Guía de Troubleshooting por problemas de interoperabilidad del cliente de red inalámbrica con CUWN

Contenido

Introducción

Este documento describe detalladamente qué informaciones necesitas de ser recogido inicialmente para investigar y para resolver problemas con eficacia tales problemas de interoperabilidad inalámbricos cuando se presentan con la solución unificada de la red inalámbrica de Cisco (CUWN). La necesidad de tal enfoque amplio llega a ser cada vez más importante con nunca el crecimiento en los números y las combinaciones de dispositivos de red inalámbrica de cliente y de radios del punto de acceso.

Prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Tecnología inalámbrica de Cisco AP
- Reguladores del Wireless LAN (WLC)
- Dispositivos de red relacionados

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

> Nota: La audiencia prevista para este documento es los ingenieros y los administradores experimentados de la red inalámbrica que son ya familiares con el uso, la configuración y el troubleshooting de estos temas.

Antecedentes

Puede ser común encontrar que dado los diversos dispositivos del cliente que exista y continúe para ser desarrollado. Una variedad de problemas pueden presentarse en lo que respecta a establecen, mantienen, o salir simplemente la mayoría de su conexión a la red inalámbrica y soportar la infraestructura.

Esto puede bajar a menudo a un problema de la Configuración simple de parte del dispositivo del cliente y/o de la infraestructura de red inalámbrica sí mismo. Sin embargo, esto se puede atribuir en algunos casos a un problema de interoperabilidad en lo que respecta a un dispositivo del cliente específico y a los componentes que lo soporten (es decir supplicant, adaptador WLAN, driver inalámbrico, etc.), y/o a los AP en la pregunta. Como ingenieros inalámbricos, tales problemas de interoperabilidad plantean una oportunidad de identificar, de resolver problemas, y de resolver los desafíos potencialmente complejos.

La información adicional a qué se delinea en este artículo se pudo pedir y necesitar para ser recogido caso por caso, dado el número sin límite de variables que pudieron dictar tales requisitos. Sin embargo, la información detallada aquí es una guía de consulta genérica para abordar cualquier problema de interoperabilidad potencial del cliente de red inalámbrica.

I. Definición del problema

El primer paso para abordar con eficacia cualquier problema con el intento para conseguir resuelto, es definir exactamente el problema a mano. Para hacer así pues, asegúrese que eso en un mínimo de estas preguntas está preguntada y sus respuestas están documentadas claramente:

- ¿El problema se restringe a un modelo específico de AP y/o del tipo de la radio (es decir 2.4 gigahertz contra 5 gigahertz)?
- ¿El problema se observa solamente en las versiones del software WLC específicas?
- Es el problema experimentado con solamente las versiones específicas del tipo de cliente y/o del software (es decir versión de OS, versión del driver de la red inalámbrica (WLAN), los etc.)
- ¿Hay otros dispositivos de red inalámbrica que no experimenten este problema? ¿Si es así cuáles son ellos?
- ¿Es el problema reproductivo mientras que el cliente está conectado con una configuración inalámbrica simplificada tal como un SSID abierto, con un ancho del canal de 20 MHz, y 802.11ac inhabilitado? (es decir hace el problema suceden en el modo 802.11n contra el modo 802.11ac solamente?).
- ¿Si el problema no es reproductivo con un SSID abierto, en qué Configuración de seguridad mínima el problema se ve? (es decir PSK o 802.1x en la red inalámbrica (WLAN)).
- ¿Cuáles eran la configuración en funcionamiento y las versiones de software anteriores?

II. Configuración del WLC y registros generales

Funcionamiento-Config

Sin la excepción, está de la necesidad absoluta para recoger la configuración del WLC del cliente para un estudio detallado de las características usadas por el cliente, su configuración específica, y otros tales detalles. Para hacer así pues, usted debe establecer una sesión del telnet/SSH a los WLC en la pregunta y salvar la salida de estos comandos CLI a un archivo de texto:

```
config paging disable

show run-config
```

La salida completa de los funcionamiento-config se prefiere siempre, como incluye la información detallada en lo que respecta a los AP unidos y a la información asociada RF, etc. Aunque en algunos casos y situaciones, por ejemplo cuando usted trabaja inicialmente con un WLC con un gran número de AP unidos (es decir 8510 WLC con 2500+ AP). Puede ser que sea preferido para recoger inicialmente apenas la configuración del WLC sin tal información AP para el estudio rápido, mientras que los funcionamiento-config completos de la demostración pudieron tomar 30 minutos o más para completar dado el número de AP. Sin embargo, puede ser que todavía sea necesario recoger los funcionamiento-config completos hechos salir en otro momento.

Para hacer así pues, usted puede recoger opcionalmente la salida de estos comandos CLI a un archivo de texto:

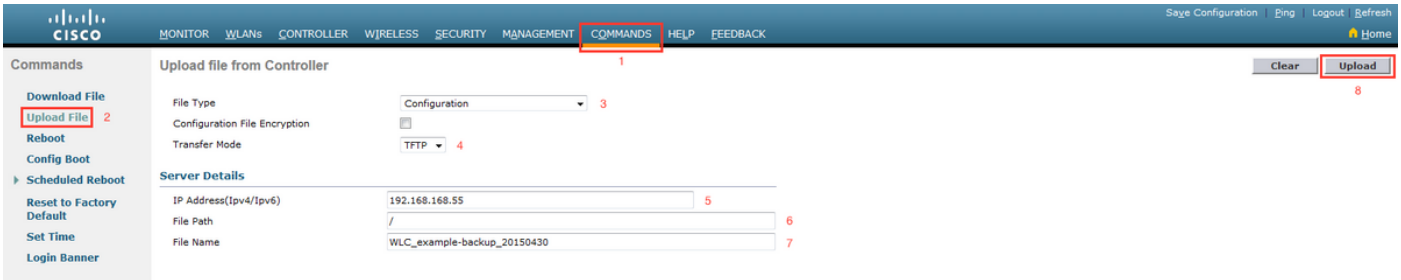
```
config paging disable

show run-config no-ap

show wlan apgroups
```

Archivo de configuración del WLC

Además de los funcionamiento-**config de la demostración** o de la salida ninguno-**ap de los funcionamiento-config de la demostración**, también se recomienda para recoger un backup completo de la configuración del WLC también. Esto seve de ayuda, si un laboratorio reconstruye las necesidades de ser conducido por la escalada TAC/HTTS y BU, para intentar y para reproducir el problema del cliente en un entorno del laboratorio de Cisco. Un respaldo del WLC se puede recoger vía el GUI o el CLI del WLC en la pregunta, con el uso del TFTP o del FTP de salvar el archivo de configuración al servidor FTP del externo TFTP/. El ejemplo abajo muestra el uso del GUI y del CLI para salvar un respaldo del WLC, con el uso del TFTP:

GUI

Comandos > archivo > configuración > carga de la carga tal y como se muestra en de la imagen.



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 del WLC

Ahora, usted también quiere recoger los registros actuales del WLC para el estudio adicional según las necesidades. Idealmente, usted quiere recoger estos registros inmediatamente

después de su prueba con un cliente de red inalámbrica por el que el problema señalado esté reproducido. Si el cliente exporta los registros del WLC a un servidor Syslog externo, después usted quiere extraerlos de allí. Si no, usted puede salvar el msglog y el traplog salvado actualmente localmente en el WLC guardando a esta sesión CLI hizo salir a otro archivo de texto:

```
config paging disable

show msglog

show traplog
```

III. Detalles e información del dispositivo del cliente

El siguiente paso es recolectar tanta información y los específicos en lo que respecta a los dispositivos del cliente funcionando que experimentan un problema de interoperabilidad inalámbrico potencial. Tal información se debe incluir, sino limitar no no necesariamente a éstos:

- Tipo de cliente (es decir tablilla, smartphone, cuaderno PC, etc.)
- El dispositivo hace y modela
- Versión de OS
- Modelo del adaptador WLAN
- Versión del driver del adaptador WLAN
- Supplicant usado (es decir Windows cero Config/Config autos, Intel PROSet, etc.)
- Seguridad configurada para uso del cliente de red inalámbrica y red inalámbrica (WLAN) (es decir ábrase, PSK, EAP-PEAP/MSCHAPv2, etc.)

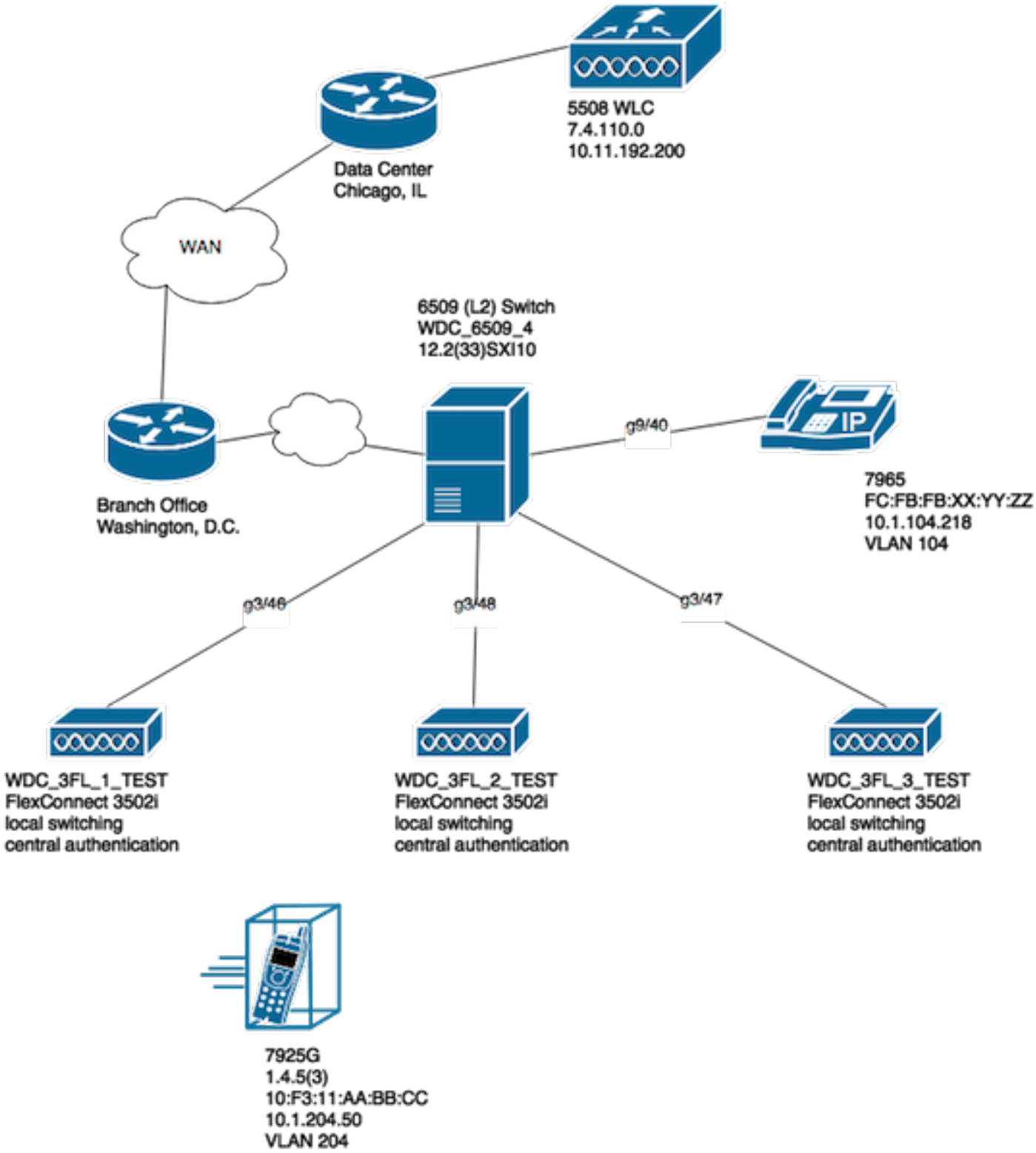
Nota: Cualquier parámetro del cliente cambiado de las configuraciones predeterminadas proporcionó por el vendedor en la pregunta (es decir estado del sueño, parámetros de itinerancia, U-APSD, etc.).

Nota: Cualquier información adicional o nota en lo que respecta a los dispositivos del cliente hasta los cuales incluye el screenshots de su configuración relacionada de la red inalámbrica (WLAN), y así sucesivamente se debe también incluir según las necesidades.

IV. Topología de red

Para acelerar más lejos esfuerzos por Troubleshooting y el proceso de la Análisis de la causa de raíz (RCA), se recomienda siempre para proporcionar un diagrama de la topología de red detallado y completo. El diagrama de la topología de red debe no sólo incluir los detalles sobre la red y la infraestructura de red inalámbrica, pero también proporciona una penetración en los dispositivos inalámbricos en la pregunta que actúa dentro de la red (es decir impresoras/los escáneres, qué VLA N del cliente son funcionando, etc.) y de sus ubicaciones en relación con una otras.

Varias herramientas (es decir Microsoft Visio, draw.io, etc.) y una variedad de estilos se pueden utilizar para crear tal diagrama de la red. El aspecto importante es asegurarse simplemente de que la información adecuada está reflejada claramente en el diagrama proporcionado para el estudio por todos los partidos y vendedores implicados. Una topología de red de muestra que captura básico, solamente información útil en lo que respecta a la infraestructura y a los dispositivos del cliente tal y como se muestra en de la imagen.



V. Detalles adicionales de la pista y los específicos

Para ayudar a asegurarse de que la información apropiada está recogida a la hora de cualquier prueba con los dispositivos del cliente que los usuarios finales experimentan los problemas con. Se recomienda de forma preventiva para crear una hoja de cálculo o similar para registrar todos los problemas de cliente y detalles relacionados observados a la hora de la prueba, tal como este ejemplo:

Dirección MAC	Nombre de usuario	Descripción del síntoma señalado	Síntoma observado usuario final	Default gateway Y/N del	Estatus de la señal de WiFi (conectado/intentando	Registre el ip

		del tiempo	ping	conectar)	
xxyy.aabb.0011 test_user1	Intermitentemente desconexiones del Punto de acceso.	Conectividad de red y asociación de red inalámbrica perdidas de AP3.	N	El intentar conectar	ifconfig en0 en0: MTU 15 flags=8863<U éter xx:yy:a inet6 fe80:: 0x4 el netmask 192.168.10.2 nd6 options media: auto estatus: act

La meta de este ejercicio es ayudar a documentar y a determinar un modelo común del interés, así como a conseguir un cuadro exacto de los problemas a mano. Una vez que esta hoja de cálculo se prepara para ser utilizada para la obtención de datos, usted está listo ahora para comenzar sus pruebas.

> Nota: Todos los debugs y capturas de paquetes recogidos necesitan ser sincronizados al mismo servidor NTP para una correlación más fácil con los registros, y se deben tomar al mismo tiempo para cualquier prueba dada.

> Nota: Proporcione una hora precisa de cuando se observa el problema, y cuando el problema parece recuperarse (si procede).

> Nota: Recoja siempre los debugs filtrados por el MAC Address del cliente en el AP y el WLC.

> Nota: No funcione con los comandos show and debug en el AP dentro de la misma sesión Telnet/SSH/console, éstos debe ser hecho por separado en una diversa sesión por consiguiente.

> Nota: Los debugs AP se prefieren para ser tomados en el telnet/SSH contra la consola, pues la consola es típicamente demasiado lenta ser eficaz.

VI. WLC - Comandos show and debug

Cuando las pruebas se conducen para reproducir y para resolver problemas los problemas de interoperabilidad potenciales del cliente de red inalámbrica, es imprescindible que los debugs y los registros adicionales estén recogidos de la infraestructura de red inalámbrica funcionando. Estas dos secciones pueden explicar detalladamente los registros específicos y la salida de los debugs inicial que se deben recoger del WLC y del AP, respectivamente.

Comandos Debug del WLC

```
config sessions timeout 0
```

```
debug client <MAC_address> debug dhcp message enable
```

En cuanto a la naturaleza del problema a mano, usted puede también agregar estos debugs del WLC caso por caso:

- permiso del detalle aaa del debug - utilice esto si hay asuntos relacionados de la autenticación con el servidor de AAA
- haga el debug del permiso de los eventos aaa - utilice esto si hay asuntos relacionados de la autenticación con el servidor de AAA
- haga el debug del aaa todo el permiso - utilice esto para los problemas del auth; la salida para este debug es prolija así que utilícelo solamente cuando absolutamente es necesario (es decir para los casos de la invalidación AAA, el etc.)
- las manos de la movilidad del debug - utilice cuando allí están vagando por los problemas entre el WLCs

Una vez que el problema se reproduce con el cliente de red inalámbrica en la pregunta, y toda la información delineada en las secciones anteriormente y después de esto se recogen y se documentan. Para ejecutar estos comandos CLI, usted debe inhabilitar los debugs en el WLC.

```
debug disable-all
```

Comandos show del WLC

```
config paging disable

show time

show client detail <MAC_address>

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

Como se mencionó anteriormente, asegure para ejecutar los debugs del WLC en una sesión del telnet/SSH y para recoger la salida para estos comandos show en otro telnet/SSH al WLC. Usted debe hacer lo mismo para recoger los comandos de debugs y show AP hizo salir detallado en éstos la sección.

VII. AP - comandos show and debug

Puntos de acceso ligeros de Cisco IOS®

Antes de que usted comience cualquier debug en cualquier IOS ligero AP implicado en la prueba, tal como los 2600, los 2700, los 3700 o los puntos de acceso de Cisco modelo anteriores. Usted debe primero ejecutar estos comandos CLI en el AP, para evitar un descanso a la hora de una sesión Telnet/SSH/console al AP en la pregunta cuando sus pruebas del cliente:

```
debug capwap console cli

config t

line vty 0 4

exec-timeout 0

session-timeout 0
```

Usted puede también seguir los siguientes pasos para utilizar la conexión de consola y para substituir la declaración del **line vty 0 4** por la **línea consola 0** en lugar de otro, para inhabilitar el ejecutivo y los tiempos de espera de la sesión para un serial/una conexión de consola por

consiguiente.

- línea consola 0 - utilice para modificar los parámetros de tiempo de espera de la sesión seriales
- el line vty 0 4 - utilice para modificar los parámetros de tiempo de espera de la sesión del telnet/SSH

Comandos show AP

Antes de que usted comience la prueba, usted debe primero recoger una muestra de estos comandos show en el AP. Usted debe recoger la salida de estos comandos show por lo menos dos veces para cada prueba que implique al cliente de red inalámbrica en la pregunta; ambos antes y después de la prueba son completos.

```
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
```

Comandos Debug AP

Una vez que usted ha recogido la salida inicial de los comandos show ya mencionados, usted puede ahora habilitar los debugs en el mismo Punto de acceso en una sesión separada del telnet/SSH como se muestra. Asegure para salvar la salida entera a un archivo de texto.

```
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
```

Leyenda

Indicador	Descripción
d0	Radio 2.4 gigahertz (slot0)
d1	Radio 5 gigahertz (slot 1)
mgmt	Paquetes de administración de la traza
vagos	Información del bloque ACK de la traza
receptor	Paquetes recibidos de la traza
claves	Claves determinadas de la traza
rxev	La traza recibió los eventos

txev	La traza transmite los eventos
txrad	La traza transmite para radiar
xmt	La traza transmite los paquetes
txfail	Fallas de transmisión de la traza
tarifas	Cambios de la tarifa de la traza

Para inhabilitar los debugs en el AP una vez que se completa la prueba y el proceso de la obtención de datos, usted puede ejecutar este comando CLI en el AP:

```
u all
```

Puntos de acceso AP-COS

Para 802.11ac los Puntos de acceso capaces de la onda 2 y posterior, por ejemplo los 1800, los 2800 y los Puntos de acceso del modelo 3800. Este un más nuevo modelo AP introduce totalmente un nuevo sistema operativo para las Plataformas del Punto de acceso designadas AP-COS. Como tal, no los comandos all según lo utilizado previamente en el Cisco IOS ligero tradicional basaron los Puntos de acceso como detallado arriba todavía se aplican. Si cuando usted resuelve problemas un problema implica el problema de interoperabilidad con los diversos dispositivos y AP-COS AP modelo del cliente STA, después este la información se debe recoger del Punto de acceso AP-COS implicado con la prueba equivalente.

Antes de que usted comience cualquier debug en cualquier AP-COS modela el AP implicado en la prueba. Usted debe primero ejecutar este el comando CLI en el AP, para evitar un descanso a la hora de una sesión Telnet/SSH/console al AP en la pregunta cuando sus pruebas del cliente:

```
exec-timeout 0
```

Comandos show AP-COS

Antes de que usted comience la prueba, usted debe primero recoger una muestra de estos comandos show en el AP. Usted debe recoger la salida de estos comandos show por lo menos dos veces para cada prueba que implique al cliente de red inalámbrica en la pregunta; ambos antes y después de la prueba son completos.

```
term len 0

show clock show tech

show client statistics <client_MAC-address>

show cont nss status

show cont nss stats

show log
```

1800 Series | Comandos Debug AP-COS

Estos debugs son específicos a las 18xx Series de Puntos de acceso. Esto es debido al hecho que los chipsetes usados para las 1800 Series de AP diferencian de ésos encontrados en los Puntos de acceso de las 2800/3800 Series, y un diverso conjunto de los debugs es requerido así en este escenario por la comparación. Los debugs correspondientes para las 2800/3800 Series AP se cubren en la siguiente sección.

Una vez que usted ha recogido la salida inicial de los comandos show ya mencionados, usted

debe ahora habilitar los debugs en los mismo 1800 Puntos de acceso en una sesión separada del telnet/SSH como se muestra. Asegure para salvar la salida entera a un archivo de texto.

```
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>
```

En algunos casos, usted puede ser que necesite también permitir a los debugs adicionales en el 18xx AP para resolver problemas más lejos los problemas de interoperabilidad del cliente. Sin embargo, éste debe ser solamente if/as hecho pedido por un ingeniero de Cisco TAC para una solicitud de servicio/un caso correspondientes.

Pues los debugs adicionales pudieron no sólo ser lejos más prolijos en su salida pero puede también introducir la carga adicional en el AP también por lo tanto que requiere adicional mide el tiempo para el análisis apropiado. Cuál bajo ciertas condiciones puede potencialmente interrumpir el servicio, si muchos dispositivos del cliente intentan conectar con el mismo AP bajo la prueba o variables similares.

Para inhabilitar los debugs en el Punto de acceso variable AP-COS - si en 1800 o las 2800/3800 Series AP - una vez se completa la prueba y el proceso de la obtención de datos, usted pueden ejecutar este comando CLI en el AP:

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

2800/3800 Series | Comandos Debug AP-COS

Una vez que usted ha recogido la salida inicial de los comandos show ya mencionados, usted debe ahora habilitar los debugs en el mismo 2800/3800 Punto de acceso en una sesión separada del telnet/SSH como se muestra. Asegure para salvar la salida entera a un archivo de texto.

```
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
```

Para inhabilitar los debugs en las 1800/2800/3800 Series AP una vez que se completa la prueba y el proceso de la obtención de datos, usted puede ejecutar este comando CLI en el AP:

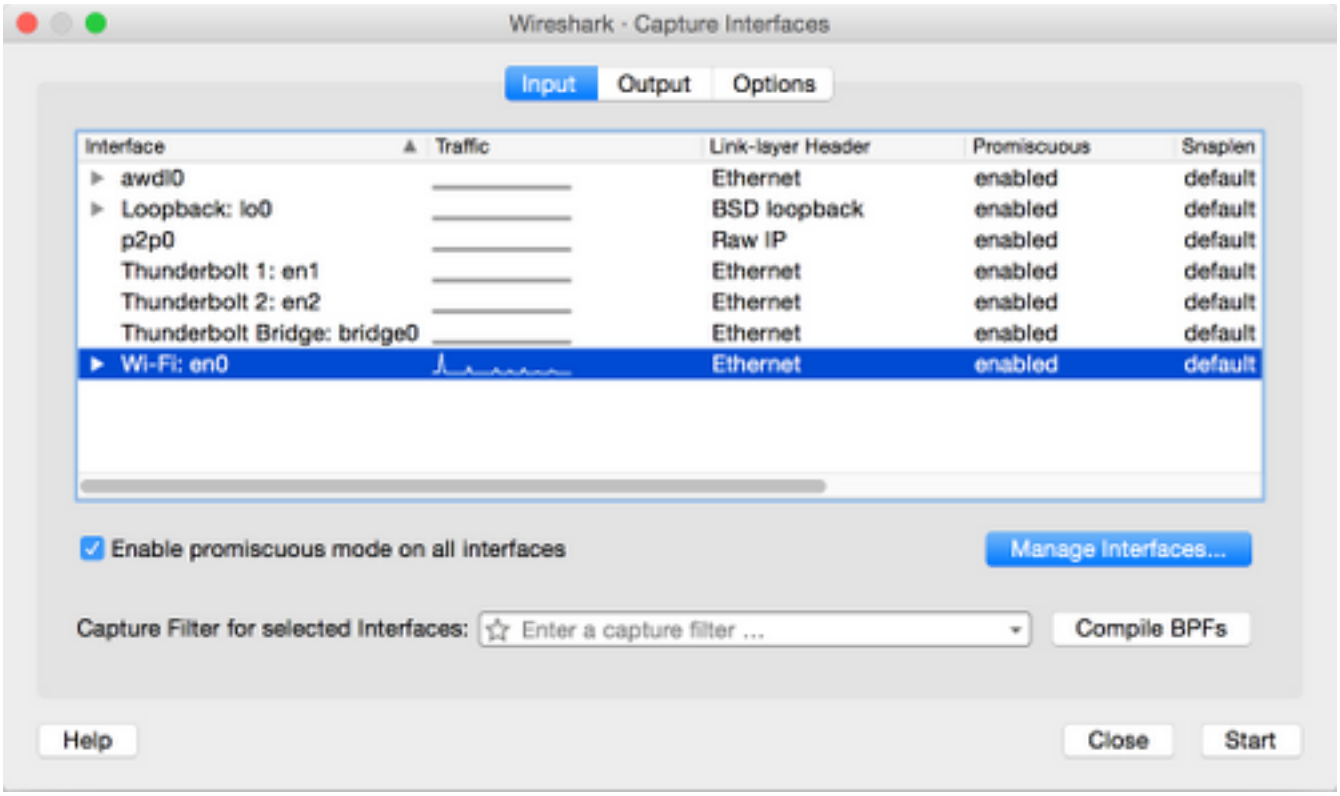
```
config ap client-trace stop
```

VIII. Capturas de paquetes laterales del cliente

Del dispositivo del cliente funcionando si es un cuaderno PC, MacBook o similar, usted debe recoger a la captura de paquetes del modo promiscuo de la interfaz inalámbrica del dispositivo del cliente usado para reproducir el problema. Las utilidades comunes como el Netmon 3.4 (Windows solamente) o Wireshark se pueden descargar y utilizar fácilmente para recoger esta captura y para salvarla a un archivo *.pcap. Depende del dispositivo, pudo también haber medios de

recoger un tcpdump o similar del cliente en la pregunta, así que usted puede ser que necesite consultar con el fabricante del dispositivo del cliente para la ayuda a este respecto.

Aquí está un ejemplo para configurar una captura de Wireshark para la interfaz inalámbrica en un MacBook Pro:



Como con cualquier captura de paquetes, sin importar qué utilidad se utilice para recogerlo, asegure para salvar el archivo en un formato de archivo del pcap (es decir *.pcap, *.pcapng, *.pkt, etc.). Éste es asegurarse de que no sólo los ingenieros de Cisco en cualquier departamento pueden ver los archivos de la captura de paquetes fácilmente, pero los ingenieros de los otros vendedores y las organizaciones también (es decir Intel, Apple, etc.). Esto permite un proceso más inconsútil de la cooperación y de la Colaboración, que facilita más lejos Cisco y a los vendedores del dispositivo del cliente para trabajar mejor junto para investigar y para resolver cualquier problema de interoperabilidad potencial.

IX. Sobre - Capturas de paquetes del aire (OTA)

Para resolver problemas con eficacia cualquier problema de interoperabilidad inalámbrico potencial o existente, es crucial recoger a una captura de paquetes de la calidad OTA del problema. Esto permite la análisis detallado de la comunicación de red inalámbrica real del 802.11 entre el cliente de red inalámbrica y las radios del Punto de acceso en la pregunta, además de dan la perspectiva adicional a los registros del lado y de la infraestructura de red inalámbrica del cliente, a los debugs, al etc. Éste es un Paso crítico que debe ser realizado para cada prueba de un problema de interoperabilidad inalámbrico potencial, sin la excepción.

Mide el tiempo sin embargo, a menudo del cliente final no se equipa ni se prepara correctamente para recoger a las capturas de paquetes OTA. Éste es un obstáculo común que de los ingenieros la cara inalámbrica a menudo, y ellas debe trabajar con el cliente para superar esto de una variedad de maneras. Este artículo de los foros del soporte de Cisco puede servir como buena punta del comienzo ayudar a dirigir y a educar al cliente por consiguiente:

el oler/captura de paquetes de la Tecnología inalámbrica del 802.11

Es de la de suma importancia esa la captura de paquetes OTA se recoja en un formato de archivo del pcap (es decir *.pcap, *.pcapng, *.pkt, etc.), e incluye los meta datos del 802.11 (es decir RSSI, el canal, la velocidad de datos, el etc.). El sniffer OTA se debe también mantener el muy cerca al dispositivo del cliente en la pregunta siempre durante las pruebas, para asegurar una perspectiva exacta del tráfico enviado y recibido a/desde el dispositivo del cliente que es probado.

> Nota: Si las pruebas en la pregunta implican un escenario de itinerancia del dispositivo del cliente, por el que más de un canal del 802.11 necesite ser monitoreado en una captura de paquetes agregada. Entonces no se recomienda actualmente para utilizar el analizador de AirMagnet WiFi de las redes de la platija.

La razón de esto es debido al hecho de que guardan las capturas de paquetes agregadas con el uso de esta utilidad actualmente en un formato de archivo propietario, y no en un formato del estilo del pcap que se pueda ver fácilmente en Wireshark u otras utilidades similares. Asegúrese de que su captura de paquetes OTA está en un formato de archivo NON-propietario, esto ayuda a asegurarse de que todos los partidos y vendedores implicados pueden revisar fácilmente cualquier capturar archivo siempre, y ayuda en última instancia a apresurar cualesquiera esfuerzos de la resolución.

en un formato que sea legible por Wireshark actual, y que incluye los meta datos del 802.11 (RSSI, canal, velocidad de datos) - vea más en: https://supportforums.cisco.com/document/75331/80211-wireless-sniffing-packet-capture#sthash.Xhlx5LSS.dpuf
Aquí están algunos métodos usuales para recoger a una captura de paquetes OTA:

- AirPCAP con Wireshark
- MacBook Pro
- Profesional del OmniPeek, empresa del OmniPeek, etc.
- Ayudante remoto del OmniPeek (ORA)
- Cisco AP en el modo del sniffer

capturas 802.11n

Para las capturas de paquetes OTA que implica a los clientes de red inalámbrica 802.11n, hay actualmente más flexibilidad y facilidad de empleo. Esto es debido a una variedad más amplia de adaptadores WLAN disponibles de la Tecnología inalámbrica USB que se puedan utilizar fácilmente con varias herramientas, tales como OmniPeek y otros.

Tome la nota en cuanto a cómo las capacidades del adaptador de red inalámbrica específico usado para recoger una captura 802.11n OTA comparan con las capacidades del chipset real de la red inalámbrica (WLAN) usado por los dispositivos del cliente que usted intenta resolver problemas. Por ejemplo, si el dispositivo del cliente experimenta un problema de interoperabilidad inalámbrico potencial que utilice el chipset capaz espacial 802.11n de la secuencia del a2 (2SS). Entonces se recomienda altamente para asegurarse de que el adaptador de red inalámbrica usado para recoger a una captura de paquetes OTA es también un 2SS o un mejor adaptador, con 802.11n o más nuevas especificaciones.

capturas 802.11ac OTA

Para 3 capturas espaciales 802.11ac de la secuencia (3SS), usted puede utilizar las capacidades nativas el oler de los 2014 MacBook Pro modelo o posterior Mac OS X corriente 10.10.x o más arriba. Si resuelve problemas el dispositivo del cliente espacial de la secuencia 802.11ac del a2, usted puede también utilizar un MacBook Air para las capturas 802.11ac. El modelo del aire del chipsets de la red inalámbrica (WLAN) del uso 2SS de MacBooks solamente actualmente a la hora de esta escritura. Usted puede referir al artículo abajo de los foros del soporte de Cisco para las instrucciones en cómo recoger a las capturas de paquetes OTA con el uso de Mac OS X, con una variedad de métodos:

Tecnología inalámbrica que huele con el uso de Mac OS X 10.6+

Usted puede también utilizar las 2702/2802/3702/3802 Series o el AP similar en el modo del sniffer para recoger a una captura de paquetes apropiada 802.11ac con 3SS. Usted puede también referir al recurso abajo para un objeto list actual de los adaptadores de red inalámbrica disponibles 802.11ac. Algunos de los cuales pueden poder potencialmente ser utilizado con las herramientas comunes como el OmniPeek y otros para recoger a una captura de paquetes 802.11ac (es decir chipsets de Ralink, de Atheros, del etc.):

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

Usted puede también utilizar las 2702/2802/3702/3802 Series o el AP similar en el modo del sniffer para recoger a una captura de paquetes apropiada 802.11ac con 3SS. Para la conveniencia, las instrucciones paso a paso en cómo configurar Cisco AP en el modo del sniffer y recoger a una captura de paquetes OTA se pueden encontrar en el artículo abajo de los foros del soporte de Cisco:

Cisco AP en el modo del sniffer

Para resolver problemas los escenarios de itinerancia con un dispositivo de red inalámbrica de cliente, el desafío común es recoger con eficacia a una captura de paquetes OTA a través de los múltiples canales. Este método simultáneamente de monitorear los canales múltiples del 802.11 es alcanzado por la colección de captura de paquetes agregada OTA. Se recomienda para utilizar los adaptadores WLAN capaces múltiples, compatibles 802.11ac USB con un software de Análisis de red compatible para alcanzar esto. Algunos adaptadores WLAN capaces comunes 802.11ac USB incluyen el adaptador de Savvius WiFi para el OmniPeek (802.11ac), Netgear A6210, o similar.

X. Resumen

Aquí está una recapitulación abreviada de la información que necesita ser recogida para resolver problemas con eficacia un problema de interoperabilidad potencial del cliente de red inalámbrica con un CUWN. Esta sección se piensa para servir como sección de referencia rápida, según las necesidades.

I. Definición del problema

- ¿El problema se restringe a un modelo específico del Punto de acceso y/o del tipo de la radio (2.4 gigahertz contra 5 gigahertz)?
- ¿El problema se observa solamente en las versiones específicas del software del regulador del Wireless LAN (WLC)?
- Es el problema experimentado con solamente las versiones específicas del tipo de cliente y/o

del software (es decir versión de OS, versión del driver de la red inalámbrica (WLAN), los etc.)
- ¿Hay otros dispositivos de red inalámbrica que no experimenten este problema? ¿Si es así cuáles son ellos?
- ¿Es el problema reproductivo mientras que el cliente está conectado con un SSID abierto, un ancho del canal de 20 MHz, y 802.11ac inhabilitado? (es decir hace el problema suceden en el modo 11n contra el modo 11ac solamente)
- ¿Si el problema no es reproductivo con un SSID abierto, en qué Configuración de seguridad mínima el problema se ve? (es decir PSK o 802.1x en la red inalámbrica (WLAN))
- ¿Cuál era la configuración en funcionamiento y las versiones de software anteriores?

II. Configuración y registros del WLC

Recoja esto del CLI de los WLC en la pregunta:

- neutralización de la paginación de los config
- muestre los funcionamiento-config

Alternativamente, usted puede también recoger apenas éstos hechos salir según las necesidades:

- neutralización de la paginación de los config
- muestre los funcionamiento-config ninguno-ap
- muestre los apgroups wlan

Respaldo de la configuración del WLC vía TFTP, FTP, etc. (GUI: **Comandos > archivo > configuración de la carga**)

Syslog del WLC

III. Información del dispositivo del cliente

- Tipo de cliente (es decir tablilla, smartphone, cuaderno PC, etc.)
- El dispositivo hace y modela
- Versión de OS
- Modelo del adaptador WLAN
- Versión del driver del adaptador WLAN
- Supplicant usado (es decir Windows cero Config/Config autos, Intel PROSet, etc.)
- Seguridad configurada para uso del cliente de red inalámbrica y red inalámbrica (WLAN) (es decir ábrase, PSK, EAP-PEAP/MSCHAPv2, etc.)

  Nota: Cualquier parámetro del cliente cambiado de las configuraciones predeterminadas proporcionó por el vendedor en la pregunta. (es decir estado del sueño, parámetros de itinerancia, U-APSD, etc.)

IV. Diagrama de la topología de red

Esto debe incluir una representación y/o los detalles en lo que respecta a los dispositivos de red inalámbrica en la red (es decir impresoras/escáneres, WLCs, los etc.)

V. Cree una hoja de cálculo para registrar todos los problemas de cliente

Ejemplo:

Dirección MAC	Nombre de usuario	Descripción del síntoma señalado	Síntoma observado usuario final del tiempo	Default gateway Y/N del ping	Estatus de la señal de WiFi (conectado/intentando conectar)	Registre el ipconfig /all (o equivalente)

La meta de este ejercicio es ayudar a identificar un modelo común, y a mostrar una imagen más exacta de los problemas as mano.

VI. Comandos show and debug en el WLC

Recoja estos debugs del WLC vía el CLI:

- descanso de sesiones de los config 0
- cliente del debug **<MAC_address>**
- permiso del mensaje DHCP del debug

Agregue los debugs adicionales sobre caso por caso la base:

- haga el debug del permiso del detalle aaa - utilice esto si hay asuntos relacionados de la autenticación con el servidor de AAA
- haga el debug del permiso de los eventos aaa - utilice esto si hay asuntos relacionados de la autenticación con el servidor de AAA
- haga el debug del aaa todo el permiso - utilice esto para los problemas del auth; esto es prolijo así que utilícelo solamente cuando es necesario (es decir para la invalidación AAA encajona el etc)
- las manos de la movilidad del debug - utilice al vagar por los problemas entre el WLCs

Recoja la salida para los comandos show del WLC vía el CLI:

- neutralización de la paginación de los config
- show time
- muestre el detalle del cliente **< el MAC address del client>** (observe al estado del cliente en el WLC)
- Haga ping al cliente del WLC

Una vez que la prueba es completa, utilice este comando de parar todos los debugs actuales en el WLC:

- haga el debug de neutralización-todo

VII. Comandos show and debug en el AP

Cisco IOS ligero AP

Esta sección detalla los debugs requeridos para las 1700/2700/3700 Series o los Puntos de acceso modelo anteriores.

Para evitar un tiempo de espera de la sesión AP a la hora de una sesión Telnet/SSH/console, utilice estos comandos:

- haga el debug de la consola cli del capwap
- config t
- línea consola 0 -- utilice para modificar los parámetros de tiempo de espera de la sesión seriales
- line vty 0 4 -- utilice para modificar los parámetros de tiempo de espera de la sesión del telnet/SSH
- EXEC-descanso 0
- sesión-descanso 0
- el término len 0

Antes de que usted comience la prueba, recoja una muestra de estos comandos show en el AP. En un mínimo recoja dos muestras de esta salida, ambos antes y después de la realización de las pruebas con el uso de estos comandos show AP vía el CLI:

- el término len 0
- *show clock*
- show tech
- muestre el manganeso del cliente del capwap
- muestre los dfs internacional do1
- show logging
- más event.log
- muestre el local del formato de hora de la visualización de la traza dot11_rst
- muestre la traza dot11_rst
- muestre el local del formato de hora de la visualización de la traza dot11_bcn
- muestre la traza dot11_bcn

Recoja estos debugs AP vía el CLI:

- haga el debug del dot11 {d0 | } addr del monitor d1 <MAC_address>
- dot11 del debug {d0 | } el mgmt de los clientes de la impresión de la traza d1 cierra los vagos del txfail del xmt receptor del txev del rxev
- término lunes

Una vez que la prueba es completa, utilice este comando de inhabilitar los debugs:

- u todo

AP-COS AP

Esta sección detalla los debugs requeridos para las 1800/2800/3800 Series AP.

Para evitar un tiempo de espera de la sesión AP a la hora de una sesión Telnet/SSH/console, utilice estos comandos:

- EXEC-descanso 0
- Antes de que usted comience la prueba, recoja una muestra de los comandos show abajo en el AP. En un mínimo recoja dos muestras de esta salida, ambos antes y después de la realización de las pruebas con el uso de estos comandos show AP vía el CLI:

- el término len 0
- *show clock*
- show tech
- muestre el <client_MAC-address> de las estadísticas del cliente
- muestre el estatus continuado NSS
- muestre el stats continuado NSS
- show log

Para los Puntos de acceso de las 1800 Series, recoja estos debugs AP vía el CLI:

- haga el debug del **<client_MAC-address> del** addr de los eventos del nivel del cliente del dot11
- haga el debug del **<client_MAC-address> del** addr de los errores del nivel del cliente del dot11
- haga el debug del **<client_MAC-address>** crítico del addr del nivel del cliente del dot11
- haga el debug del **<client_MAC-address> del** addr de la información del nivel del cliente del dot11
- haga el debug del **<client_MAC-address> del** addr del eapol del datapath del cliente del dot11
- haga el debug del **<client_MAC-address> del** addr DHCP del datapath del cliente del dot11
- haga el debug del **<client_MAC-address> del** addr arp del datapath del cliente del dot11
- llame lunes

Para los Puntos de acceso de las 2800/3800 Series, recoja estos debugs AP vía el CLI:

- el direccionamiento de la cliente-traza ap de los config agrega el **<client_MAC-address>**
- el filtro todo de la cliente-traza ap de los config habilita
- permiso del registro de la consola de la salida de la cliente-traza ap de los config
- comienzo de la cliente-traza ap de los config
- término lunes

Una vez que la prueba es completa, utilice este comando de inhabilitar los debugs:

- **parada de la cliente-traza ap de los config**

VIII. Capturas del lado del cliente

Recoja a una captura de paquetes promiscua del Netmon 3.4 (Windows XP o 7 solamente) o de Wireshark del adaptador WLAN del dispositivo del cliente.

IX. capturas OTA

capturas 802.11n

- AirPCAP con Wireshark
- MacBook Pro
- Profesional del OmniPeek, empresa, etc.
- Ayudante remoto del OmniPeek (ORA)
- Cisco AP en el modo del sniffer

capturas 802.11ac

- Para 11ac 3SS captura, usted puede utilizar los 2014 Macbook Pro o un funcionamiento posterior 10.10.x o más arriba (no utilice el MacBook Air para las capturas 11ac si es posible, como él es solamente un dispositivo 2SS actualmente).
- Usted puede también utilizar 2702, 3702 o Cisco similar AP en el modo del sniffer.
- Para los escenarios de itinerancia y con el uso del software de Análisis de red profesional tal como OmniPeek de Savvius. Se recomienda para utilizar los adaptadores WLAN capaces múltiples, compatibles 802.11ac USB, tales como el adaptador de Savvius WiFi para el OmniPeek (802.11ac), Netgear A6210, o similar.

XI. Apéndice A - Extremidades y trucos adicionales

Windows:

Para recoger una cierta información adicional en lo que respecta a la conexión de red inalámbrica actual y a otros detalles relacionados directamente de un PC de Windows. Usted puede hacer uso de estos Comandos relacionados wlan del netsh en la línea de comando de 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
```

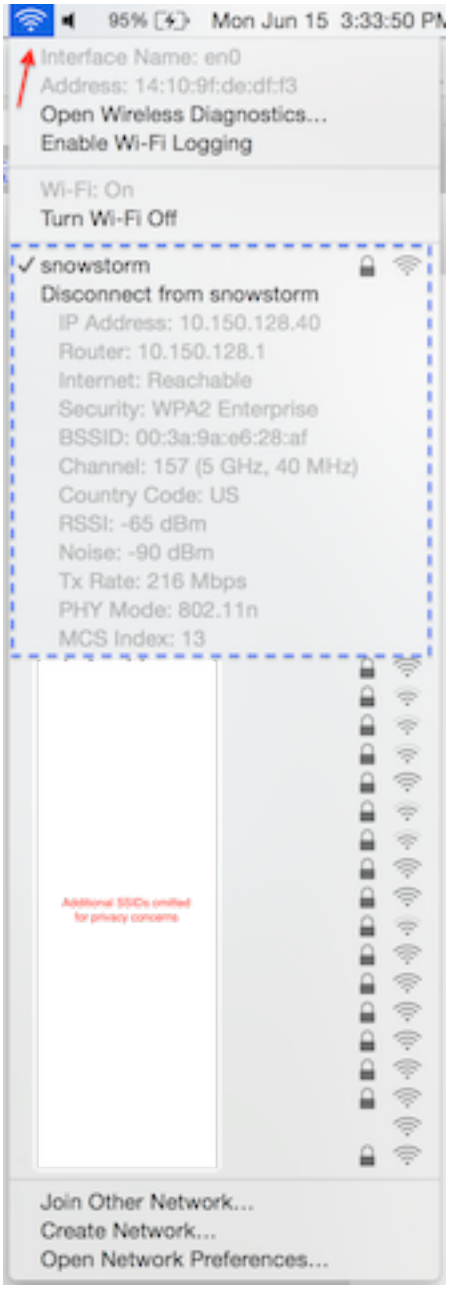
```
    Physical address       : 58:94:6b:3e:a1:d0
    State                  : connected
    SSID                   : snowstorm
    BSSID                  : 00:3a:9a:e6:28:af
    Network type           : Infrastructure
    Radio type             : 802.11n
    Authentication         : WPA2-Enterprise
    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/OS X

Para recoger la salida equivalente como el comando de **/all del ipconfig** en un PC de Windows, usted puede en lugar de otro utilizar Linux común/comando unix del **ifconfig** de enumerar la información detallada para todas las interfaces de la red en Apple MacBook. Según las necesidades, usted puede también especificar para recibir la salida para apenas la interfaz inalámbrica nativa para MacBook dado (en0 o en1, depende del modelo). Por ejemplo este ejemplo:

```
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
```

Para conseguir algún rápido pero la información detallada en lo que respecta a la conexión de red inalámbrica actual en MacBook. Usted puede también seleccionar el icono de WiFi en la esquina superior derecha del escritorio mientras que usted sostiene simultáneamente el **botón Option Button** en su teclado tal y como se muestra en de la imagen.



Otra opción útil es utilizar la línea de comando oculto aeropuerto llamado utilidad. Se recomienda altamente para utilizar solamente esto con su propio MacBook o funcionando en un ambiente de laboratorio. Pues algunos administradores de la red no pudieron desear conceder el acceso a esta utilidad en MacBook de un usuario final, así que utilice el nivel adecuado de precaución por consiguiente. Para proceder, ingrese esto en la terminal en el MacBook en la pregunta:

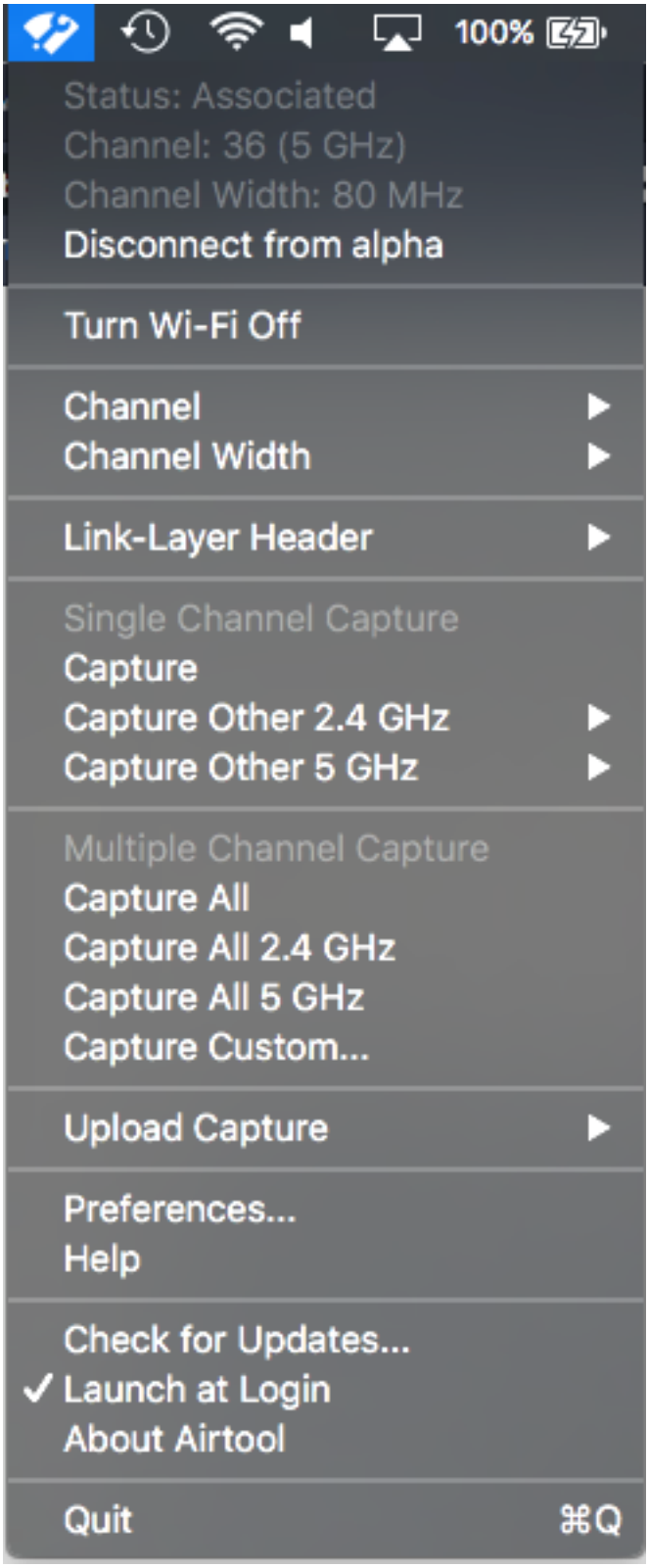
```
bash-3.2$ ifconfig en0
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
ether 14:10:9f:de:df:f3
inet6 fe80::1610:9fff:fede:dff3%en0 prefixlen 64 scopeid 0x4
inet 10.150.128.40 netmask 0xffffe000 broadcast 10.150.159.255
nd6 options=1<PERFORMNUD>
media: autoselect
status: active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

Ahora usted puede invitar la utilidad CLI del aeropuerto fácilmente. Un ejemplo cuyo incluye esto:

```
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
```

Para facilitar más lejos el proceso para recoger una captura de paquetes del canal OTA del 802.11 con el uso de las capacidades de un MacBook Pro o similar confiable, sola. Usted puede leverage las capacidades embeded en MaOS con el uso del método inalámbrico de los diagnósticos > del sniffer o de similar según lo discutido previamente, pero usted puede utilizar opcionalmente una utilidad de tercera persona llamada Airtool también (OS X 10.8 y posterior). La ventaja es una interfaz simple para recoger rápidamente a una captura de paquetes OTA, que consigue guardada directamente al escritorio con apenas algunos tecleos con la derecha del app UI de la barra de menú superior en su pantalla.



Los links de la Más información y de la descarga para Airtool se pueden encontrar en este URL:

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