Guia de Troubleshooting para questões de interoperabilidade do cliente Wireless com CUWN

Índice

Introdução

Este documento descreve em detalhe que informação necessária ser recolhido inicialmente para investigar e pesquisar defeitos eficazmente tais questões de interoperabilidade wireless quando elevaram com solução unificada da rede Wireless de Cisco (CUWN). A necessidade para tal abordagem abrangente torna-se cada vez mais importante com nunca o crescimento nos números e nas combinações de dispositivos do cliente Wireless e de rádios do Access Point (AP).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco Wireless AP
- Controladores do Wireless LAN (WLC)
- Dispositivos de rede relacionados

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

> **Note**: A audiência pretendida para este documento é os coordenadores e os administradores experientes da rede Wireless que são já familiares com o uso, a configuração e o Troubleshooting destes assuntos.

Informações de Apoio

Podem ser comuns encontrar que dado os vários dispositivos do cliente que exista e continue a ser tornado. Uma variedade de edições podem elevarar a propósito de estabelecem, mantêm, ou

simplesmente obter o a maioria fora de sua conexão à rede Wireless e apoiar a infraestrutura.

Isto pode frequentemente vir para baixo a uma edição da configuração simples da parte do dispositivo do cliente e/ou do infraestrutura Wireless próprio. Contudo, em alguns casos isto pode ser atribuído a uma questão de interoperabilidade a propósito de um dispositivo do cliente específico e dos componentes que o apoiem (isto é suplicante, adaptador de WLAN, direcionador wireless, etc.), e/ou aos AP na pergunta. Como coordenadores wireless, tais questões de interoperabilidade levantam uma oportunidade de identificar, pesquisar defeitos, e resolver potencialmente desafios do complexo.

A informação adicional ao que é esboçada neste artigo pôde ser pedida e precisado de ser recolhido numa base casuística, dado o número ilimitado de variáveis que puderam ditar tais exigências. Contudo, a informação detalhada aqui é uma diretriz genérica para endereçar toda a questão de interoperabilidade potencial do cliente Wireless.

I. Definição do problema

A primeira etapa para aproximar eficazmente todo o problema com a intenção para obter resoluto, é definir exatamente a edição à mão. Para fazer assim, assegure-se de que isso em um mínimo destas perguntas esteja perguntado e suas respostas estejam documentadas claramente:

- A edição é restringida a um modelo específico de AP e/ou do tipo de rádio (isto é 2.4 gigahertz contra gigahertz 5)?
- A edição é observada somente em versões de software WLC específicas?
- Éa edição experimentada com somente versões específicas do tipo de cliente e/ou do software (isto é versão de OS, versão do driver WLAN, etc.)
- Há algum outro dispositivo Wireless que não experimentarem esta edição? Em caso afirmativo, que são eles?
- Éa edição reprodutível quando o cliente for conectado a uma instalação wireless simplificada tal como um SSID aberto, com uma largura do canal de 20 megahertz, e a 802.11ac desabilitado? (isto é faz a edição acontecem no modo 802.11n contra o modo 802.11ac somente?).
- Se a edição não é reprodutível com um SSID aberto, em que configuração de segurança mínima a edição está visto? (isto é PSK ou 802.1X no WLAN).
- Que eram a configuração em funcionamento e as versões de software precedentes?

II. configuração WLC e logs gerais

Corrida-configuração

Sem exceção, é da necessidade absoluta para recolher a configuração WLC do cliente para uma revisão detalhada das características usadas pelo cliente, por sua instalação específica, e por outros tais detalhes. Para fazer assim, você deve estabelecer uma sessão do telnet/SSH ao WLC na pergunta e salvar a saída destes comandos CLI a um arquivo de texto:

```
config paging disable

show run-config
```

A saída completa da corrida-configuração é preferida sempre, como inclui a informação detalhada a propósito dos AP juntados e da informação associada RF, etc. Embora em alguns casos e situações, como quando você trabalhar inicialmente com um WLC com um grande número AP juntados (isto é 8510 WLC com 2500+ AP). Pôde-se preferir recolher inicialmente apenas a configuração do WLC sem tal informação AP para a revisão rápida, enquanto a corrida-configuração completa da mostra pôde tomar 30 minutos ou mais para terminar dado o número de AP. Contudo, pôde ainda ser precisado de recolher a corrida-configuração completa output mais tarde.

Para fazer assim, você pode opcionalmente recolher a saída destes comandos CLI a um arquivo de texto:

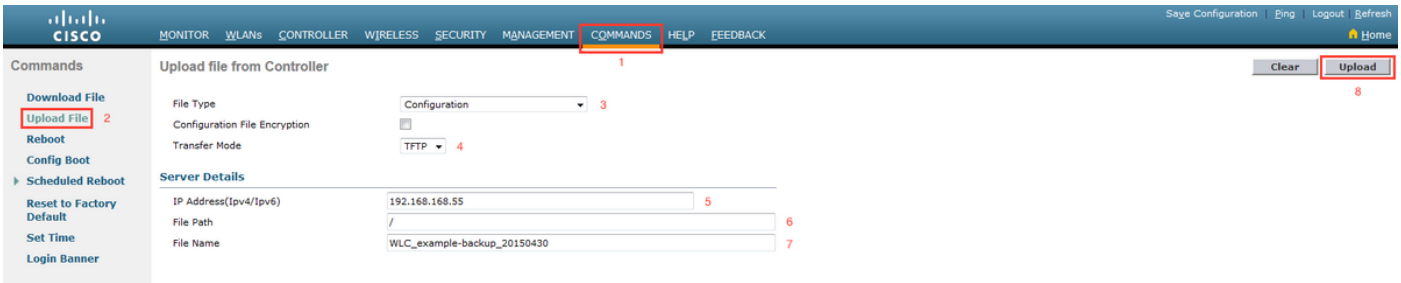
```
config paging disable

show run-config no-ap

show wlan apgroups
```

Arquivo de configuração WLC

Além do que a corrida-**configuração da mostra** ou a saída nenhum-**ap da corrida-configuração da mostra**, igualmente recomenda-se recolher também um backup total da configuração WLC. Isto é do auxílio, se um laboratório recreia necessidades de ser conduzido pelo agravamento TAC/HTTS e BU, para tentar e reproduzir a edição do cliente em um ambiente do laboratório Cisco. Um backup do WLC pode ser recolhido através do GUI ou do CLI do WLC na pergunta, com o uso do TFTP ou do FTP salvar o arquivo de configuração ao servidor FTP externo TFTP/. O exemplo abaixo mostra o uso do GUI e do CLI para salvar um backup do WLC, com o uso do TFTP:

GUI

Comandos > arquivo > configuração > transferência de arquivo pela rede da transferência de arquivo pela rede segundo as indicações da imagem.



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 do WLC

Neste tempo, você igualmente quer recolher os logs atuais do WLC para a revisão adicional como

necessária. Idealmente, você quer recolher estes logs imediatamente depois de seu teste com um cliente Wireless por meio de que a edição relatada é reproduzida. Se o cliente exporta os logs WLC para um servidor syslog externo, a seguir você quer recuperá-los de lá. Se não, você pode salvar o msglog e o traplog armazenado atualmente localmente no WLC salvar esta sessão CLI output a um outro arquivo de texto:

```
config paging disable

show msglog

show traplog
```

III. Detalhes e informação do dispositivo do cliente

A próxima etapa é recolher tanta informação e específicos a propósito dos dispositivos do cliente no uso que experimentam uma questão de interoperabilidade wireless potencial. Tal informação deve incluir, mas não necessariamente ser limitada a estes:

- Tipo de cliente (isto é tabuleta, smartphone, caderno PC, etc.)
- O dispositivo faz e modela
- Versão de OS
- Modelo do adaptador de WLAN
- Versão do driver do adaptador de WLAN
- Suplicante usado (isto é Windows zero configurações/auto configuração, Intel PROSet, etc.)
- Segurança configurada para o uso do cliente Wireless e WLAN (isto é abra, PSK, EAP-PEAP/MSCHAPv2, etc.)
- Note todos os parâmetros do cliente que forem mudados das configurações padrão fornecidas pelo vendedor na pergunta (isto é estado do sono, parâmetros vagueando, U-APSD, etc.).

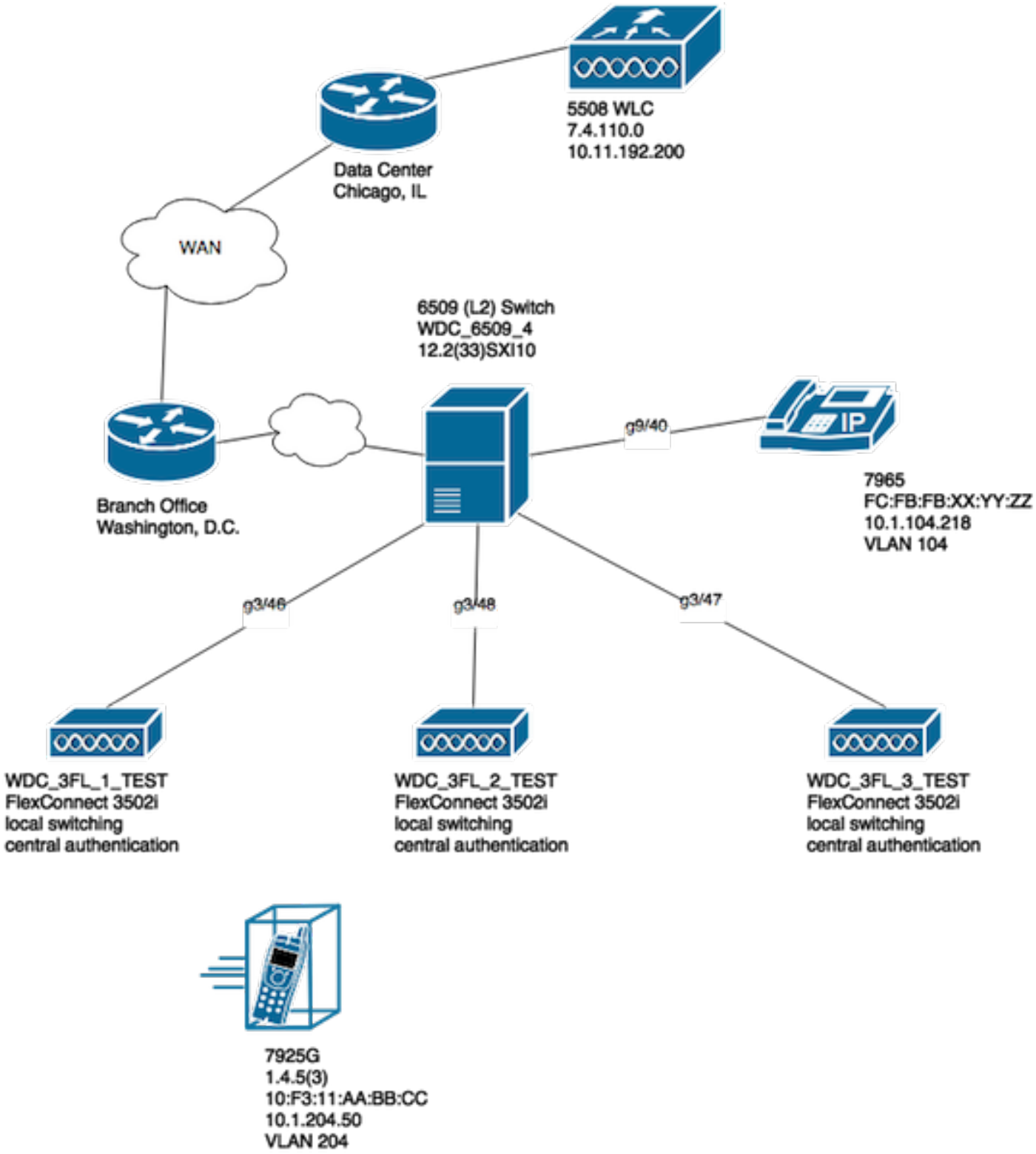
Note: Toda a informação adicional ou notas a propósito dos dispositivos do cliente até que inclui screenshots de sua configuração relacionada WLAN, e assim por diante devem igualmente ser incluídas como necessária.

IV. Topologia de rede

Para expedir mais empenhos no Troubleshooting e o processo da análise da causa raiz (RCA), recomenda-se sempre fornecer um diagrama de topologia de rede detalhado e completo. O diagrama de topologia de rede não deve somente incluir detalhes sobre a rede e o infraestrutura Wireless, mas igualmente fornece uma introspecção nos dispositivos wireless na pergunta que se opera dentro da rede (isto é impressoras/varredores, que cliente VLAN seja no uso, etc.) e de seus lugar relativo a um outros.

Um número de ferramentas (isto é Microsoft Visio, draw.io, etc.) e uma variedade de estilos podem ser usados para criar tal diagrama da rede. O aspecto importante é assegurar-se de simplesmente que a informação apropriada esteja refletida claramente no diagrama fornecido para a revisão por todos os partidos e vendedores involvidos. Uma topologia de rede de exemplo que capture básico, mas informação util a propósito da infraestrutura e dos dispositivos do cliente

segundo as indicações da imagem.



V. Detalhes adicionais da trilha e os específicos

Para ajudar a assegurar-se de que a informação apropriada esteja recolhida na altura de todo o teste com os dispositivos do cliente que os utilizadores finais experimentam edições com. Recomenda-se criar preemptively uma planilha ou similar para gravar todos os problemas de cliente e detalhes relativos observados na altura do teste, tal como este exemplo:

Endereço MAC	Username	Descrição do sintoma relatado	Sintoma observado	Gateway padrão	Estado do sinal de WiFi	Grave o ipcon

		utilizador final do tempo	Y/N do sibilo	(conectado/tentando conectar)	
xxyy.aabb.0011 test_user1	Intermitentemente disconexões do Access point.	Conectividade de rede e wireless association perdidos de AP3.	N	Tentativa conectar	ifconfig en0 en0: MTU 15 flags=8863<U éter xx:yy:a inet6 fe80:: transmissã inet nd6 options media: auto estado: ativ

O objetivo deste exercício é ajudar a documentar e determinar um teste padrão comum do interesse, assim como a obter uma imagem exata das edições à mão. Uma vez que esta planilha é preparada para ser usada para o levantamento de dados, você está agora pronto para começar seus testes. Algumas considerações adicionais, contudo importantes são como segue:

Note: Tudo debuga e necessidade recolhida capturas de pacote de informação de ser sincronizado ao mesmo servidor de NTP para uma correlação mais fácil com os logs, e deve ser tomado ao mesmo tempo para todo o teste dado.

Note: Forneça um rótulo de tempo preciso de quando a edição está observada, e quando a edição parece recuperar (se aplicável).

Note: Recolha sempre debuga filtrado pelo endereço MAC de cliente no AP e no WLC.

Note: Não execute comandos show and debug no AP dentro da mesma sessão Telnet/SSH/console, estes deve ser feito separadamente em uma sessão diferente em conformidade.

Note: O AP debuga é preferido ser tomado no telnet/SSH contra o console, porque o console é tipicamente demasiado lento ser eficaz.

VI. WLC - Comandos show and debug

Quando os testes são conduzidos para reproduzir e pesquisar defeitos questões de interoperabilidade potenciais do cliente Wireless, é imperativo que debuga e os logs adicionais estejam recolhidos do infraestrutura Wireless no uso. Estas duas seções podem explicar em detalhe os logs específicos e o resultado do debug inicial que devem ser recolhidos do WLC e do AP, respectivamente.

Comandos Debug WLC

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

No que diz respeito à natureza da edição à mão, você pode igualmente adicionar estes WLC debuga numa base casuística:

- **debugar o detalhe aaa permitem** - use isto se há uns problemas relacionados da autenticação com o servidor AAA
- **debugar eventos aaa permitem** - use isto se há uns problemas relacionados da autenticação com o servidor AAA
- **debugar o aaa que todos permitem** - use isto para edições do AUTH; a saída para esta debuga é verboso assim que use-o somente quando absolutamente necessário (isto é para casos da ultrapassagem AAA, etc.)
- **debugar a entrega da mobilidade** - use quando lá estão vagueando edições entre WLC

Uma vez que a edição é reproduzida com o cliente Wireless na pergunta, e toda a informação esboçada nas seções previamente e após este estão recolhidos e documentados. A fim executar estes comandos CLI, você deve desabilitar debuga no WLC.

```
debug disable-all
```

Comandos show WLC

```
config paging disable

show time

show client detail <MAC_address>

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

Como mencionado previamente, assegure para executar o WLC debuga em uma sessão do telnet/SSH e recolhem a saída para estes comandos show em um outro telnet/SSH ao WLC. Você deve fazer o mesmos para recolher os comandos de debug e show AP output detalhado nestes a seção.

VII. AP - Comandos show and debug

Access point de pouco peso do Cisco IOS

Antes que você comece algum debuga em todos os IO de pouco peso AP envolvidos no teste, tal como os 2600, os 2700, os 3700 ou os pontos de acesso da Cisco modelo prévios. Você deve primeiramente executar estes comandos CLI no AP, a fim evitar um intervalo na altura de uma sessão Telnet/SSH/console ao AP na pergunta quando seus testes do cliente:

```
debug capwap console cli

config t

line vty 0 4

exec-timeout 0

session-timeout 0
```

Você pode igualmente seguir estas etapas para usar a conexão de console e para substituir pelo contrário a indicação do **line vty 0 4** com a **linha console 0**, a fim desabilitar em conformidade o executivo e os timeouts de sessão para uma série/conexão de console.

- linha console 0 - use para alterar parâmetros de timeout de sessão de série
- o line vty 0 4 - use para alterar parâmetros de timeout de sessão do telnet/SSH

Comandos show AP

Antes que você comece o teste, você deve primeiramente recolher uma amostra destes comandos show no AP. Você deve recolher a saída destes comandos show pelo menos duas vezes para cada teste que envolve o cliente Wireless na pergunta; ambos antes e depois do teste estão 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

Uma vez que você recolheu a saída inicial dos comandos show acima mencionados, você pode agora permitir debuga no mesmo Access point em uma sessão separada do telnet/SSH como mostrado. Assegure para salvar a saída inteira a um arquivo 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
```

Legenda

Bandeira	Descrição
d0	Rádio 2.4 gigahertz (slot 0)
d1	Rádio gigahertz 5 (slot1)
mgmt	Pacotes de gerenciamento do traço
vagabundos	Informação do bloco ACK do traço
receptor	Pacotes recebidos do traço

chaves	Chaves ajustadas do traço
rxev	O traço recebeu eventos
txev	O traço transmite eventos
txrad	O traço transmite para transmitir por rádio
xmt	O traço transmite pacotes
txfail	Falhas de transmissão do traço
taxas	Mudanças da taxa do traço

Para desabilitar debuga no AP uma vez que o teste e o processo do levantamento de dados são terminados, você pode executar este comando CLI no AP:

```
u all
```

Access point AP-COS

Para 802.11ac Access point capazes da onda 2 e mais tarde, como os 1800, os 2800 e os Access point do modelo 3800. Este um modelo mais novo AP introduz um sistema operacional completamente novo para as Plataformas do Access point referidas como AP-COS. Como tal, não os comandos all como usados previamente no Cisco IOS de pouco peso tradicional basearam Access point como detalhado acima ainda aplicam-se. Se quando você pesquisa defeitos uma edição envolve a questão de interoperabilidade com os vários dispositivos do cliente STA e o AP-COS AP modelo, a seguir este a informação deve ser recolhida do Access point AP-COS envolvido com o teste equivalente.

Antes que você comece algum debuga em todo o modelo AP AP-COS envolvido no teste. Você deve primeiramente executar este o comando CLI no AP, a fim evitar um intervalo na altura de uma sessão Telnet/SSH/console ao AP na pergunta quando seus testes do cliente:

```
exec-timeout 0
```

Comandos show AP-COS

Antes que você comece o teste, você deve primeiramente recolher uma amostra destes comandos show no AP. Você deve recolher a saída destes comandos show pelo menos duas vezes para cada teste que envolve o cliente Wireless na pergunta; ambos antes e depois do teste estão 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

Estes debugam são específicos ao 18xx Series dos Access point. Isto é devido ao fato que os chipset usados para o 1800 Series dos AP diferem daqueles encontrados nos Access point do

2800/3800 Series, e assim um grupo diferente de debuga é exigido nesta encenação pela comparação. A correspondência debuga para o 2800/3800 Series que os AP são cobertos na próxima seção.

Uma vez que você recolheu a saída inicial dos comandos show acima mencionados, você deve agora permitir debuga nos mesmo 1800 Access point em uma sessão separada do telnet/SSH como mostrado. Assegure para salvar a saída inteira a um arquivo 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>
```

Em alguns casos, você pôde precisar de permitir igualmente o adicional debuga no 18xx AP para pesquisar defeitos mais questões de interoperabilidade do cliente. Contudo, este deve ser somente if/as feito pedido por um engenheiro de TAC da Cisco para um pedido/exemplo correspondentes do serviço.

Enquanto adicional debuga não pôde somente ser distante mais verboso em sua saída mas pode igualmente introduzir a carga adicional no AP também daqui onde exige adicional cronometra para a análise apropriada. Qual sob certas condições pode potencialmente interromper o serviço, se muitos dispositivos do cliente tentam conectar ao mesmo AP sob o teste ou variáveis similares.

Para desabilitar debuga no Access point variante AP-COS - se em uns 1800 ou no 2800/3800 Series AP - uma vez o teste e o processo do levantamento de dados são terminados, você podem executar este comando CLI no AP:

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

2800/3800 Series | Comandos Debug AP-COS

Uma vez que você recolheu a saída inicial dos comandos show acima mencionados, você deve agora permitir debuga no mesmo 2800/3800 de Access point em uma sessão separada do telnet/SSH como mostrado. Assegure para salvar a saída inteira a um arquivo 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
```

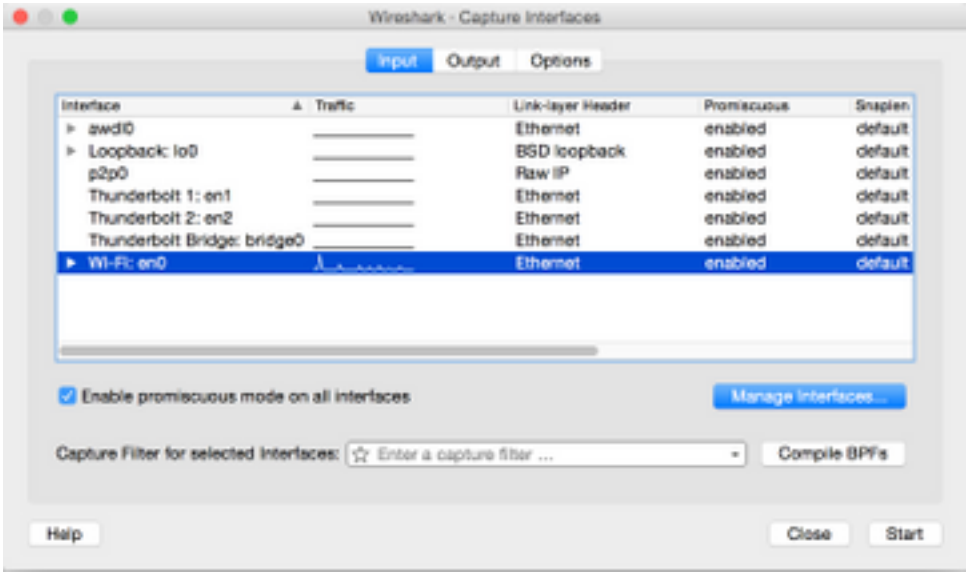
Para desabilitar debuga no 1800/2800/3800 Series AP uma vez que o teste e o processo do levantamento de dados são terminados, você pode executar este comando CLI no AP:

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

VIII. Capturas de pacote de informação laterais do cliente

Do dispositivo do cliente no uso se é um caderno PC, MacBook ou similar, você deve recolher a captura de pacote de informação do modo misturado da relação wireless do dispositivo do cliente usado para reproduzir a edição. As utilidades comuns como Netmon 3.4 (Windows somente) ou Wireshark podem prontamente ser transferidos e usado para recolher esta captação e para salvar à um arquivo *.pcap. Depende do dispositivo, pôde igualmente haver uns meios recolher um tcpdump ou similar do cliente na pergunta, assim que você pôde precisar de consultar a este respeito com o fabricante do dispositivo do cliente para o auxílio.

Está aqui um exemplo para configurar uma captação de Wireshark para a relação wireless em um MacBook Pro:



Como com toda a captura de pacote de informação, apesar do que utilidade for usada para o recolher, assegure para salvar o arquivo em um formato do arquivo do pcap (isto é *.pcap, *.pcapng, *.pkt, etc.). Este é assegurar-se de que não somente os engenheiros da Cisco em todo o departamento possam ver os arquivos da captura de pacote de informação facilmente, mas coordenadores dos outros fornecedores e das organizações também (isto é Intel, Apple, etc.). Isto permite um processo mais sem emenda da cooperação e da Colaboração, que facilite mais Cisco e os vendedores do dispositivo do cliente para trabalhar melhor junto para investigar e resolver todas as questões de interoperabilidade potenciais.

IX. Sobre - Capturas de pacote de informação do ar (OTA)

A fim pesquisar defeitos eficazmente todas as questões de interoperabilidade wireless potenciais ou existentes, é crucial recolher uma captura de pacote de informação da qualidade OTA da edição. Isto permite a análise detalhada da comunicação Wireless real do 802.11 entre o cliente Wireless e os rádios do Access point na pergunta, além do que dá uma perspectiva mais adicional ao lado do cliente e os logs do infraestrutura Wireless, debugam, etc. Este é um passo crítico que deva ser realizado para cada teste de uma questão de interoperabilidade wireless potencial, sem exceção.

Cronometra contudo, frequentemente o cliente final não é equipado nem é preparado corretamente para recolher capturas de pacote de informação OTA. Este é um obstáculo comum

que dos coordenadores a cara wireless frequentemente, e elas deva trabalhar com o cliente para superar esta em uma variedade de maneiras. Este artigo dos fóruns do apoio de Cisco pode servir como um bom ponto do começo para ajudar a guiar em conformidade e educar o cliente:

sniffing wireless/captura de pacote de informação do 802.11

Éda importância suprema essa a captura de pacote de informação OTA seja recolhido em um formato do arquivo do pcap (isto é *.pcap, *.pcapng, *.pkt, etc.), e inclui o meta do 802.11 - os dados (isto é RSSI, o canal, a taxa de dados, etc.). O sniffer OTA deve igualmente ser mantido na proximidade final ao dispositivo do cliente na pergunta em todas as vezes durante os testes, assegurar uma perspectiva exata do tráfego enviado e recebido para/desde o dispositivo do cliente que está sendo testado.

> **Note**: Se os testes na pergunta envolvem uma encenação vagueando do dispositivo do cliente, por meio de que mais de um canal do 802.11 precisa de ser monitorado em uma captura de pacote de informação agregada. Então não se recomenda atualmente usar o analisador de AirMagnet WiFi das redes do solha.

A razão para esta é devido ao fato de que as capturas de pacote de informação agregadas com o uso desta utilidade salvar atualmente em um formato do arquivo proprietário, e não em um formato do estilo do pcap que possa prontamente ser visto em Wireshark ou em outras utilidades similares. Assegure-se de que sua captura de pacote de informação OTA esteja em um formato do arquivo NON-proprietário, isto ajuda a assegurar-se de que todos os partidos e vendedores envolvidos possam prontamente rever todos os arquivos de captura em todas as vezes, e ajuda finalmente a expedir quaisquer esforços da definição.

em um formato que sejam legível por Wireshark atual, e que inclua o meta do 802.11 - os dados (RSSI, canal, taxa de dados) - veja mais em:
https://supportforums.cisco.com/document/75331/80211-wireless-sniffing-packet-capture#sthash.Xhlx5LSS.dpuf
Estão aqui alguns métodos comuns para recolher uma captura de pacote de informação OTA:

- AirPCAP com Wireshark
- MacBook Pro
- Profissional do OmniPeek, empresa do OmniPeek, etc.
- Assistente remoto do OmniPeek (ORA)
- Cisco AP no modo do sniffer

captações 802.11n

Para capturas de pacote de informação OTA que envolve os clientes Wireless 802.11n, há presentemente mais flexibilidade e acessibilidade. Isto é devido a uma variedade mais larga de adaptadores de WLAN disponíveis do Sem fio USB que podem prontamente ser usados com um número de ferramentas, tais como o OmniPeek e o outro.

Tome a nota a respeito de como as capacidades do adaptador Wireless específico usado para recolher uma captação 802.11n OTA comparam com as capacidades do chipset real WLAN usado pelos dispositivos do cliente que você tenta pesquisar defeitos. Por exemplo, se o dispositivo do cliente experimenta uma questão de interoperabilidade wireless potencial que use 2 um chipset capaz espacial do córrego (2SS) 802.11n. Então é altamente recomendado assegurar-se de que o adaptador Wireless usado para recolher uma captura de pacote de

informação OTA seja igualmente um 2SS ou um adaptador melhor, com 802.11n ou especificações mais novas.

captações 802.11ac OTA

Para 3 captações 802.11ac espaciais do córrego (3SS), você pode usar as capacidades nativas do sniffing de uns 2014 MacBook Pro modelo ou um Mac OS X running mais atrasado 10.10.x ou mais altamente. Se pesquisando defeitos 2 um dispositivo do cliente espacial do córrego 802.11ac, você pode igualmente usar um MacBook Air para as captações 802.11ac. O modelo do ar de conjuntos de chip do uso 2SS somente WLAN de MacBooks atualmente na altura desta escrita. Você pode referir o artigo abaixo dos fóruns do apoio de Cisco para instruções em como recolher capturas de pacote de informação OTA com o uso de Mac OS X, com uma variedade de métodos:

Sniffing wireless com o uso de Mac OS X 10.6+

Você pode igualmente usar um 2702/2802/3702/3802 Series ou o AP similar no modo do sniffer para recolher uma captura de pacote de informação 802.11ac apropriada com 3SS. Você pode igualmente referir o recurso abaixo para uma lista atual dos adaptadores Wireless 802.11ac disponíveis. Alguns de que pode poder ser usado potencialmente com as ferramentas comuns como o OmniPeek e o outro para recolher uma captura de pacote de informação 802.11ac (isto é conjuntos de chip de Ralink, de Atheros, etc.):

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

Você pode igualmente usar um 2702/2802/3702/3802 Series ou o AP similar no modo do sniffer para recolher uma captura de pacote de informação 802.11ac apropriada com 3SS. Para a conveniência, as instruções passo a passo em como configurar Cisco AP no modo do sniffer e recolher uma captura de pacote de informação OTA podem ser encontradas no artigo abaixo dos fóruns do apoio de Cisco:

Cisco AP no modo do sniffer

Para pesquisar defeitos encenações vagueando com um dispositivo do cliente Wireless, o desafio comum é recolher eficazmente uma captura de pacote de informação OTA através dos canais múltiplos. Este método simultaneamente de monitorar os canais múltiplos do 802.11 é conseguido pela coleção da captura de pacote de informação agregada OTA. Recomenda-se usar adaptadores de WLAN capazes múltiplos, compatíveis 802.11ac USB com um software de análise de rede compatível a fim conseguir isto. Alguns adaptadores de WLAN capazes comuns 802.11ac USB incluem o adaptador de Savvius WiFi para o OmniPeek (802.11ac), o Netgear A6210, ou similar.

X. Resumo

Está aqui um breve resumo da informação que precisa de ser recolhida para pesquisar defeitos eficazmente uma questão de interoperabilidade potencial do cliente Wireless com um CUWN. Esta seção é pretendida servir como uma seção de referência rápida, como necessário.

I. Definição do problema

- A edição é restringida a um modelo específico do tipo do Access point e/ou do rádio (2.4

gigahertz contra gigahertz 5)?
- A edição é observada somente em versões específicas do software do controlador do Wireless LAN (WLC)?
- Éa edição experimentada com somente versões específicas do tipo de cliente e/ou do software (isto é versão de OS, versão do driver WLAN, etc.)
- Há algum outro dispositivo Wireless que não experimentarem esta edição? Em caso afirmativo, que são eles?
- Éa edição reprodutível quando o cliente for conectado a um SSID aberto, a uma largura do canal de 20 megahertz, e a 802.11ac desabilitado? (isto é faz a edição acontecem no modo 11n contra o modo 11ac somente)
- Se a edição não é reprodutível com um SSID aberto, em que configuração de segurança mínima a edição está visto? (isto é PSK ou 802.1X no WLAN)
- Que era a configuração em funcionamento e as versões de software precedentes?

II. configuração e logs WLC

Recolha isto do CLI do WLC na pergunta:

- desabilitação da paginação da configuração
- mostre a corrida-configuração

Alternativamente, você pode igualmente recolher apenas estes output como necessários:

- desabilitação da paginação da configuração
- mostre a corrida-configuração nenhum-ap
- mostre apgroups wlan

Backup da configuração WLC através de TFTP, de FTP, etc. (GUI: **Comandos > arquivo > configuração da transferência de arquivo pela rede**)

Syslog do WLC

III. Informação do dispositivo do cliente

- Tipo de cliente (isto é tabuleta, smartphone, caderno PC, etc.)
- O dispositivo faz e modela
- Versão de OS
- Modelo do adaptador de WLAN
- Versão do driver do adaptador de WLAN
- Suplicante usado (isto é Windows zero configurações/auto configuração, Intel PROSet, etc.)
- Segurança configurada para o uso do cliente Wireless e WLAN (isto é abra, PSK, EAP-PEAP/MSCHAPv2, etc.)

> **Note**: Todos os parâmetros do cliente mudados das configurações padrão forneceram pelo vendedor na pergunta. (isto é estado do sono, parâmetros vagueando, U-APSD, etc.)

IV. Diagrama de topologia de rede

Isto deve incluir uma representação e/ou detalhes a propósito dos dispositivos Wireless na rede (isto é impressoras/varredores, WLC, etc.)

V. Crie uma planilha para gravar todos os problemas de cliente

Exemplo:

Endereço MAC	Username	Descrição do sintoma relatado	Sintoma observado utilizador final do tempo	Gateway padrão Y/N do sibilo	Estado do sinal de WiFi (conectado/tentando conectar)	Grave o ipconfi /all (ou o equivalente)

O objetivo deste exercício é ajudar a identificar um teste padrão comum, e a apresentar uma imagem mais exata das edições à mão.

VI. Comandos show and debug no WLC

Recolha estes WLC debuga através do CLI:

- **intervalo de sessões 0 da configuração**
- **debugar o <MAC_address> do cliente**
- **debugar o mensagem DHCP permitem**

Adicionar o adicional debuga caso por caso na base:

- **debugar o detalhe aaa permitem** - use isto se há uns problemas relacionados da autenticação com servidor AAA
- **debugar eventos aaa permitem** - use isto se há uns problemas relacionados da autenticação com servidor AAA
- **debugar o aaa que todos permitem** - use isto para edições do AUTH; isto é verboso assim que use-o somente quando necessário (isto é para a ultrapassagem AAA encaixota etc.)
- **debugar a entrega da mobilidade** - use ao vaguear edições entre WLC

Recolha a saída para os comandos show WLC através do CLI:

- **desabilitação da paginação da configuração**
- **show time**
- **mostre o detalhe do cliente < o endereço MAC do client>** (note o estado do cliente no WLC)
- Sibile o cliente do WLC

Uma vez que o teste está completo, use este comando parar toda atual debuga no WLC:

- **debugar o desabilitação-todo**

VII. Comandos show and debug no AP

Cisco IOS de pouco peso AP

Esta seção detalha debuga exigido para o 1700/2700/3700 Series ou os Access point modelo prévios.

Para evitar um timeout de sessão AP na altura de uma sessão Telnet/SSH/console, use estes comandos:

- debugar o console CLI do capwap
- config t
- linha console 0 -- use para alterar parâmetros de timeout de sessão de série
- line vty 0 4 -- use para alterar parâmetros de timeout de sessão do telnet/SSH
- EXEC-intervalo 0
- sessão-intervalo 0
- o termo len 0

Antes que você comece o teste, recolha uma amostra destes comandos show no AP. Em um mínimo recolha duas amostras desta saída, ambos antes e depois da conclusão dos testes com o uso destes comandos show AP através do CLI:

- o termo len 0
- *show clock*
- show tech
- mostre o manganês do cliente do capwap
- mostre dfs int do1
- show logging
- mais event.log
- mostre o local do formato de período do indicador do traço dot11_rst
- mostre o traço dot11_rst
- mostre o local do formato de período do indicador do traço dot11_bcn
- mostre o traço dot11_bcn

Recolha estes AP debuga através do CLI:

- debugar o dot11 {d0 | } <MAC_address> do ADDR do monitor d1
- debugar o dot11 {d0 | } o mgmt dos clientes da cópia do traço d1 fecha vagabundos do txfail do xmt receptor do txev do rxev
- termo segunda-feira

Uma vez que o teste está completo, use este comando desabilitar debuga:

- u todo

AP-COS AP

Esta seção detalha debuga exigido para o 1800/2800/3800 Series AP.

Para evitar um timeout de sessão AP na altura de uma sessão Telnet/SSH/console, use estes comandos:

- EXEC-intervalo 0

Antes que você comece o teste, recolha uma amostra dos comandos show abaixo no AP. Em um mínimo recolha duas amostras desta saída, ambos antes e depois da conclusão dos testes com o uso destes comandos show AP através do CLI:

- o termo len 0
- *show clock*
- show tech
- mostre o <client_MAC-address> das estatísticas do cliente

- **mostre estado cont NSS**
- **mostre stats cont NSS**
- **show log**

Para os Access point do 1800 Series, recolha estes AP debuga através do CLI:

- **debugar o <client_MAC-address> do ADDR dos eventos do nível do cliente do dot11**
- **debugar o <client_MAC-address> do ADDR dos erros do nível do cliente do dot11**
- **debugar o <client_MAC-address> crítico do ADDR do nível do cliente do dot11**
- **debugar o <client_MAC-address> do ADDR da informação do nível do cliente do dot11**
- **debugar o <client_MAC-address> do ADDR do eapol do datapath do cliente do dot11**
- **debugar o <client_MAC-address> do ADDR DHCP do datapath do cliente do dot11**
- **debugar o <client_MAC-address> do ADDR arp do datapath do cliente do dot11**
- **denomine segunda-feira**

Para os Access point do 2800/3800 Series, recolha estes AP debuga através do CLI:

- **o endereço do cliente-traço ap da configuração adiciona o <client_MAC-address>**
- **o filtro todo do cliente-traço ap da configuração permite**
- **o console log da saída do cliente-traço ap da configuração permite**
- **começo do cliente-traço ap da configuração**
- **termo segunda-feira**

Uma vez que o teste está completo, use este comando desabilitar debuga:

- **parada do cliente-traço ap da configuração**

VIII. Captações do lado do cliente

Recolha uma captura de pacote de informação promíscuo de Netmon 3.4 (Windows XP ou 7 somente) ou de Wireshark do adaptador de WLAN do dispositivo do cliente.

IX. captações OTA

captações 802.11n

- AirPCAP com Wireshark
- MacBook Pro
- Profissional do OmniPeek, empresa, etc.
- Assistente remoto do OmniPeek (ORA)
- Cisco AP no modo do sniffer

captações 802.11ac

- Para 11ac 3SS captura, você pode usar uns 2014 Macbook Pro ou um corredor mais atrasado 10.10.x ou mais altamente (não use o MacBook Air para as captações 11ac se possível, como ele é somente um dispositivo 2SS atualmente).
- Você pode igualmente usar uns 2702, 3702 ou Cisco similar AP no modo do sniffer.
- Para encenações vagueando e com o uso do software de análise de rede profissional tal como o OmniPeek de Savvius. Recomenda-se usar adaptadores de WLAN capazes

múltiplos, compatíveis 802.11ac USB, tais como o adaptador de Savvius WiFi para o OmniPeek (802.11ac), o Netgear A6210, ou similar.

XI. Apêndice A - Pontas e truques adicionais

Windows

Para recolher alguma informação adicional a propósito da conexão Wireless atual e de outros detalhes relacionados diretamente de um PC Windows. Você pode utilizar estes comandos relacionados wlan do netsh na linha 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
```

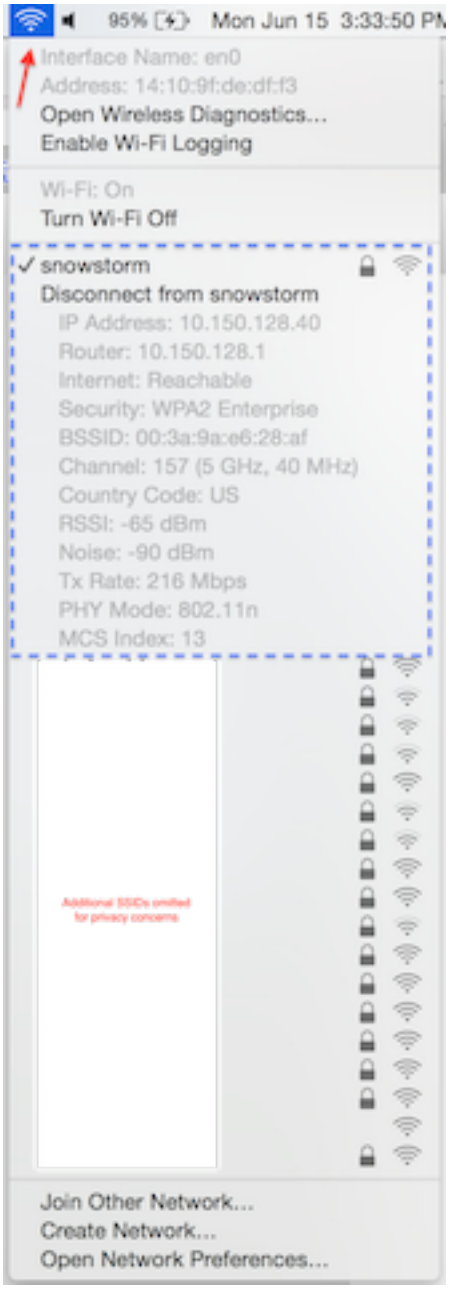
```
    Radio type             : 802.11n
    Authentication         : WPA2-Enterprise
    Cipher                 : CCMP
    Connection mode        : Profile
    Channel                : 157
    Receive rate (Mbps)    : 300
    Transmit rate (Mbps)   : 300
    Signal                 : 80%
    Profile                : 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 (anteriormente OS X)

A fim recolher a saída equivalente como o comando de **/all do ipconfig em um** PC Windows, você pode pelo contrário usar Linux comum/comando unix do **ifconfig** alistar a informação detalhada para todas as interfaces de rede em Apple MacBook. Como necessário, você pode igualmente especificar para receber a saída para apenas a relação wireless nativa para MacBook dado (en0 ou en1, depende do modelo). Como este exemplo:

```
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
```

A fim obter algum rápido mas a informação detalhada a propósito da conexão Wireless atual em MacBook. Você pode igualmente selecionar o ícone de WiFi no canto superior direito do desktop quando você guardar simultaneamente o **botão Option Button em** seu teclado segundo as indicações da imagem.



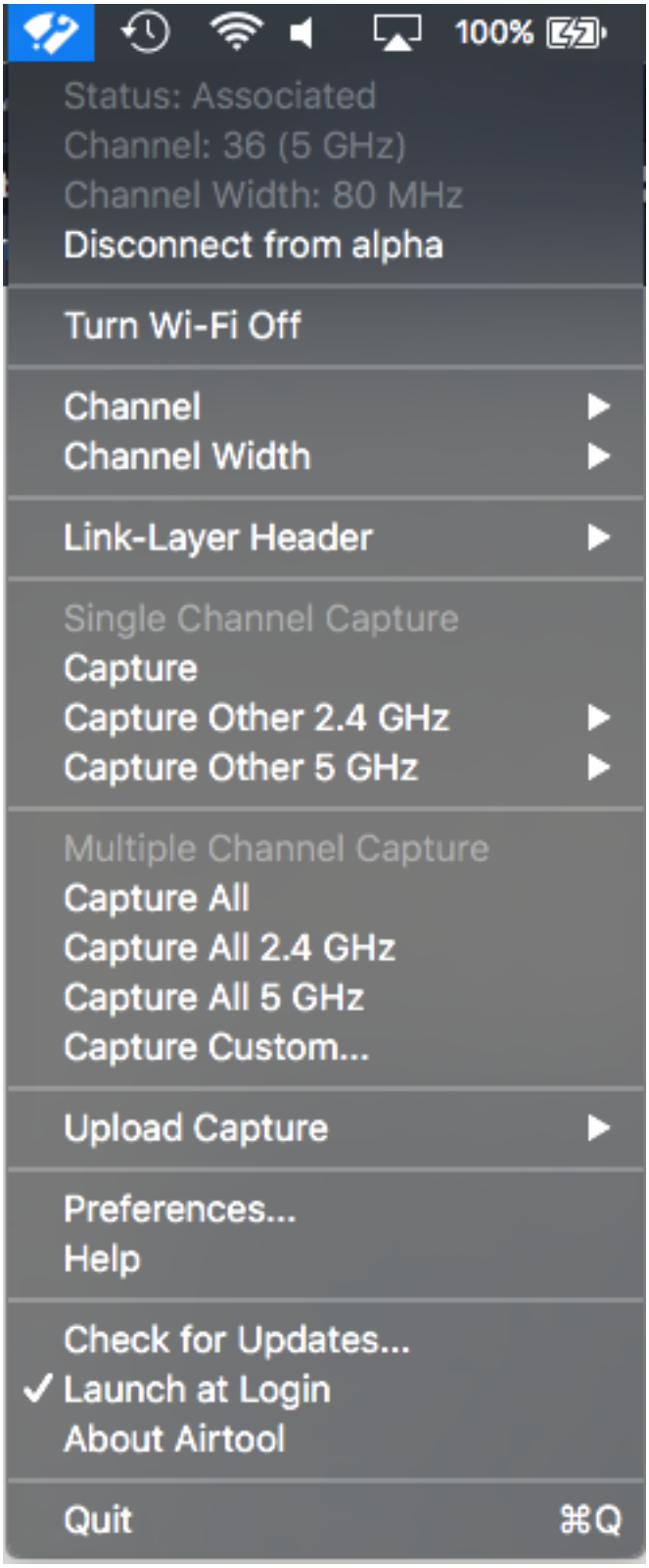
Uma outra opção útil é utilizar a linha de comando oculto aeroporto chamado utilidade. É altamente recomendado utilizar somente esta com seu próprio MacBook ou um no uso em um ambiente de laboratório. Porque alguns administradores de rede não puderam desejar conceder o acesso a esta utilidade em MacBook de um utilizador final, assim que usam o nível apropriado do cuidado em conformidade. Para continuar, inscreva isto no terminal em MacBook na pergunta:

```
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 0xfffffe000 broadcast 10.150.159.255
nd6 options=1<PERFORMNUD>
media: autoselect
status: active
```

Agora você pode convidar o utilitário de CLI do aeroporto facilmente. Um exemplo de que inclui isto:

```
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 mais o processo para recolher uma captura de pacote de informação do canal OTA do 802.11 com o uso das capacidades de um MacBook Pro ou similar seguro, único. Você pode leverage as capacidades embeded no macOS com o uso do método wireless dos diagnósticos > do sniffer ou de similar como discutidas previamente, mas opcionalmente você pode usar uma utilidade da terceira chamada Airtool também (OS X 10.8 e mais atrasado). O benefício é uma interface simples para recolher rapidamente uma captura de pacote de informação OTA, que obtenha salvar diretamente ao desktop com apenas alguns cliques com o direito do app UI da barra de menus superior em sua tela.



Os links da informação adicional e da transferência para Airtool podem ser encontrados nesta URL:

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