een goede analyse. Welke onder bepaalde omstandigheden de service mogelijk kan onderbreken, als veel clientapparaten proberen verbinding te maken met hetzelfde toegangspunt tijdens tests of vergelijkbare variabelen.

Om de debugs op het AP-COS variant access point uit te schakelen - of het nu op een 1800 of 2800/3800 Series AP is - kunt u deze CLI-opdracht uitvoeren op het AP, zodra het test- en gegevensverzamelingsproces is voltooid:

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

### 2800/3800 Series | Opdrachten voor debuggen van AP-COS

Nadat u de eerste uitvoer van de bovengenoemde showopdrachten hebt verzameld, moet u de debugs op dezelfde 2800/3800 access point(en) nu inschakelen in een afzonderlijke Telnet/SSH-sessie zoals aangegeven op de afbeelding. Zorg ervoor dat de gehele uitvoer in een tekstbestand wordt opgeslagen.

```
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
```

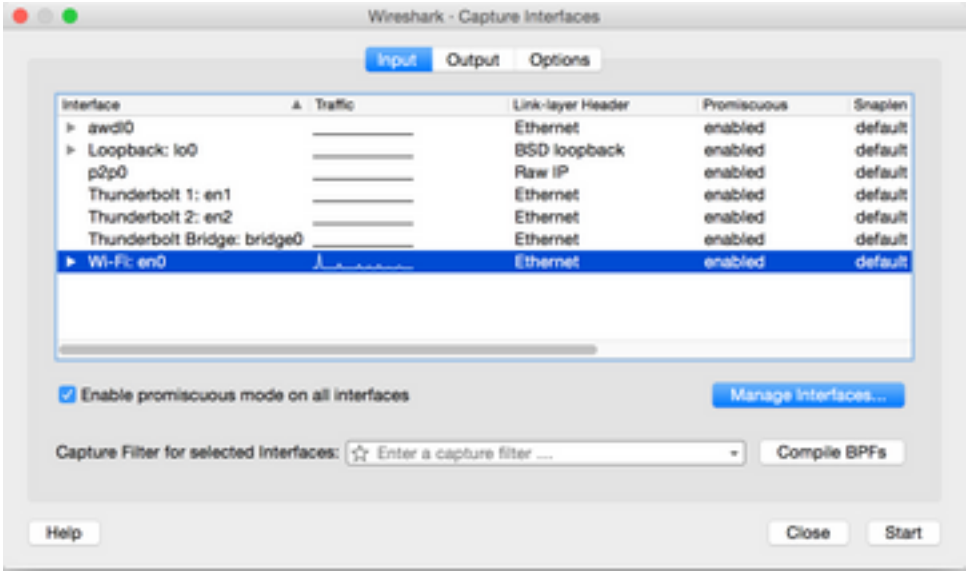
Om de debugs op de 1800/2800/3800 Series AP uit te schakelen zodra het test- en gegevensverzamelingsproces is voltooid, kunt u deze CLI-opdracht uitvoeren op het AP:

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

# VIII. pakketvastlegging aan clientzijde

Van het gebruikte clientapparaat als het een notebook-pc, MacBook of iets dergelijks is, moet u de pakketopname met promiscuous mode van de draadloze interface van het clientapparaat verzamelen dat wordt gebruikt om het probleem te reproduceren. Gemeenschappelijke hulpprogramma's zoals Netmon 3.4 (alleen Windows) of Wireshark kunnen eenvoudig worden gedownload en worden gebruikt om deze opname te verzamelen en op te slaan als een *.pcap-bestand. Het hangt van het apparaat af, er kunnen ook middelen zijn om een tcpdump of soortgelijk van de klant in kwestie te verzamelen, zodat u misschien moet raadplegen met de klant fabrikant van het apparaat voor hulp in dit verband.

Hier is een voorbeeld om een Wireshark opname te configureren voor de draadloze interface op een MacBook Pro:




Zoals met elke pakketopname, ongeacht welk hulpprogramma wordt gebruikt om het te verzamelen, zorg ervoor dat het bestand in een pcap-bestandsformaat wordt opgeslagen (*.pcap, *.pcapng, *.pkt,...). Dit om ervoor te zorgen dat niet alleen Cisco-engineers op elke afdeling de packet capture-bestanden eenvoudig kunnen bekijken, maar ook engineers van andere leveranciers en organisaties (Intel, Apple,...). Dit maakt een naadloos samenwerkings- en samenwerkingsproces mogelijk, waardoor zowel Cisco als de leverancier(s) van clientapparaten beter kunnen samenwerken om mogelijke interoperabiliteitsproblemen te onderzoeken en op te lossen.

# IX. Over-the-Air (OTA) pakketvastlegging

Om op een effectieve manier mogelijke of bestaande problemen met draadloze interoperabiliteit op te lossen, is het van cruciaal belang om een OTA-pakketopname van hoge kwaliteit van het probleem te verzamelen. Hierdoor is een gedetailleerde analyse mogelijk van de werkelijke 802.11 draadloze communicatie tussen de draadloze client- en access point radio(s) in kwestie, naast een verder perspectief voor de clientzijde en draadloze infrastructuur logbestanden, en debugs. Dit is

een cruciale stap die voor elke test van een potentieel draadloos interoperabiliteitsprobleem, zonder uitzondering, moet worden volbracht.

Echter, vaak is de eindklant niet goed uitgerust of voorbereid om OTA pakketopnamen te verzamelen. Dit is een veelvoorkomend obstakel waar draadloze engineers vaak mee te maken hebben en ze moeten samenwerken met de klant om dit op verschillende manieren te overwinnen. Dit artikel in de Cisco-ondersteuningsforums kan dienen als een goed startpunt om de klant te helpen begeleiden en te informeren over de volgende punten:

802.11 draadloze snuffeling/pakketopname

Het is van het grootste belang dat de OTA-pakketopname(en) in een pcap-bestandsformaat (*.pcap, *.pcapng, *.pkt,..) wordt verzameld en 802.11 metagegevens bevat (RSSI, kanaal, gegevenssnelheid,..). Het OTA-snuifje moet ook tijdens de test(s) te allen tijde dicht bij het desbetreffende cliëntapparaat worden gehouden om een nauwkeurig perspectief te waarborgen van het verkeer dat naar/van het geteste cliëntapparaat wordt verzonden en ontvangen.

> **Opmerking**: Als de test(s) in kwestie betrekking hebben op een client device roaming-scenario, waarbij meer dan één 802.11-kanaal moet worden bewaakt in een geaggregeerde pakketopname. Het is momenteel niet aan te raden om AirMagnet WiFi Analyzer te gebruiken van Fluke Networks.

De reden hiervoor is dat geaggregeerd pakketvastlegging met het gebruik van deze voorziening momenteel wordt opgeslagen in een bedrijfseigen bestandsindeling en niet in een pcap-stylesheet die gemakkelijk kan worden bekeken in Wireshark of andere soortgelijke hulpprogramma's. Zorg ervoor dat uw OTA-pakketvastlegging in een niet-bedrijfseigen bestandsindeling is, dit helpt ervoor te zorgen dat alle betrokken partijen en leveranciers alle opnamebestanden op elk moment gemakkelijk kunnen beoordelen en uiteindelijk kunnen helpen bij het versnellen van eventuele oplossingsinspanningen.

in een formaat dat leesbaar is door de huidige Wireshark, en dat 802.11 meta data (RSSI, kanaal, data rate) bevat - Zie meer op: https://supportforums.cisco.com/document/75331/80211-wireless-sniffing-packet-capture#sthash.Xhlx5LSS.dpuf
Hier zijn sommige gemeenschappelijke methodes om een OTA pakketopname te verzamelen:

- AirPCAP met draadloos
- MacBook Pro
- Lijst wordt bijgewerkt... Soortgelijke hotels
- OmniPeek Remote Assistant (ORA)
- Cisco AP in Sniffer modus

## 802.11n opnamen

Voor OTA-pakketopname waarbij 802.11n draadloze clients betrokken zijn, is er momenteel meer flexibiliteit en gebruiksgemak. Dit is te wijten aan een grotere verscheidenheid aan beschikbare draadloze USB WLAN-adapters die gemakkelijk kunnen worden gebruikt met een aantal tools, zoals OmniPeek en anderen.

Houd er rekening mee hoe de mogelijkheden van de specifieke draadloze adapter(s) die worden gebruikt voor het verzamelen van een 802.11n OTA-opname, kunnen worden vergeleken met de mogelijkheden van de werkelijke WLAN-chipset die wordt gebruikt door de clientapparaten die u

probeert op te lossen. Bijvoorbeeld, als het clientapparaat een potentieel draadloos interoperabiliteitsprobleem ondervindt dat een 2 spatial stream (2S) capabele 802.11n chipset gebruikt. Vervolgens wordt het ten zeerste aanbevolen om ervoor te zorgen dat de draadloze adapter die wordt gebruikt om een OTA-pakketopname te verzamelen ook een 2S of betere adapter is, met 802.11n of nieuwere specificaties.

### 802.11ac OTA-opnamen

Voor 3 spatial stream (3SS) opnamen van 802.11ac kunt u gebruik maken van de native snuffelmogelijkheden van een 2014 model MacBook Pro of later met Mac OS X 10.10.x of hoger. Als probleemoplossing een 2 spatial stream 802.11ac-clientapparaat is, kunt u ook een MacBook Air gebruiken voor 802.11ac opnamen. Het Air-model van MacBooks gebruikt momenteel alleen 2SS WLAN-chipsets op het moment van schrijven. U kunt het genoemde artikel van de de ondersteuningsforums van Cisco voor instructies op hoe te om OTA pakketopnamen met het gebruik van Mac OS X, door een verscheidenheid van methodes te verzamelen raadplegen:

Draadloos snuffelen met het gebruik van Mac OS X 10.6+

U kunt ook een 2702/2802/3702/3802 reeks of soortgelijke AP in snuffelmodus gebruiken om een juiste 802.11ac pakketopname met 3S te verzamelen. U kunt ook de vermelde bron raadplegen voor een huidige lijst met beschikbare draadloze 802.11ac-adapters. Sommige daarvan kunnen potentieel worden gebruikt met gangbare tools zoals OmniPeek en anderen om een 802.11ac pakketopname te verzamelen (chipsets van Ralink, Atheros,...):

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

U kunt ook een 2702/2802/3702/3802 reeks of soortgelijke AP in snuffelmodus gebruiken om een juiste 802.11ac pakketopname met 3S te verzamelen. Voor het gemak zijn stap-voor-stap instructies hoe u een Cisco AP in snuffelmodus kunt configureren en een OTA-pakketopname kunt verzamelen te vinden in het artikel over Cisco-ondersteuningsforums:

Cisco AP in Sniffer modus

Voor het oplossen van problemen roamende scenario's met een draadloos cliëntapparaat, is de gemeenschappelijke uitdaging effectief een OTA pakketopname over veelvoudige kanalen te verzamelen. Deze methode om gelijktijdig meerdere 802.11-kanalen te controleren wordt bereikt door de verzameling van geaggregeerde OTA-pakketvastlegging. Het wordt aanbevolen om hiervoor meerdere, compatibele 802.11ac-compatibele USB WLAN-adapters te gebruiken met een compatibele software voor netwerkanalyse. Enkele veelgebruikte 802.11ac-compatibele USB WLAN-adapters zijn de Savvius WiFi-adapter voor OmniPeek (802.11ac), Netgear A6210 of vergelijkbaar.

## X. Samenvatting

Hier is een korte samenvatting van de informatie die moet worden verzameld om effectief problemen op te lossen met een potentiële draadloze client interoperabiliteit probleem met een CUWN. Dit deel is bedoeld als een snelle referentiesectie, indien nodig.

### I. Probleemdefinitie

- Is de kwestie beperkt tot een specifiek model van toegangspunt(en) en/of radiotype (2,4 GHz

versus 5 GHz)?
- Wordt het probleem alleen waargenomen bij specifieke versie(s) van WLC-software (Wireless LAN controller)?
- Is het probleem ondervonden met alleen specifieke versie(s) van clienttype(s) en/of software (OS-versie, WLAN-driver-versie,...)
- Zijn er nog andere draadloze apparaten die dit probleem niet ervaren? Zo ja, welke?
- Is het probleem reproduceerbaar terwijl de client is verbonden met een open SSID, een kanaalbreedte van 20 MHz en 802.11ac uitgeschakeld? (Gebeurt het probleem alleen in de 11n-modus versus de 11ac-modus)
- Als de kwestie niet reproduceerbaar met open SSID is, bij welke minimumveiligheidsconfiguratie wordt de kwestie gezien? (PSK of 802.1X op het WLAN)
- Wat waren de vorige best bekende configuratie- en softwareversies?

## II. WLC-configuratie en -logbestanden

Verzamel dit van de CLI van de WLC(s) in kwestie:

- config paging uitschakelen
- toon in werking stellen-configureren

U kunt ook naar wens alleen deze uitvoer verzamelen:

- config paging uitschakelen
- toon in werking stellen-Config geen-app
- WLAN-groepen weergeven

Back-up van de WLC-configuratie via TFTP, FTP,...(GUI: **Opdrachten > Bestand uploaden > Configuratie**)

Syslogs van WLC

## III. Apparaatgegevens client

- Clienttype (tablet, smartphone, notebook-pc,...)
- Merk en model apparaat
- Versie besturingssysteem
- WLAN-adaptermodel
- Versie WLAN-adapterstuurprogramma
- Gebruikte supervisor (Windows Zero Config / Auto Config, Intel PROSet,...)
- Beveiliging geconfigureerd voor gebruik door de draadloze client en WLAN (Open, PSK, EAP-PEAP/MSCHAPv2,...)

> **Opmerking**: clientparameters gewijzigd van standaardinstellingen die door de betreffende verkoper zijn opgegeven. (slaaptoestand, roaming parameters, U-APSD,...)

## IV. Netwerktopologiediagram

Dit omvat een weergave en/of details met betrekking tot de draadloze apparaten in het netwerk (printers/scanners, WLC's,...)

## V. Een spreadsheet maken om alle problemen met de client op te nemen

Voorbeeld:

| MAC-adres Username | Beschrijving van het gemelde symptoom | Waargenomen symptoom door eindgebruiker | Standaard gateway Y/N pingen | WiFi-signaalstatus (verbonden/proberen verbinding te maken) | Record ipconfig/a equivaler |
|---|---|---|---|---|---|

Het doel van deze oefening is om een gemeenschappelijk patroon te helpen identificeren, en een nauwkeuriger beeld van het (de) onderwerp(en) in kwestie te geven.

## VI. Opdrachten op de WLC tonen en debuggen

Verzamel deze debugs WLC via de CLI:

- tijd-out voor configuratie-sessies 0
- debug client <MAC_address>
- debug DHCP bericht activeren

Voeg de extra debugs op case-by-case basis toe:

- debug aaa detail enable - gebruik dit als er authenticatie gerelateerde problemen zijn met AAA server
- debug aaa gebeurtenissen enabled - gebruik dit als er authenticatie gerelateerde problemen zijn met AAA server
- debug aaa all enable - gebruik dit voor auth issues; dit is breedsprakig dus gebruik het alleen wanneer nodig (voor AAA override cases en dergelijke)
- debug mobility handoff - gebruik bij roaming problemen tussen WLC's

Verzamel de output voor WLC tonen bevelen via CLI:

- config paging uitschakelen
- show tijd
- toon cliëntdetail <mac-adres van cliënt> (neem nota van de cliëntstaat op WLC)
- De client vanuit de WLC pingen

Zodra de test volledig is, gebruik dit bevel om alle huidige debugs op WLC tegen te houden:

- debug, uitschakelen

## VII. Opdrachten op het toegangspunt tonen en debuggen

### Lichtgewicht Cisco IOS® AP's

In dit gedeelte worden de vereiste debuggen voor de 1700/2700/3700-serie of oudere model access points beschreven.

Gebruik deze opdrachten om een time-out van een AP-sessie te voorkomen op het moment van een Telnet-/SSH-/console-sessie:

- debug capwap console client
- Config t
- lijnconsole 0 — gebruik om seriële sessietime-outparameters aan te passen
- line vty 0 4 — gebruik om Telnet/SSH-sessietime-outparameters aan te passen
- Exec-time-out 0
- sessie-time-out 0
- term leng 0

Alvorens u de test begint, verzamel een steekproef van deze showbevelen op AP. Verzamel ten minste twee monsters van deze uitvoer, zowel voor als na de voltooiing van tests met het gebruik van deze AP tonen opdrachten via de CLI:

- term leng 0
- toonklok
- show tech
- capswapclient tonen mn
- int do1 dfs tonen
- logboekregistratie tonen
- meer event.log
- toon spoor dot11_rst weergave tijd formaat lokaal
- toon spoor dot11_rst
- toon spoor dot11_bcn display tijd formaat lokaal
- toon spoor dot11_bcn

Verzamel deze AP debugs via de CLI:

- debug dot11 { d0 | d1} monitoradres <MAC_address>
- debug dot11 { d0 | d1} traceer printclients mgmt toetsen rxev txev rcv xmt txfail ba
- term mon

Zodra de test volledig is, gebruik deze opdracht om de debugs uit te schakelen:

- u allen

### AP-COS access points

In dit gedeelte worden de vereiste debuggen voor de AP's van de 1800/2800/3800-reeks beschreven.

Gebruik deze opdrachten om een time-out van een AP-sessie te voorkomen op het moment van een Telnet-/SSH-/console-sessie:

- Exec-time-out 0

Alvorens u de test begint, verzamel een steekproef van de showbevelen op AP. Verzamel ten minste twee monsters van deze uitvoer, zowel voor als na de voltooiing van tests met het gebruik van deze AP tonen opdrachten via de CLI:

- term leng 0
- toonklok
- show tech
- toon clientstatistieken <client_MAC-adres>
- toon inhoud nss status

- **nss-stats weergeven**
- **show log**

Voor de 1800 Series access points verzamelt u deze AP-debugs via de CLI:

- **debug dot11 client level events addr <client_MAC-address>**
- **debug dot11 client level error addr <client_MAC-address>**
- **debug dot11 clientniveau kritisch adres <client_MAC-address>**
- **debug dot11 client level info addr <client_MAC-address>**
- **debug dot11 client datapath adr <client_MAC-adres>**
- **debug dot11 client datapath DHCP addr <client_MAC-address>**
- **debug dot11 client datapath arp addr <client_MAC-address>**
- **term mon**

Voor de 2800/3800 Series access points, verzamel deze AP debugs via de CLI:

- **config ap client-trace adres add <client_MAC-address>**
- **config ap client-trace filter alles inschakelen**
- **configuratie ap client-trace uitvoerconsole-log inschakelen**
- **configuratie ap client-trace start**
- **term mon**

Zodra de test volledig is, gebruik deze opdracht om de debugs uit te schakelen:

- **client-traceringsstop voor configuratieap**

## VIII. Opnamen aan clientzijde

Verzamel of een promiscuous Netmon 3.4 (alleen Windows XP of 7) of Wireshark pakketopname van de WLAN-adapter van het clientapparaat.

## IX. OTA-opnamen

### 802.11n opnamen

- AirPCAP met draadloos
- MacBook Pro
- Lijst wordt bijgewerkt...
- OmniPeek Remote Assistant (ORA)
- Cisco AP in Sniffer modus

### 802.11ac-opnamen

- Voor 11ac 3SS-opnamen kunt u een 2014 Macbook Pro of later met 10.10.x of hoger gebruiken (gebruik MacBook Air niet voor 11ac opnamen indien mogelijk, aangezien het momenteel een 2-SS-apparaat is).
- U kunt ook een 2702, 3702 of soortgelijk Cisco AP in snuffelmodus gebruiken.
- Voor roaming scenario's en met het gebruik van professionele netwerkanalyse software zoals OmniPeek van Savvius. Aanbevolen wordt om meerdere, compatibele 802.11ac-compatibele USB WLAN-adapters te gebruiken, zoals de Savvius WiFI-adapter voor OmniPeek

(802.11ac), Netgear A6210 of een soortgelijke adapter.

# XI. Bijlage A - Aanvullende tips en trucs

## Windows

*Om direct vanaf een Windows-pc aanvullende informatie te verzamelen over de huidige draadloze verbinding en andere verwante gegevens. U kunt deze opdrachten in verband met netsh-WLAN gebruiken via de opdrachtregel voor Windows (CMD):*

```
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
```

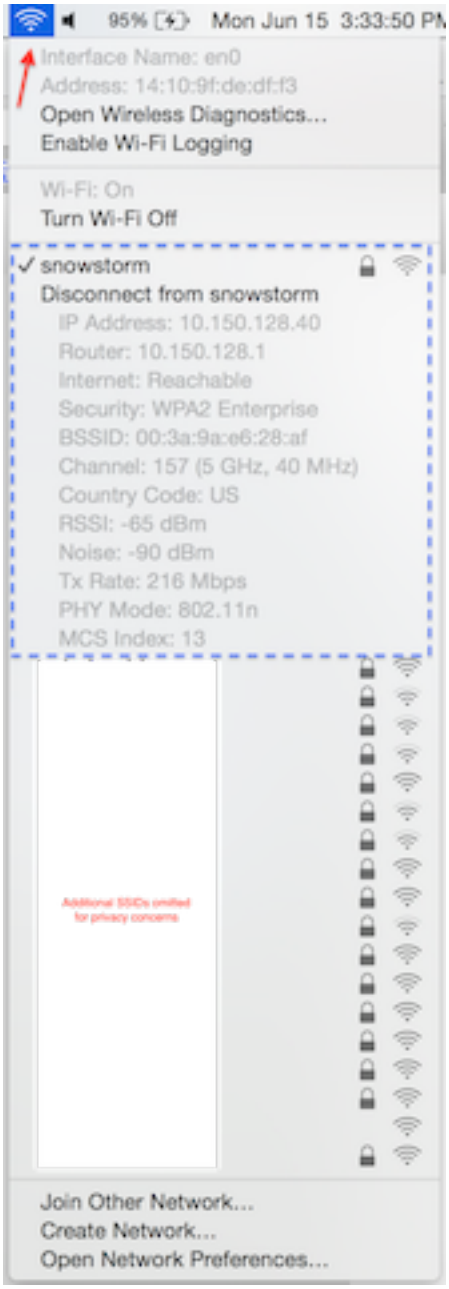
```
    Cipher                 : CCMP
    Connection mode        : Profile
    Channel                : 157
    Receive rate (Mbps)    : 300
    Transmit rate (Mbps)   : 300
    Signal                 : 80%
    Profile                : snowstorm

    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 (voorheen OS X)

Om de equivalente uitvoer te verzamelen als de **ipconfig/all** opdracht op een Windows PC, kunt u in plaats daarvan de gemeenschappelijke Linux/Unix opdracht van **ifconfig** gebruiken om gedetailleerde informatie voor alle netwerkinterfaces op een Apple MacBook te vermelden. Indien nodig kunt u ook specificeren om de uitvoer te ontvangen voor alleen de native draadloze interface voor een gegeven MacBook (of en0 of en1, het hangt af van het model). Bijvoorbeeld:

```
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
```

Om snel maar gedetailleerd informatie te krijgen over de huidige draadloze verbinding op een MacBook. U kunt ook het pictogram WiFi in de rechterbovenhoek van het bureaublad selecteren terwijl u tegelijkertijd de **optieknop** op uw toetsenbord houdt zoals in de afbeelding.




Een andere handige optie is om de verborgen opdrachtregel utility, genaamd airport, te gebruiken. Het is zeer aan te raden om dit alleen te gebruiken met uw eigen MacBook of een in gebruik in een lab omgeving. Aangezien sommige netwerkbeheerders wellicht geen toegang tot dit hulpprogramma willen verlenen op de MacBook van een eindgebruiker, moet u de juiste mate van voorzichtigheid gebruiken. Om verder te gaan, voer dit in Terminal in op de MacBook in kwestie:

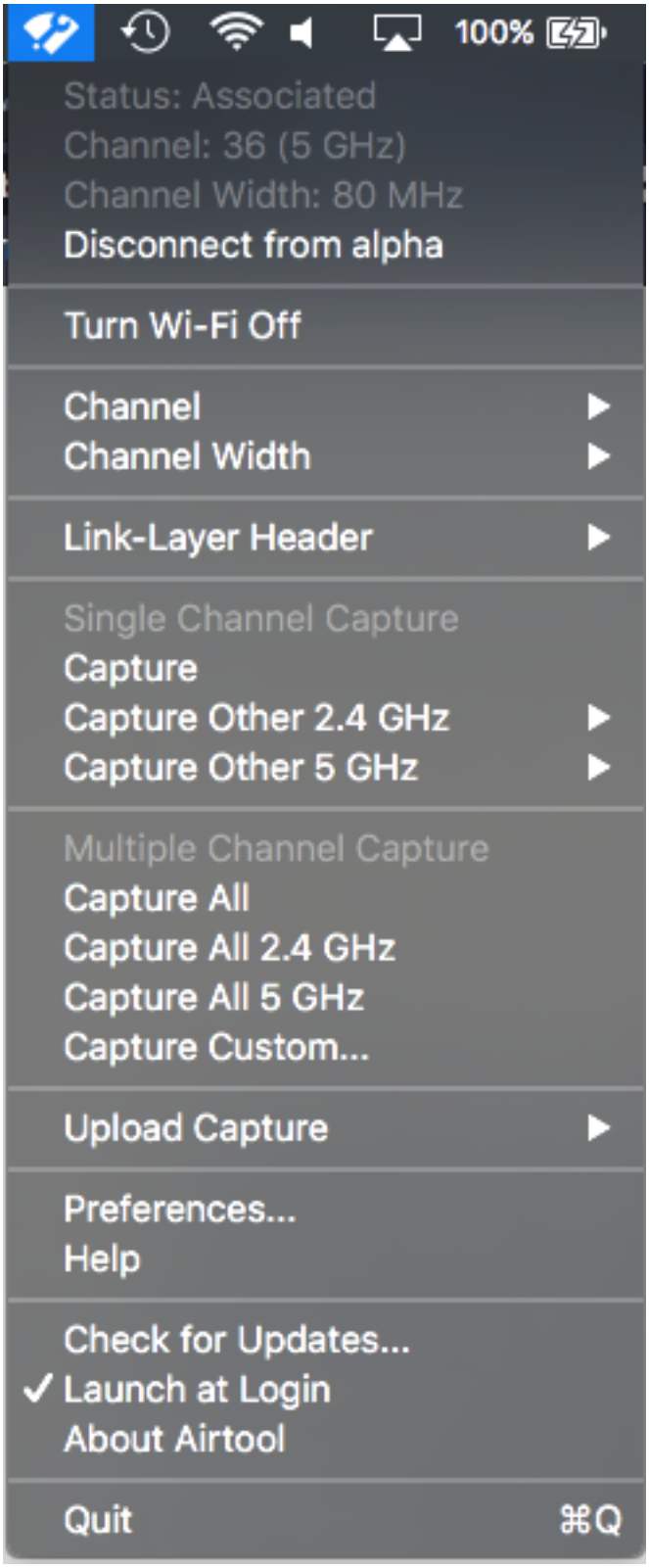
```
sudo ln -s
/System/Library/PrivateFrameworks/Apple80211.framework/Versions/Current/Resources/airport
/usr/local/bin/airport
```

U kunt nu eenvoudig een beroep doen op de luchthaven CLI utility. Een voorbeeld hiervan is:

```
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
```

Om het proces verder te vereenvoudigen om een betrouwbare, enkele 802.11-kanaals OTA pakketopname te verzamelen met behulp van de mogelijkheden van een MacBook Pro of vergelijkbaar. U kunt gebruikmaken van de ingesloten functies in macOS met het gebruik van de methode Wireless Diagnostics > Sniffer of vergelijkbaar zoals eerder besproken, maar u kunt ook een hulpprogramma van derden gebruiken, Airtool genaamd (OS X 10.8 en hoger). Het voordeel is een eenvoudige interface om snel een OTA pakketopname te verzamelen, die direct wordt opgeslagen op het bureaublad met slechts een paar klikken door de app UI direct vanaf de bovenste menubalk op uw scherm.




Meer informatie en downloadlinks voor Airtool vindt u op deze URL:

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

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.