Guide de dépannage pour des problèmes d'interopérabilité de client sans fil avec CUWN

Contenu

Introduction
Conditions préalables
Conditions requises
Composants utilisés
Informations générales
I. **Définition du problème**
II. configuration WLC et logs généraux
Passage-config
Fichier de configuration WLC
GUI
CLI
Syslog du WLC
III. Détails périphériques et informations de client
IV. Topologie du réseau
V. Détails supplémentaires de piste et les particularités
VI. WLC - Commandes d'exposition et de debug
Commandes de debug WLC
Commandes show WLC
VII. AP - Commandes d'exposition et de debug
Points d'accès légers de Cisco IOS
Commandes show AP
Commandes de debug AP
Points d'accès AP-COS
Commandes show AP-COS
Gamme 1800 | Commandes de debug AP-COS
Gamme 2800/3800 | Commandes de debug AP-COS
VIII. Captures de paquet de côté client
IX. Au-dessus du - Captures de paquet de l'air (OTA)
captures 802.11n
captures 802.11ac OTA
X. Résumé
I. **Définition du problème**
II. configuration et logs WLC
III. L'information sur le périphérique de client
IV. Diagramme de topologie du réseau
V. Créez un tableur pour enregistrer toutes les questions de client
VI. Commandes d'exposition et de debug sur le WLC
VII. Commandes d'exposition et de debug sur AP

Cisco IOS léger aps
AP-COS aps
VIII. Captures de côté client
IX. captures OTA
captures 802.11n
captures 802.11ac
XI. Annexe A - Conseils et astuces supplémentaires
Windows
MaOS (autrefois SYSTÈME D'EXPLOITATION X)

Introduction

Ce document décrit en détail quel besoin d'informations d'être au commencement collecté efficacement pour étudier et dépanner de tels problèmes d'interopérabilité Sans fil quand ils surgissent avec la solution du réseau sans fil unifié de Cisco (CUWN). Le besoin d'une telle approche globale devient de plus en plus important avec jamais la croissance des nombres et des combinaisons des périphériques de client sans fil et des radios du Point d'accès (AP).

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Radio aps de Cisco
- Contrôleurs LAN Sans fil (WLC)
- Périphériques relatifs de réseau

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

> **Note**: Le public visé pour ce document sont des ingénieurs réseau et des administrateurs Sans fil expérimentés qui sont déjà au courant de l'utilisation, de la configuration et du dépannage de ces thèmes.

Informations générales

Il peut être commun pour constater que donné le divers client les périphériques qu'existez et continuez pour être développés. Un grand choix de questions peuvent surgir quant à établissent, mettent à jour, ou simplement obtenir les la plupart hors de leur connexion au réseau Sans fil et

prendre en charge l'infrastructure.

Ceci peut souvent descendre à une question simple de configuration de la part du périphérique de client et/ou de l'infrastructure Sans fil lui-même. Cependant, dans certains cas ceci peut être attribué à un problème d'interopérabilité quant à un périphérique spécifique et aux composants de client qui le prennent en charge (c.-à-d. suppliant, adaptateur WLAN, gestionnaire Sans fil, etc.), et/ou aux aps en question. En tant qu'ingénieurs Sans fil, de tels problèmes d'interopérabilité posent une occasion d'identifier, dépanner, et résoudre des défis potentiellement complexes.

Les informations complémentaires à ce qui est tracée les grandes lignes en cet article pourraient être demandées et étées nécessaires pour être collectées au cas par cas, donné le nombre illimité de variables qui pourraient dicter de telles conditions requises. Cependant, les informations détaillées ici sont une instruction générique pour aborder n'importe quel problème d'interopérabilité potentiel de client sans fil.

I. Définition du problème

La première étape pour traiter efficacement n'importe quel problème avec l'intention pour obtenir résolu, est de définir exactement la question actuelle. Pour faire ainsi, assurez que cela à un minimum de ces questions sont demandés et leurs réponses sont clairement documentées :

- La question est-elle limitée à un modèle spécifique d'aps et/ou de type de radio (c.-à-d. 2.4 gigahertz contre 5 gigahertz) ?
- Est-ce qu'on observe la question seulement sur des versions spécifiques de logiciel WLC ?
- Est la question éprouvée avec seulement des versions spécifiques des types de client et/ou du logiciel (c.-à-d. version de système d'exploitation, version de gestionnaire WLAN, etc.)
- Y a-t-il de autres périphériques sans fil qui n'éprouvent pas cette question ? Si oui, quelles sont-elles ?
- La question est-elle reproductible tandis que le client est connecté à une configuration sans fil simplifiée telle qu'un SSID ouvert, à une largeur de canal de 20 MHZ, et à 802.11ac désactivé ? (c.-à-d. fait la question se produisent sur le mode 802.11n contre le mode 802.11ac seulement ?).
- Si la question n'est pas reproductible avec un SSID ouvert, à quelle configuration de sécurité minimum la question est vu ? (c.-à-d. PSK ou 802.1X sur le WLAN).
- Quelle était la configuration en cours et les versions de logiciel précédentes ?

II. configuration WLC et logs généraux

Passage-config

Sans exception, il est de la nécessité absolue pour collecter la configuration WLC du client pour un examen détaillé des caractéristiques utilisées par le client, leur installation spécifique, et d'autres tels détails. Pour faire ainsi, vous devez établir une session Telnet/SSH au WLC en question et sauvegarder la sortie de ces commandes CLI à un fichier texte :

```
config paging disable

show run-config
```

La pleine sortie de passage-config est toujours préférée, car elle inclut les informations détaillées quant aux aps joints et aux informations associées rf, etc. Bien que dans certains cas et situations, comme quand vous travaillez au commencement avec un WLC avec un grand nombre d'aps joints (c.-à-d. 8510 WLC avec 2500+ aps). Il pourrait préférer collecter au commencement juste la configuration du WLC sans une telle informations AP pour l'examen rapide, pendant que le plein show run-config pourrait prendre 30 minutes ou plus pour se terminer donné le nombre d'aps. Cependant, il pourrait encore être nécessaire pour collecter le plein passage-config sorti à une date ultérieure.

Pour faire ainsi, vous pouvez sur option collecter la sortie de ces commandes CLI à un fichier texte :

```
config paging disable

show run-config no-ap

show wlan apgroups
```

Fichier de configuration WLC

En plus du **show run-config** ou de la sortie du **show run-config NO--AP**, il est également recommandé pour collecter une sauvegarde complète de la configuration WLC aussi bien. C'est d'assistance, si un laboratoire recréent les besoins d'être conduit par la transmission des problèmes TAC/HTTS et de BU, pour essayer et reproduire la question du client dans un environnement de TP Cisco. Une sauvegarde du WLC peut être collectée par l'intermédiaire du GUI ou du CLI du WLC en question, avec l'utilisation du TFTP ou du FTP de sauvegarder le fichier de configuration au serveur TFTP/FTP externe. L'exemple ci-dessous affiche que l'utilisation du GUI et du CLI sauvegardait une sauvegarde du WLC, avec l'utilisation du TFTP :

GUI

Commands > Upload File > configuration > téléchargement suivant les indications de l'image.

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
```

Syslog du WLC

Àce moment, vous voulez également collecter les logs en cours du WLC pour l'examen supplémentaire comme nécessaire. Dans le meilleur des cas, vous voulez collecter ces logs juste

après votre test avec un client sans fil par lequel la question signalée soit reproduite. Si le client exporte le WLC se connecte à un serveur externe de Syslog, alors vous voulez les récupérer de là. Autrement, vous pouvez sauvegarder le msglog et le traplog actuellement enregistré localement sur le WLC en enregistrant cette session ILC a sorti à un autre fichier texte :

```
config paging disable

show msglog

show traplog
```

III. Détails périphériques et informations de client

L'étape suivante est de recueillir autant les informations et des particularités quant aux dispositifs de client en service qui éprouvent un problème d'interopérabilité Sans fil potentiel. Une telle informations devraient inclure, mais être pas nécessairement limitées à ces derniers :

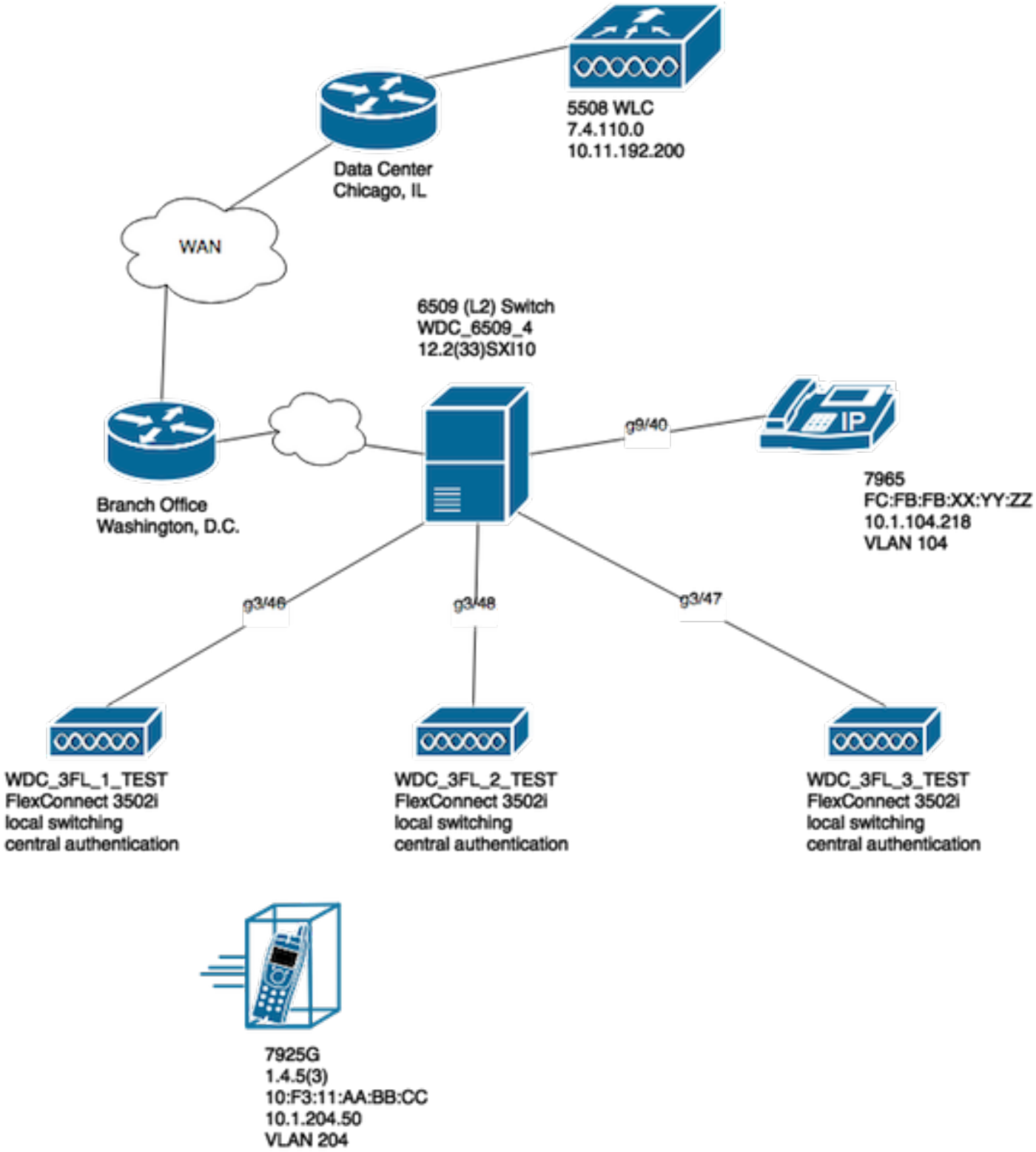
- Type de client (c.-à-d. tablette, smartphone, ordinateur portable, etc.)
- Marque et modèle de périphérique
- Version de système d'exploitation
- Modèle d'adaptateur WLAN
- Version de pilote de l'adaptateur WLAN
- Suppliant utilisé (c.-à-d. config de Windows Zero/config automatique, Intel PROSet, etc.)
- Sécurité configurée à l'usage du client sans fil et WLAN (c.-à-d. ouvrez-vous, PSK, EAP-PEAP/MSCHAPv2, etc.)
- Notez tous les paramètres de client qui ont été changés des valeurs par défaut fournies par le constructeur en question (c.-à-d. état de sommeil, paramètres errants, U-APSD, etc.).

Note: Les toutes les informations complémentaires ou notes quant aux dispositifs de client jusqu'auxquels inclut des captures d'écran de son WLAN ont associé des configurations, et ainsi de suite doivent également être incluses comme nécessaire.

IV. Topologie du réseau

Pour accélérer plus loin des procédures de dépannage et le processus de l'analyse de cause principale (RCA), il est toujours recommandé pour fournir un diagramme détaillé et complet de topologie du réseau. Le diagramme de topologie du réseau devrait non seulement inclure des détails au sujet de l'infrastructure de réseau et de radio, mais fournit également une vue dans les dispositifs Sans fil en question qui fonctionne dans le réseau (c.-à-d. imprimantes/scanners, quel client VLAN soyez en service, etc.) et leurs emplacements relativement à un des autres.

Un certain nombre d'outils (c.-à-d. Microsoft Visio, draw.io, etc.) et un grand choix de styles peuvent être utilisés pour créer un tel schéma de réseau. L'important aspect est de s'assurer simplement que les informations appropriées sont clairement reflétées dans le diagramme donné pour l'examen par tous les interlocuteurs et constructeurs impliqués. Une topologie de réseau d'exemple qui capture de base, mais les informations utiles quant aux périphériques d'infrastructure et de client suivant les indications de l'image.



V. Détails supplémentaires de piste et les particularités

Pour aider à s'assurer que l'information correcte est collectée au moment de n'importe quel test avec les dispositifs de client que les utilisateurs finaux éprouvent des questions avec. Il est recommandé pour créer de préemption un tableur ou semblable pour enregistrer tous les questions de client et détails associés observés au moment du test, tel que cet exemple :

Adresse MAC	Nom d'utilisateur	Description de symptôme signalé	Symptôme observé par utilisateur	Y/N de passerelle par défaut de ping	État de signal WiFi (connecté/essayant de se connecter)	Enregistrez l'ipconfig

		final de temps			
xxyy.aabb.0011 test_user1	Par intermittence démonter de Point d'accès.	Association perdue de connexion réseau et de radio d'AP3.	N	Essayer à connecter	ifconfig en0 en0 : mtu 1500 flags=8863<UP,BR Ether xx:yy:aa:bb: inet6 fe80::848:cb 0x4 émission 192.168. nd6 options=201< medias : autosele état : actif

Le but de cet exercice est d'aider à documenter et déterminer un modèle commun d'intérêt, aussi bien qu'à obtenir une image précise des questions actuelles. Une fois que ce tableur est préparé être utilisé pour la collecte des informations, vous êtes maintenant prêt à commencer vos tests. Quelques considérations supplémentaires, pourtant importantes sont comme suit :

Note: Tout met au point et des captures de paquet collectées doivent être synchronisées au même serveur de NTP pour une corrélation plus facile avec les logs, et doivent être prises en même temps pour n'importe quel test donné.

Note: Fournissez un horodateur précis de quand la question est observée, et quand la question semble récupérer (si c'est approprié).

Note: Collectez toujours met au point filtré par adresse MAC de client sur AP et WLC.

Note: N'exécutez pas l'exposition et des commandes de débogage sur AP dans la même session Telnet/SSH/console, ceux-ci devraient être faites séparément en session différente en conséquence.

Note: AP met au point sont préférés être pris sur Telnet/SSH contre la console, car la console est en général trop lente pour être efficace.

VI. WLC - Commandes d'exposition et de debug

Quand des tests sont effectués pour reproduire et dépanner les problèmes d'interopérabilité potentiels de client sans fil, il est impératif que mette au point et des logs supplémentaires soient collectés de l'infrastructure Sans fil en service. Ces deux sections peuvent expliquer en détail les logs spécifiques et la sortie de débogage initiale qui devraient être collectés du WLC et de l'AP, respectivement.

Commandes de debug WLC

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

En ce qui concerne la nature de la question actuelle, vous pouvez également ajouter ces WLC met au point au cas par cas :

- **enable de détail de debug aaa** - utilisez ceci s'il y a des questions connexes d'authentification avec le serveur d'AAA
- **enable d'événements de debug aaa** - utilisez ceci s'il y a des questions connexes d'authentification avec le serveur d'AAA
- **debug aaa tout l'enable** - utilisez ceci pour les questions authentiques ; la sortie pour ceci mettent au point est bavarde ainsi utilisez-le seulement si absolument nécessaire (c.-à-d. pour des cas de priorité d'AAA, etc.)
- **transfert de debug mobility** - utilisation quand là errent des questions entre WLCs

Une fois que la question est reproduite avec le client sans fil en question, et toutes les informations tracées les grandes lignes dans les sections antérieurement et après ceci sont collectés et documentés. Afin d'exécuter ces commandes CLI, vous devez désactiver met au point sur le WLC.

```
debug disable-all
```

Commandes show WLC

```
config paging disable

show time

show client detail <MAC_address>

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

Comme précédemment mentionné, assurez pour exécuter le WLC met au point en une session Telnet/SSH et collecte la sortie pour ces commandes show dans un autre Telnet/SSH au WLC. Vous devez faire la même chose pour collecter AP met au point et les commandes show sortent détaillé dans cette section.

VII. AP - Commandes d'exposition et de debug

Points d'accès légers de Cisco IOS

Avant que vous commenciez en met au point sur n'importe quel IOS léger AP impliqué dans le test, tel que les 2600, les 2700, les 3700 ou les points d'accès Cisco modèles antérieurs. Vous devez d'abord exécuter ces commandes CLI sur AP, afin d'éviter un délai d'attente au moment d'une session Telnet/SSH/console à AP en question quand vos tests de client :

```
debug capwap console cli

config t

line vty 0 4

exec-timeout 0

session-timeout 0
```

Vous pouvez également suivre ces étapes pour utiliser la connexion de console et pour remplacer le **line vty 0** déclarations **4** par la **line console 0** à la place, afin de désactiver les délais d'attente d'exécutif et de session pour une interface série/connexion de console en conséquence.

- line console 0 - utilisation de modifier des paramètres de dépassement de délai séquentiels de session
- line vty 0 4 - utilisation de modifier des paramètres de dépassement de délai de session Telnet/SSH

Commandes show AP

Avant que vous commenciez le test, vous devez d'abord collecter un échantillon de ces commandes show sur AP. Vous devriez collecter la sortie de ces commandes show au moins deux fois pour chaque test qui fait participer le client sans fil en question ; chacun des deux avant et après le test sont complets.

```
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
```

Commandes de debug AP

Une fois que vous avez collecté la sortie initiale des commandes show mentionnées ci-dessus, vous pouvez maintenant activer met au point sur le même Point d'accès en session distincte Telnet/SSH comme affichée. Assurez pour sauvegarder la sortie entière à un fichier texte.

```
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
```

Légende

Indicateur	Description
d0	Radio 2.4 gigahertz (emplacement 0)
d1	Radio 5 gigahertz (emplacement 1)

mgmt	Paquets de gestion de suivi
Ba	Les informations du bloc ACK de suivi
récepteur	Le suivi a reçu des paquets
clés	Clés réglées de suivi
rxev	Le suivi a reçu des événements
txev	Le suivi transmettent des événements
txrad	Le suivi transmettent pour transmettre par radio
xmt	Le suivi transmettent des paquets
txfail	Le suivi transmettent des pannes
débits	Modifications de débit de suivi

Pour désactiver met au point sur AP une fois que le procédé de test et de collecte des informations est terminé, vous peut exécuter cette commande CLI sur AP :

```
u all
```

Points d'accès AP-COS

Pour 802.11ac les Points d'accès capables de l'onde 2 et plus tard, comme les 1800, les 2800 et les Points d'accès 3800 modèles. Ces un plus nouveau modèle aps introduisent un système d'exploitation complètement nouveau pour les Plateformes de Point d'accès désignées sous le nom d'AP-COS. En soi, non toutes les commandes comme précédemment utilisées sur le Cisco IOS léger traditionnel ont basé des Points d'accès comme détaillé ci-dessus s'appliquent toujours. Si quand vous dépannez une question implique le problème d'interopérabilité des divers périphériques et de l'AP-COS aps modèles du client STA, alors ces les informations devraient être collectées du Point d'accès AP-COS impliqué du test équivalent.

Avant que vous commenciez en met au point sur n'importe quel modèle AP AP-COS impliqué dans le test. Vous devez d'abord exécuter ces la commande CLI sur AP, afin d'éviter un délai d'attente au moment d'une session Telnet/SSH/console à AP en question quand vos tests de client :

```
exec-timeout 0
```

Commandes show AP-COS

Avant que vous commenciez le test, vous devez d'abord collecter un échantillon de ces commandes show sur AP. Vous devriez collecter la sortie de ces commandes show au moins deux fois pour chaque test qui fait participer le client sans fil en question ; chacun des deux avant et après le test sont complets.

```
term len 0

show clock show tech

show client statistics <client_MAC-address>

show cont nss status

show cont nss stats

show log
```

Gamme 1800 | Commandes de debug AP-COS

Ceux-ci met au point sont spécifiques à la gamme 18xx de Points d'accès. C'est dû au fait que les jeux de puces utilisés pour la gamme 1800 d'aps diffèrent de ceux trouvés aux Points d'accès de gamme 2800/3800, et un ensemble différent de met au point ainsi sont exigés dans ce scénario par comparaison. La correspondance met au point pour la gamme 2800/3800 que des aps est couverts dans la section suivante.

Une fois que vous avez collecté la sortie initiale des commandes show mentionnées ci-dessus, vous devez maintenant activer met au point sur les même 1800 Points d'accès en session distincte Telnet/SSH comme affichée. Assurez pour sauvegarder la sortie entière à un fichier texte.

```
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>
```

Dans certains cas, vous pourriez devoir activer également le supplémentaire met au point sur le 18xx AP pour dépanner plus loin des problèmes d'interopérabilité de client. Cependant, ceci devrait être seulement if/as fait demandé par un ingénieur TAC Cisco pour une demande de service/cas correspondants.

Pendant que supplémentaire met au point pourrait non seulement être bien plus bavard dans leur sortie mais peut également introduire le chargement supplémentaire sur AP aussi bien par conséquent où il exige supplémentaire chronomètrent pour l'analyse appropriée. Ce qui dans certaines conditions peut potentiellement perturber le service, si beaucoup de périphériques de client tente de se connecter à même AP sous le test ou les variables semblables.

Pour désactiver met au point sur le Point d'accès variable AP-COS - si sur une gamme 1800 ou 2800/3800 AP - le procédé de collecte une fois de test et de données est terminé, vous peut exécuter cette commande CLI sur AP :

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

Gamme 2800/3800 | Commandes de debug AP-COS

Une fois que vous avez collecté la sortie initiale des commandes show mentionnées ci-dessus, vous devez maintenant activer met au point sur le même 2800/3800 Point d'accès en session distincte Telnet/SSH comme affichée. Assurez pour sauvegarder la sortie entière à un fichier texte.

```
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
```

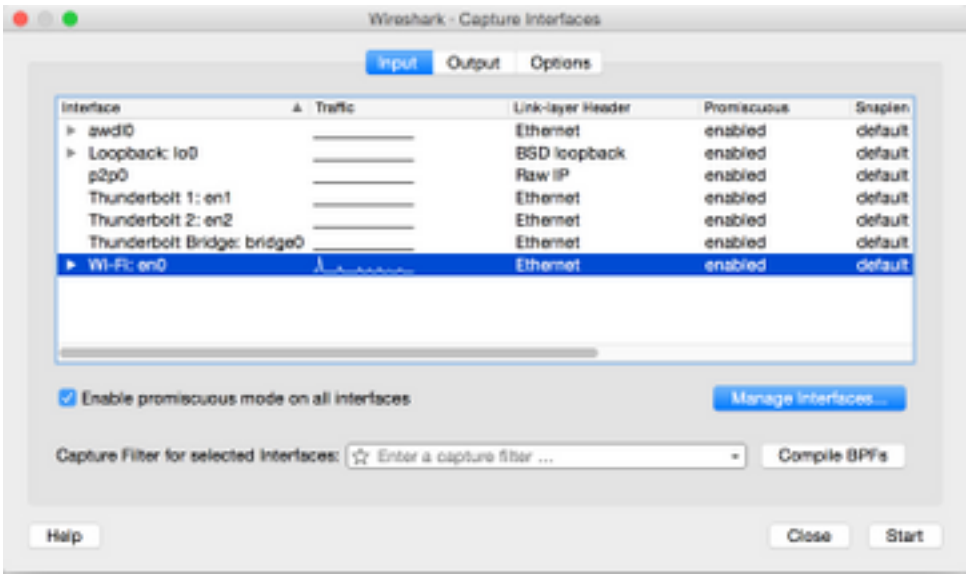
Pour désactiver met au point sur la gamme 1800/2800/3800 AP une fois que le procédé de collecte de test et de données est terminé, vous peut exécuter cette commande CLI sur AP :

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

VIII. Captures de paquet de côté client

Du périphérique de client en service s'il est un ordinateur portable, MacBook ou semblable, vous devez collecter la capture promiscueuse de paquet de mode de l'interface Sans fil du périphérique de client utilisé pour reproduire la question. Des utilitaires communs comme Netmon 3.4 (Windows seulement) ou Wireshark peuvent être aisément téléchargés et utilisés pour collecter cette capture et pour la sauvegarder à un fichier *.pcap. Il dépend du périphérique, il pourrait également y avoir des moyens de collecter un tcpdump ou semblable du client en question, ainsi vous pourriez devoir consulter avec le constructeur d'appareils de client pour l'assistance à cet égard.

Voici un exemple pour configurer une capture Wireshark pour l'interface Sans fil sur un MacBook Pro :



Comme avec n'importe quelle capture de paquet, indépendamment quel utilitaire est utilisé pour le collecter, assurez pour sauvegarder le fichier dans un format de fichier de pcap (c.-à-d. *.pcap, *.pcapng, *.pkt, etc.). C'est de s'assurer que non seulement les ingénieurs de Cisco dans n'importe quel service peuvent visualiser les fichiers de capture de paquet facilement, mais des ingénieurs d'autres constructeurs et des organismes aussi bien (c.-à-d. Intel, Apple, etc.). Ceci tient compte d'un procédé plus sans couture de coopération et de Collaboration, qui facilite plus loin Cisco et les constructeurs de périphérique de client pour fonctionner mieux ensemble pour étudier et résoudre tous les problèmes d'interopérabilité potentiels.

IX. Au-dessus du - Captures de paquet de l'air (OTA)

Afin de dépanner efficacement tous les problèmes d'interopérabilité Sans fil potentiels ou existants, il est crucial de collecter une capture de paquet de la qualité OTA de la question. Ceci tient compte de l'analyse détaillée de la communication sans fil réelle de 802.11 entre le client sans fil et les radios de Point d'accès en question, en plus de donnent davantage de point de vue

au côté client et les logs d'infrastructure de radio, met au point, etc. C'est une étape essentielle qui doit faire pour chaque test d'un problème d'interopérabilité Sans fil potentiel, sans exception.

Chronomètre cependant, souvent le consommateur final n'est pas correctement équipé ou est préparé pour collecter des captures de paquet OTA. C'est un obstacle commun que d'ingénieurs la face Sans fil souvent, et eux doit fonctionner avec le client pour surmonter ceci d'un grand choix de manières. Cet article des forum de support de Cisco peut servir de bon point de début pour aider à guider et instruire le client en conséquence :

reniflement de radio de 802.11/capture de paquet

Il est d'importance primordiale que les captures de paquet OTA soient collecté dans un format de fichier de pcap (c.-à-d. *.pcap, *.pcapng, *.pkt, etc.), et inclut les méta-données de 802.11 (c.-à-d. RSSI, le canal, le débit de données, etc.). Le renifleur OTA devrait également être maintenu dans la grande proximité au périphérique de client en question à tout moment pendant les tests, pour assurer un point de vue précis du trafic envoyé et reçu à/de le périphérique de client étant testé.

> **Note**: Si les tests en question impliquent un scénario errant de périphérique de client, par lequel plus d'un canal de 802.11 doive être surveillé dans une capture agrégée de paquet. Alors il n'est pas actuellement recommandé pour utiliser l'analyseur de WiFi d'AirMagnet des réseaux de fluke.

La raison pour ceci est due au fait qui a agrégé des captures de paquet avec l'utilisation de cet utilitaire sont actuellement enregistrés dans un format de fichier de propriété industrielle, et pas dans un format de style de pcap qui peut être aisément visualisé dans Wireshark ou d'autres utilitaires semblables. Assurez-vous que votre capture de paquet OTA est dans un format de fichier non-de propriété industrielle, ceci aide à s'assurer que tous les parties et constructeurs concernés peuvent aisément examiner tous les fichiers de capture à tout moment, et aide finalement à accélérer n'importe quels efforts de résolution.

dans un format qui est accessible en lecture par Wireshark en cours, et qui inclut les méta-données de 802.11 (RSSI, canal, débit de données) - voyez plus à : https://supportforums.cisco.com/document/75331/80211-wireless-sniffing-packet-capture#sthash.Xhlx5LSS.dpuf
Voici quelques méthodes classiques pour collecter une capture de paquet OTA :

- AirPCAP avec Wireshark
- MacBook Pro
- Professionnel d'OmniPeek, entreprise d'OmniPeek, etc.
- Assistant distant d'OmniPeek (ORA)
- Cisco AP en mode de renifleur

captures 802.11n

Pour OTA le paquet le capture qui fait participer les clients sans fil 802.11n, là est actuellement plus de flexibilité et de simplicité d'utilisation. C'est dû à une plus grande variété d'adaptateurs disponibles de la radio USB WLAN qui peuvent être aisément utilisés avec un certain nombre d'outils, tels qu'OmniPeek et d'autres.

Prenez la note quant à la façon dont les capacités des adaptateurs Sans fil spécifiques utilisés pour collecter une capture 802.11n OTA rivalisent avec les capacités du jeu de puces de l'effectif

WLAN utilisé par les dispositifs de client que vous tentez de dépanner. Par exemple, si le périphérique de client éprouve un problème d'interopérabilité Sans fil potentiel qui utilise 2 un jeu de puces capable du flux spatial (2SS) 802.11n. Alors on le recommande fortement de s'assurer que l'adaptateur Sans fil utilisé pour collecter une capture de paquet OTA est également un 2SS ou un meilleur adaptateur, avec 802.11n ou plus nouvelles caractéristiques.

captures 802.11ac OTA

Pour 3 captures 802.11ac du flux spatial (3SS), vous pouvez utiliser les capacités indigènes de reniflement des 2014 MacBook Pro modèles ou un plus défunt Mac OS X courant 10.10.x ou plus élevé. Si dépannant 2 un périphérique de client du flux spatial 802.11ac, vous pouvez également utiliser un MacBook Air pour les captures 802.11ac. Le modèle d'air des jeux de puces de l'utilisation 2SS seulement WLAN de MacBooks actuellement au moment de cette écriture. Vous pouvez se référer à Cisco ci-dessous prenez en charge l'article de forum pour des instructions sur la façon dont collecter des captures de paquet OTA avec l'utilisation du Mac OS X, par un grand choix de méthodes :

Radio reniflant avec l'utilisation du Mac OS X 10.6+

Vous pouvez également employer une gamme 2702/2802/3702/3802 ou AP semblable en mode de renifleur pour collecter une saisie appropriée du paquet 802.11ac avec 3SS. Vous pouvez également se référer à la ressource ci-dessous pour une liste en cours d'adaptateurs disponibles de la radio 802.11ac. Certains dont peut pouvoir être utilisé potentiellement avec les outils communs comme OmniPeek et d'autres pour collecter une capture du paquet 802.11ac (c.-à-d. jeux de puces de Ralink, d'Atheros, etc.) :

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

Vous pouvez également employer une gamme 2702/2802/3702/3802 ou AP semblable en mode de renifleur pour collecter une saisie appropriée du paquet 802.11ac avec 3SS. Pour la commodité, des instructions pas à pas sur la façon dont configurer Cisco AP en mode de renifleur et collecter une capture de paquet OTA peuvent être trouvées dans l'article ci-dessous de forum de support de Cisco :

Cisco AP en mode de renifleur

Pour le dépannage des scénarios d'itinérance avec un périphérique de client sans fil, le défi commun est de collecter efficacement une capture de paquet OTA à travers des plusieurs canaux. Cette méthode de surveiller simultanément de plusieurs canaux de 802.11 est réalisée par la collecte de la capture agrégée de paquet OTA. Il est recommandé pour employer le multiple, les adaptateurs capables compatibles 802.11ac USB WLAN avec un logiciel d'analyse réseau compatible afin de réaliser ceci. Quelques adaptateurs capables communs 802.11ac USB WLAN incluent l'adaptateur de WiFi de Savvius pour OmniPeek (802.11ac), Netgear A6210, ou semblable.

X. Résumé

Voici une brève récapitulation des informations qui doivent être collectées pour dépanner efficacement un problème d'interopérabilité potentiel de client sans fil avec un CUWN. Cette section est destinée pour servir de section de référence rapide, comme nécessaire.

I. Définition du problème

- La question est-elle limitée à un modèle spécifique du type de Point d'accès et/ou de radio (2.4 gigahertz contre 5 gigahertz) ?
- Est-ce qu'on observe la question seulement sur des versions spécifiques de logiciel Sans fil du contrôleur LAN (WLC) ?
- Est la question éprouvée avec seulement des versions spécifiques des types de client et/ou du logiciel (c.-à-d. version de système d'exploitation, version de gestionnaire WLAN, etc.)
- Y a-t-il de autres périphériques sans fil qui n'éprouvent pas cette question ? Si oui, quelles sont-elles ?
- La question est-elle reproductible tandis que le client est connecté à un SSID ouvert, à une largeur de canal de 20 MHZ, et à 802.11ac désactivé ? (c.-à-d. fait la question se produisent sur le mode 11n contre le mode 11ac seulement)
- Si la question n'est pas reproductible avec un SSID ouvert, à quelle configuration de sécurité minimum la question est vu ? (c.-à-d. PSK ou 802.1X sur le WLAN)
- Quelle était la configuration en cours et les versions de logiciel précédentes ?

II. configuration et logs WLC

Collectez ceci du CLI du WLC en question :

- débronchement de pagination de config
- show run-config

Alternativement, vous pouvez également collecter juste ces derniers sortis comme nécessaires :

- débronchement de pagination de config
- show run-config NO--AP
- apgroups de show wlan

Sauvegarde de la configuration WLC par l'intermédiaire de TFTP, de FTP, etc. (GUI : **Commands > Upload File > configuration**)

Syslog du WLC

III. L'information sur le périphérique de client

- Type de client (c.-à-d. tablette, smartphone, ordinateur portable, etc.)
- Marque et modèle de périphérique
- Version de système d'exploitation
- Modèle d'adaptateur WLAN
- Version de pilote de l'adaptateur WLAN
- Suppliant utilisé (c.-à-d. config de Windows Zero/config automatique, Intel PROSet, etc.)
- Sécurité configurée à l'usage du client sans fil et WLAN (c.-à-d. ouvrez-vous, PSK, EAP-PEAP/MSCHAPv2, etc.)

> **Note**: Tous les paramètres de client ont changé des valeurs par défaut fournies par le constructeur en question. (c.-à-d. état de sommeil, paramètres errants, U-APSD, etc.)

IV. Diagramme de topologie du réseau

Ceci devrait inclure une représentation et/ou des détails quant aux périphériques sans fil dans le réseau (c.-à-d. imprimantes/scanners, WLCs, etc.)

V. Créez un tableur pour enregistrer toutes les questions de client

Exemple :

Adresse MAC	Nom d'utilisateur	Description de symptôme signalé	Symptôme observé par utilisateur final de temps	Y/N de passerelle par défaut de ping	État de signal WiFi (connecté/essayant de se connecter)	Enregistrez l'ipconfig /all (ou l'équivalent)

Le but de cet exercice est d'aider à identifier un modèle commun, et à présenter une image plus précise des questions actuelles.

VI. Commandes d'exposition et de debug sur le WLC

Collectez ces WLC met au point par l'intermédiaire du CLI :

- **config sessions timeout 0**
- **mettez au point le <MAC_address> de client**
- **enable de message de debug dhcp**

Ajoutez le supplémentaire met au point sur le cas par cas :

- **enable de détail de debug aaa** - utilisez ceci s'il y a des questions connexes d'authentification avec le serveur d'AAA
- **enable d'événements de debug aaa** - utilisez ceci s'il y a des questions connexes d'authentification avec le serveur d'AAA
- **debug aaa tout l'enable** - utilisez ceci pour les questions authentiques ; c'est bavard ainsi utilisez-le seulement si nécessaire (c.-à-d. pour le dépassement d'AAA enferme etc.)
- **transfert de debug mobility** - utilisation en errant des questions entre WLCs

Collectez la sortie pour les commandes show WLC par l'intermédiaire du CLI :

- **débronchement de pagination de config**
- **show time**
- **show client detail < mac-address de client>** (notez l'état de client sur le WLC)
- Cinglez le client du WLC

Une fois le test est complet, utilisent cette commande d'arrêter tout le courant met au point sur le WLC :

- **debug disable-all**

VII. Commandes d'exposition et de debug sur AP

Cisco IOS léger aps

Cette section détaille met au point requis pour la gamme 1700/2700/3700 ou les Points d'accès

modèles antérieurs.

Pour éviter un délai d'attente de session AP au moment d'une session Telnet/SSH/console, utilisez ces commandes :

- mettez au point la console cli de capwap
- configuration t
- line console 0 -- utilisation de modifier des paramètres de dépassement de délai séquentiels de session
- line vty 0 4 -- utilisation de modifier des paramètres de dépassement de délai de session Telnet/SSH
- exec-timeout 0
- session-timeout 0
- le terme len 0

Avant que vous commenciez le test, collectez un échantillon de ces commandes show sur AP. À un minimum collectez deux échantillons de cette sortie, chacun des deux avant et après la fin des tests avec l'utilisation de ces commandes show AP par l'intermédiaire du CLI :

- le terme len 0
- *show clock*
- affichez le tech
- affichez le manganèse de client de capwap
- affichez les dfs international do1
- show logging
- plus d'event.log
- gens du pays de format horaire d'affichage du show trace dot11_rst
- show trace dot11_rst
- gens du pays de format horaire d'affichage du show trace dot11_bcn
- show trace dot11_bcn

Collectez les ces AP met au point par l'intermédiaire du CLI :

- debug dot11 {d0 | } <MAC_address> d'adr du moniteur d1
- debug dot11 {d0 | } le mgmt de clients d'impression du suivi d1 introduit le Ba de txfail de xmt récepteur de txev de rxev
- terme lundi

Une fois le test est complet, utilisent cette commande de désactiver met au point :

- u tout

AP-COS aps

Cette section détaille met au point requis pour la gamme 1800/2800/3800 aps.

Pour éviter un délai d'attente de session AP au moment d'une session Telnet/SSH/console, utilisez ces commandes :

- exec-timeout 0

Avant que vous commenciez le test, collectez un échantillon des commandes show ci-dessous sur AP. À un minimum collectez deux échantillons de cette sortie, chacun des deux avant et après la

fin des tests avec l'utilisation de ces commandes show AP par l'intermédiaire du CLI :

- **le terme len 0**
- ***show clock***
- **affichez le tech**
- **affichez le <client_MAC-address> de statistiques de client**
- **affichez l'état à suivre NSS**
- **affichez les stats à suivre NSS**
- **show log**

Pour les Points d'accès de gamme 1800, collectez les ces AP met au point par l'intermédiaire du CLI :

- **<client_MAC-address> d'adr d'événements de niveau de client de debug dot11**
- **<client_MAC-address> d'adr d'erreurs de niveau de client de debug dot11**
- **<client_MAC-address> essentiel d'adr de niveau de client de debug dot11**
- **<client_MAC-address> d'adr de l'information de niveau de client de debug dot11**
- **<client_MAC-address> d'adr d'eapol de datapath de client de debug dot11**
- **<client_MAC-address> d'adr DHCP de datapath de client de debug dot11**
- **<client_MAC-address> d'adr d'ARP de datapath de client de debug dot11**
- **terme lundi**

Pour les Points d'accès de gamme 2800/3800, collectez les ces AP met au point par l'intermédiaire du CLI :

- **l'adresse de client-suivi du config AP ajoutent le <client_MAC-address>**
- **le filtre tout de client-suivi du config AP activent**
- **enable de console-log de sortie de client-suivi du config AP**
- **début de client-suivi du config AP**
- **terme lundi**

Une fois le test est complet, utilisent cette commande de désactiver met au point :

- **arrêt de client-suivi du config AP**

VIII. Captures de côté client

Capture collectez de Netmon 3.4 (Windows XP ou 7 seulement) ou de Wireshark paquet promiscueux de l'adaptateur WLAN du périphérique de client.

IX. captures OTA

captures 802.11n

- AirPCAP avec Wireshark
- MacBook Pro
- Professionnel d'OmniPeek, entreprise, etc.
- Assistant distant d'OmniPeek (ORA)
- Cisco AP en mode de renifleur

captures 802.11ac

- Pour des captures 11ac 3SS, vous pouvez utiliser des 2014 Macbook Pro ou une exécution postérieure 10.10.x ou plus élevé (n'utilisez pas le MacBook Air pour les captures 11ac si possible, en tant que lui est seulement un périphérique 2SS actuellement).
- Vous pouvez également utiliser des 2702, 3702 ou Cisco semblable AP en mode de renifleur.
- Pour les scénarios errants et avec l'utilisation du logiciel d'analyse réseau professionnel tel qu'OmniPeek de Savvius. Il est recommandé pour utiliser le multiple, les adaptateurs capables compatibles 802.11ac USB WLAN, tels que l'adaptateur de WiFi de Savvius pour OmniPeek (802.11ac), Netgear A6210, ou semblable.

XI. Annexe A - Conseils et astuces supplémentaires

Windows

Pour collecter quelques informations complémentaires quant à la connexion Sans fil en cours et à d'autres détails relatifs directement d'un PC Windows. Vous pouvez se servir de ces commandes relatives wlan de netsh dans la ligne de commande 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
```

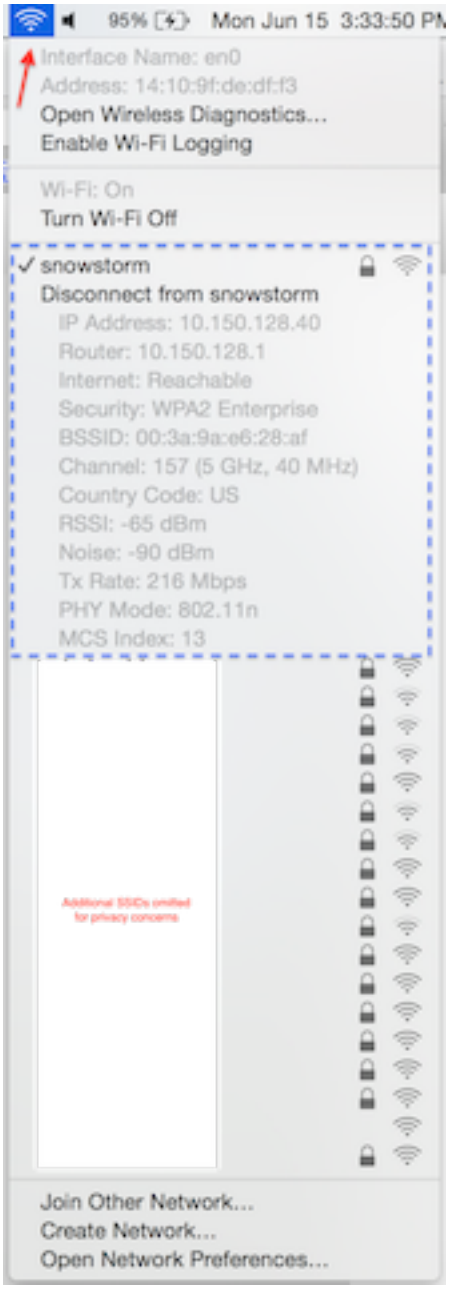
```
    Name                   : Wireless Network Connection
    Description            : Intel(R) Centrino(R) Advanced-N 6200 AGN
    GUID                   : 8fa038f8-74e0-4167-98f9-de0943f0096c
    Physical address       : 58:94:6b:3e:a1:d0
    State                  : connected
    SSID                   : 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  --
```

MaOS (autrefois SYSTÈME D'EXPLOITATION X)

Afin de collecter la sortie équivalente comme commande de **/all d'ipconfig** sur un PC Windows, vous pouvez à la place utiliser la commande commune de Linux/Unix de l'**ifconfig** de répertorier les informations détaillées pour toutes les interfaces réseau sur Apple MacBook. Comme nécessaire, vous pouvez également spécifier pour recevoir la sortie pour juste l'interface Sans fil indigène pour MacBook donné (en0 ou en1, il dépend du modèle). Comme cet exemple :

```
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
```

Afin d'obtenir un certain rapide mais les informations détaillées quant à la connexion Sans fil en cours sur MacBook. Vous pouvez également sélectionner l'icône de WiFi dans l'angle supérieur droit de l'appareil de bureau tandis que vous tenez simultanément la **case d'option** sur votre clavier suivant les indications de l'image.



Une autre option utile est d'utiliser la ligne de commande masquée aéroport appelé par utilitaire. Il est fortement recommandé pour utiliser seulement ceci avec votre propre MacBook ou un en service dans un environnement de travaux pratiques. Car quelques administrateurs réseau ne pourraient pas souhaiter accorder l'accès à cet utilitaire sur MacBook d'un utilisateur final, ainsi utilisent le niveau approprié de l'attention en conséquence. Pour poursuivre, présentez ceci dans le terminal sur MacBook en question :

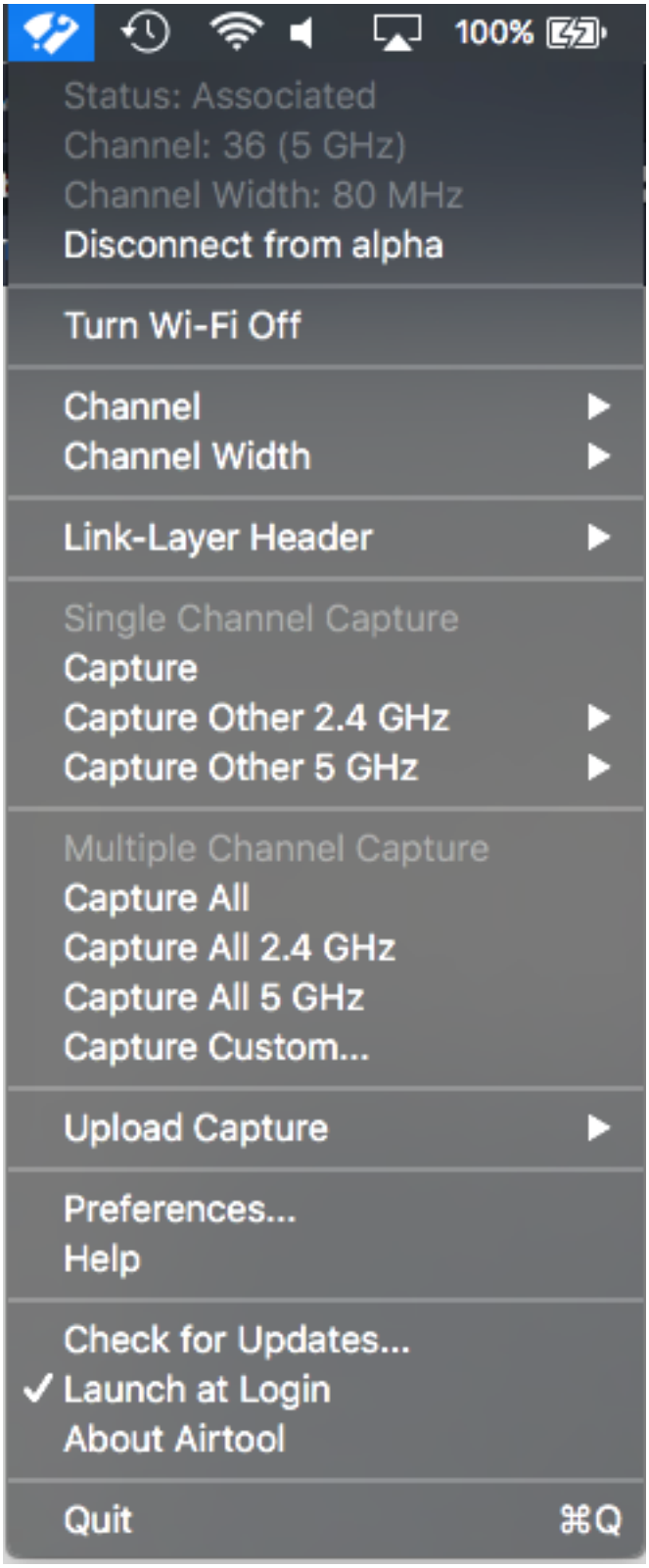
```
bash-3.2$ ifconfig en0
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
ether 14:10:9f:de:df:f3
inet6 fe80::1610:9fff:fede:dff3%en0 prefixlen 64 scopeid 0x4
inet 10.150.128.40 netmask 0xffffe000 broadcast 10.150.159.255
nd6 options=1<PERFORMNUD>
```

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

Maintenant vous pouvez inviter l'utilitaire CLI d'aéroport facilement. Un exemple dont inclut ceci :

```
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
```

Pour soulager plus loin le processus pour collecter une capture de paquet du canal OTA de 802.11 avec l'utilisation des capacités d'un MacBook Pro ou semblable fiable et simple. Vous pouvez accroître les capacités embeded dans le MaOS avec l'utilisation de la méthode Sans fil de diagnostics > de renifleur ou de semblable comme discuté précédemment, mais sur option vous pouvez utiliser un tiers utilitaire appelé aussi bien Airtool (OS X 10.8 et plus tard). L'avantage est une interface simple pour collecter rapidement une capture de paquet OTA, qui obtient enregistré directement à l'appareil de bureau avec juste quelques clics par l'app UI juste de la barre de menu principal sur votre écran.



Des liens des informations supplémentaires et de téléchargement pour Airtool peuvent être trouvés à cet URL :

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