Risoluzione dei problemi di interoperabilità dei client wireless con CUWN

Sommario

Introduzione

Questo documento descrive i problemi di interoperabilità che si verificano con la soluzione Cisco Unified Wireless Network (CUWN).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Wireless AP
- WLC (Wireless LAN Controller)
- Dispositivi di rete correlati

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

> **Nota**: i destinatari di questo documento sono ingegneri e amministratori di reti wireless esperti che hanno già familiarità con l'utilizzo, la configurazione e la risoluzione dei problemi di questi argomenti.

Premesse

Può essere comune trovare che dato i vari dispositivi client che esistono e continuano a essere sviluppati. È possibile che sorgano diversi problemi relativi alla creazione, alla manutenzione o semplicemente al raggiungimento del massimo dalla connessione alla rete wireless e al supporto dell'infrastruttura.

Questo spesso si riduce a un semplice problema di configurazione da parte del dispositivo client e/o dell'infrastruttura wireless stessa. Tuttavia, in alcuni casi ciò può essere attribuito a un

problema di interoperabilità relativo a uno specifico dispositivo client e ai componenti che lo supportano (supplicant, scheda WLAN, driver wireless, ecc.) e/o agli access point in questione. In qualità di tecnici wireless, tali problemi di interoperabilità offrono l'opportunità di identificare, risolvere e risolvere problemi potenzialmente complessi.

Questo documento descrive in dettaglio le informazioni che devono essere raccolte inizialmente per indagare e risolvere in modo efficace questi problemi di interoperabilità wireless quando si presentano con la soluzione Cisco Unified Wireless Network (CUWN). La necessità di un tale approccio globale diventa sempre più importante con l'aumento costante del numero e delle combinazioni di dispositivi client wireless e radio dei punti di accesso.Potrebbero essere richieste ulteriori informazioni su quanto delineato in questo articolo, che dovrebbero essere raccolte caso per caso, dato il numero illimitato di variabili che potrebbero dettare tali requisiti. Tuttavia, le informazioni qui riportate rappresentano una linea guida generica per risolvere eventuali problemi di interoperabilità dei client wireless.

I. Definizione del problema

Il primo passo per affrontare in modo efficace qualsiasi problema con l'intento di ottenere una soluzione, è quello di definire accuratamente il problema in questione. A tal fine, assicurarsi che almeno queste domande vengano poste e che le loro risposte siano chiaramente documentate:

- Il problema è limitato a uno specifico modello di access point e/o tipo radio (2,4 GHz rispetto a 5 GHz)?
- Il problema è stato rilevato solo su una o più versioni specifiche del software WLC?
- Il problema si verifica solo con versioni specifiche di tipi di client e/o software (versione del sistema operativo, versione del driver WLAN, ecc.)?
- Esistono altri dispositivi wireless che non rilevano questo problema? In caso affermativo, quali?
- Il problema è riproducibile quando il client è connesso a un'installazione wireless semplificata, ad esempio un SSID aperto, con una larghezza di canale di 20 MHz e 802.11ac disabilitato? in altre parole, il problema si verifica solo in modalità 802.11n rispetto alla modalità 802.11ac?
- Se il problema non è riproducibile con un SSID aperto, a quale configurazione di protezione minima è associato il problema? (PSK o 802.1X sulla WLAN).
- Quali erano le precedenti versioni software e di configurazione valide?

II. Configurazione WLC e registri generali

Run-Config

Senza eccezioni, è assolutamente necessario raccogliere la configurazione WLC per un'analisi dettagliata delle funzionalità utilizzate dal cliente, della loro configurazione specifica e di altri dettagli simili. A tal fine, è necessario stabilire una sessione Telnet/SSH sui WLC in questione e salvare l'output di questi comandi CLI in un file di testo:

```
config paging disable

show run-config
```

L'uscita di configurazione di esecuzione completa è sempre preferibile, in quanto include informazioni dettagliate relative agli access point collegati e alle informazioni RF associate.

Tuttavia, in alcuni casi e situazioni, ad esempio quando si lavora inizialmente con un WLC con un numero elevato di AP aggiunti (8510 WLC con oltre 2500 AP). Inizialmente, si potrebbe preferire raccogliere solo la configurazione del WLC senza tali informazioni sull'access point per poterla esaminare rapidamente, in quanto il completamento della configurazione di esecuzione completa potrebbe richiedere 30 minuti o più, dato il numero di access point. Tuttavia, potrebbe essere necessario raccogliere l'output completo della configurazione di esecuzione in un secondo momento.

A tale scopo, è possibile raccogliere facoltativamente l'output di questi comandi CLI in un file di testo:

```
config paging disable

show run-config no-ap

show wlan apgroups
```

File di configurazione WLC

Oltre all'output **show run-config** o **show run-config no-ap**, si consiglia di raccogliere anche un backup completo della configurazione WLC. Ciò è utile, se il ricreazione di un laboratorio deve essere eseguita sia da TAC/HTTS che da Escalation BU, per cercare di riprodurre il problema in un ambiente lab Cisco. Un backup del WLC può essere raccolto tramite la GUI o la CLI del WLC in questione, con l'uso del TFTP o dell'FTP per salvare il file di configurazione sul server TFTP/FTP esterno. L'esempio mostra come usare sia la GUI sia la CLI per salvare un backup del WLC, con l'uso del TFTP:

GUI

Comandi > Carica file > Configurazione > Carica come mostrato nell'immagine.

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 dal WLC

A questo punto, si desidera anche raccogliere i log correnti dal WLC per un'ulteriore revisione, se necessario. Idealmente, si desidera raccogliere questi log subito dopo il test con un client wireless in cui il problema segnalato viene riprodotto. Se il cliente esporta i log WLC in un server syslog esterno, è possibile recuperarli da tale server. In caso contrario, è possibile salvare il file msglog e

il traplog correntemente archiviati nel WLC salvando l'output di questa sessione CLI in un altro file di testo:

```
config paging disable

show msglog

show traplog
```

III. Dettagli e informazioni sul dispositivo client

Il passo successivo consiste nel raccogliere quante informazioni e specifiche sui dispositivi client in uso possano presentare un potenziale problema di interoperabilità wireless. Tali informazioni devono comprendere, tra l'altro:

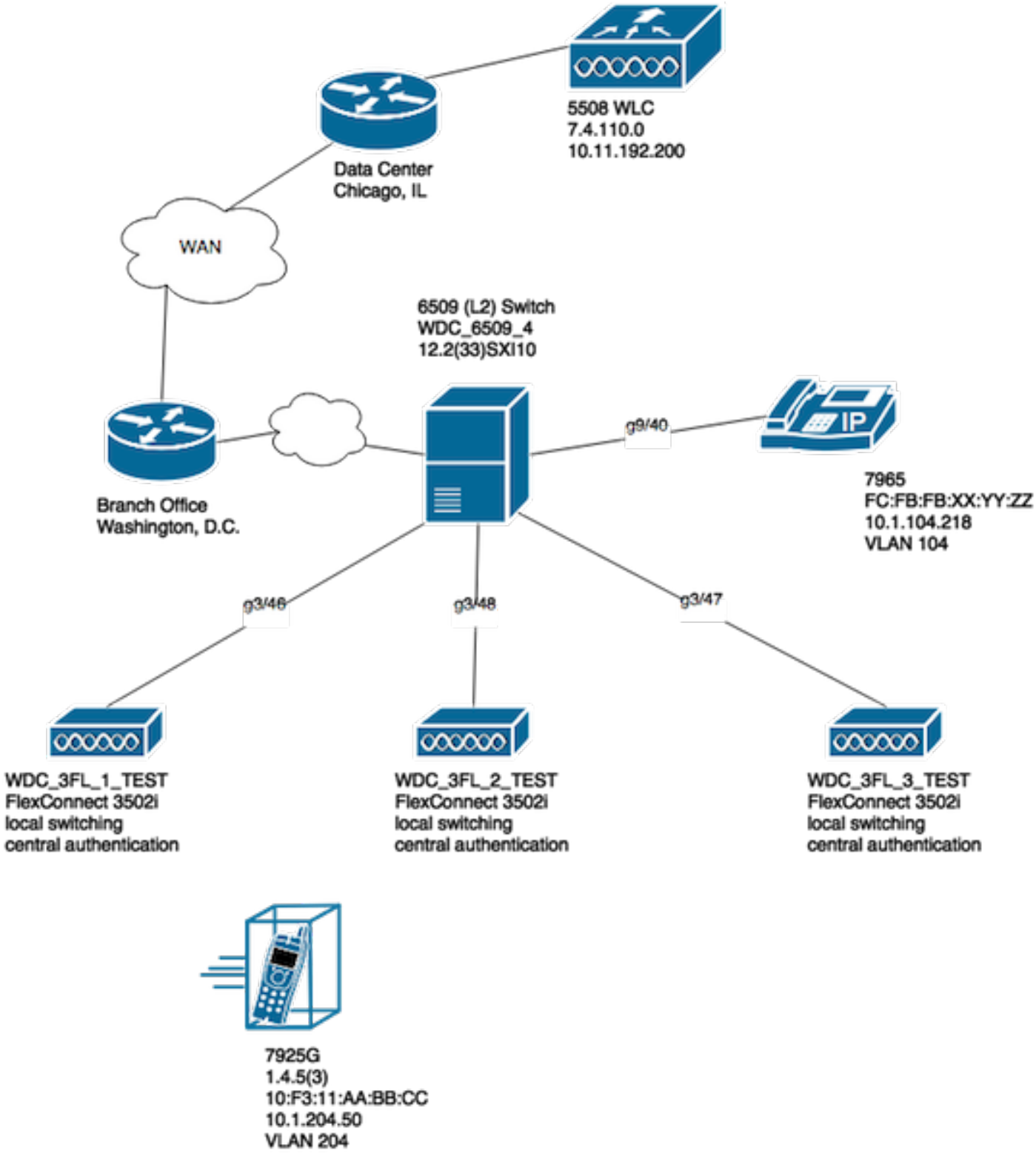
- Tipo di client (tablet, smartphone, notebook, ecc.)
- Marca e modello del dispositivo
- Versione del sistema operativo
- Modello scheda WLAN
- Versione driver scheda WLAN
- Supplicant used (Windows Zero Config / Auto Config, Intel PROSet,...)
- Sicurezza configurata per l'utilizzo da parte del client wireless e della WLAN (Open, PSK, EAP-PEAP/MSCHAPv2,...)
- Prendere nota di eventuali parametri client modificati rispetto alle impostazioni predefinite fornite dal fornitore in questione (stato di sospensione, parametri di roaming, U-APSD,...).

Nota: se necessario, è necessario includere anche eventuali informazioni o note aggiuntive relative ai dispositivi client fino a cui sono inclusi gli screenshot delle configurazioni WLAN.

IV. Topologia di rete

Per accelerare ulteriormente le operazioni di risoluzione dei problemi e il processo RCA (Root Cause Analysis), si consiglia sempre di fornire un diagramma della topologia di rete dettagliato e completo. Il diagramma della topologia di rete non deve solo includere dettagli sulla rete e sull'infrastruttura wireless, ma deve anche fornire informazioni dettagliate sui dispositivi wireless in questione che operano all'interno della rete (stampanti/scanner, VLAN client in uso, ecc.) e sulla loro posizione relativa l'una all'altra.

Per creare un diagramma di rete di questo tipo è possibile utilizzare diversi strumenti (Microsoft Visio, draw.io,...) e diversi stili. L'aspetto importante è semplicemente garantire che le informazioni corrette siano chiaramente riportate nel diagramma fornito per la revisione da parte di tutte le parti coinvolte e dei fornitori. Topologia di rete di esempio che acquisisce informazioni di base ma utili relative sia all'infrastruttura che ai dispositivi client, come mostrato nell'immagine.



V. Registrazione dei dettagli aggiuntivi e delle specifiche

Garantire che le informazioni appropriate vengano raccolte al momento di qualsiasi test con i dispositivi client in cui gli utenti finali riscontrano problemi. Si consiglia di creare preventivamente un foglio di calcolo o un modulo simile per registrare tutti i problemi del client e i relativi dettagli osservati al momento del test, come nell'esempio seguente:

Indirizzo MAC	Username	Descrizione del sintomo segnalato	Ora in cui l'utente finale ha osservato il	Eseguire il ping del gateway predefinito	Stato del segnale WiFi (connesso/tentativo di connessione)	Record ipconfig /a

		sintomo	S/N		
xxyy.aabb.0011 utente_test1	Si disconnette in modo intermittente dal punto di accesso.	Connettività di rete e associazione wireless interrotte da AP3.	N	Tentativo di connessione in corso	ifconfig en0 en0: flags=8863<UP,B mtu 1500 etere xx:yy:aa:b inet6 fe80::848: inet 192.168.10. nd6 options=20 supporti: selezio stato: attivo

L'obiettivo di questo esercizio è quello di documentare e determinare un modello di interesse comune, nonché di ottenere un'immagine accurata dei problemi in questione. Una volta preparato il foglio di calcolo per la raccolta dei dati, è possibile iniziare i test. Di seguito sono riportate alcune considerazioni aggiuntive ma importanti.

> **Nota**: tutti i debug e le acquisizioni di pacchetti raccolti devono essere sincronizzati sullo stesso server NTP per una correlazione più semplice con i log e devono essere eseguiti contemporaneamente per ogni test.

> **Nota**: fornire un timestamp preciso che indichi quando il problema è stato rilevato e quando sembra ripresentarsi (se applicabile).

> **Nota**: raccoglie sempre i debug filtrati per indirizzo MAC del client sull'access point e sul WLC.

> **Nota**: non eseguire i comandi show e debug sull'access point nella stessa sessione Telnet/SSH/console, in quanto vengono eseguiti separatamente in una sessione diversa di conseguenza.

> **Nota**: si preferisce eseguire i debug AP su Telnet/SSH anziché su Console, poiché la console è in genere troppo lenta per essere efficace.

VI. WLC - Comandi Show e Debug

Quando si eseguono test per riprodurre e risolvere potenziali problemi di interoperabilità dei client wireless, è indispensabile raccogliere i debug e i registri aggiuntivi dall'infrastruttura wireless in uso. Nelle due sezioni vengono descritti in dettaglio i log specifici e l'output del debug iniziale raccolti rispettivamente dal WLC e dall'AP.

Comandi di debug WLC

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

Per quanto riguarda la natura del problema in questione, è possibile aggiungere questi debug

WLC caso per caso:

- **debug aaa detail enable**: da utilizzare in caso di problemi di autenticazione con il server AAA
- **debug aaa events enable** - da utilizzare in caso di problemi di autenticazione con il server AAA
- **debug aaa all enable**: utilizzare questo comando per problemi di autenticazione. L'output di questo debug è dettagliato, quindi utilizzarlo solo quando assolutamente necessario (per casi di override AAA,...)
- **debug mobility handoff** - da utilizzare in caso di problemi di roaming tra WLC

Una volta che il problema è stato riprodotto con il client wireless in questione, e tutte le informazioni delineate nelle sezioni precedenti e successive sono state raccolte e documentate. Per eseguire questi comandi CLI, è necessario disabilitare i debug sul WLC.

```
debug disable-all
```

Comandi Show WLC

```
config paging disable

show time

show client detail <MAC_address>

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

Come accennato in precedenza, accertarsi di eseguire i debug WLC in una sessione Telnet/SSH e di raccogliere l'output di questi comandi show in un'altra sessione Telnet/SSH sul WLC. Lo stesso deve essere fatto per raccogliere i debug dell'access point e visualizzare l'output dei comandi descritto in questa sezione.

VII. AP - Comandi Show e Debug

Access point Cisco IOS® lightweight

Prima di avviare il debug sui Cisco IOS® Lightweight Access Point coinvolti nel test, come i Cisco 2600, 2700, 3700 o i Cisco Access Point del modello precedente. È necessario eseguire questi comandi CLI sull'access point per evitare un timeout al momento di una sessione Telnet/SSH/console sugli access point in questione quando il client esegue i test:

```
debug capwap console cli

config t

line vty 0 4

exec-timeout 0

session-timeout 0
```

Èinoltre possibile seguire questa procedura per utilizzare la connessione della console e sostituire l'istruzione **line vty 0 4** con la **console 0**, in modo da disabilitare di conseguenza i timeout di esecuzione e di sessione per una connessione seriale/console.

- line console 0 - utilizzare per modificare i parametri di timeout della sessione seriale
- line vty 0 4 - utilizzare per modificare i parametri di timeout della sessione Telnet/SSH

Comandi Show AP

Prima di iniziare il test, è necessario raccogliere un esempio di questi comandi show sull'access point. Raccogliere l'output di questi comandi show almeno due volte per ogni test che coinvolge il client wireless in questione, sia prima che dopo il completamento del test.

```
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
```

Comandi di debug AP

Dopo aver raccolto l'output iniziale dei comandi show sopra menzionati, è possibile abilitare i debug sullo stesso punto di accesso in una sessione Telnet/SSH separata, come mostrato. Assicurarsi di salvare l'intero output in un file di testo.

```
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
```

Contrassegna	Descrizione
d0	Radio da 2,4 GHz (slot 0)
d1	Radio 5 GHz (slot 1)
gestione	Pacchetti di gestione traccia
baccano	Informazioni ACK blocco di traccia
rcv	Traccia pacchetti ricevuti
tasti	Chiavi set di traccia
rxev	Traccia eventi ricevuti
txev	Traccia eventi di trasmissione
txrad	Trasmissione di traccia alla radio
xmt	Traccia pacchetti di trasmissione
txfail	Errori di trasmissione di traccia
tariffe	Rileva modifiche velocità

Per disabilitare i debug sull'access point una volta completati il processo di test e raccolta dei dati, è possibile eseguire questo comando CLI sull'access point:

```
u all
```

Access point AP-COS

per access point compatibili con lo standard 802.11ac wave 2 e versioni successive, ad esempio i modelli 1800, 2800 e 3800. I nuovi modelli di access point introducono un sistema operativo completamente nuovo per le piattaforme di access point note come AP-COS. Di conseguenza, non tutti i comandi precedentemente utilizzati sui tradizionali access point basati su Cisco IOS® lightweight sono ancora validi. Se la risoluzione di un problema implica l'interoperabilità con diversi dispositivi STA client e punti di accesso modello AP-COS, le informazioni devono essere raccolte dai punti di accesso AP-COS interessati dal test equivalente.

Prima di avviare il debug su uno o più access point AP-COS coinvolti nel test. È necessario eseguire questi comandi CLI sull'access point per evitare un timeout al momento di una sessione Telnet/SSH/console sugli access point in questione quando il client esegue i test:

```
exec-timeout 0
```

Comandi Show AP-COS

Prima di iniziare il test, è necessario raccogliere un esempio di questi comandi show sull'access point. Raccogliere l'output di questi comandi show almeno due volte per ogni test che coinvolge il client wireless in questione, sia prima che dopo il completamento del test.

```
term len 0

show clock show tech

show client statistics <client_MAC-address>

show cont nss status

show cont nss stats

show log
```

Serie 1800 | Comandi di debug AP-COS

Questi debug sono specifici della serie 18xx di access point. Ciò è dovuto al fatto che i chipset usati per la serie 1800 di access point sono diversi da quelli trovati nei punti di accesso della serie 2800/3800, quindi in questo scenario è richiesto un insieme diverso di debug. I bug corrispondenti ai access point serie 2800/3800 sono illustrati nella sezione successiva.

Dopo aver raccolto l'output iniziale dei comandi show menzionati, è necessario abilitare i debug sugli stessi punti di accesso 1800 in una sessione Telnet/SSH separata, come mostrato. Assicurarsi di salvare l'intero output in un file di testo.

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

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

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

debug dot11 client level info addr <client_MAC-address>

debug dot11 client datapath eapol addr <client_MAC-address>

debug dot11 client datapath dhcp addr <client_MAC-address>

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

In alcuni casi, potrebbe essere necessario abilitare anche i debug aggiuntivi sull'access point 18xx per risolvere ulteriormente i problemi di interoperabilità dei client. Tuttavia, questa operazione deve essere eseguita solo se/come richiesto da un tecnico Cisco TAC per una richiesta/un caso di assistenza corrispondente.

Poiché i debug aggiuntivi potrebbero non solo essere molto più dettagliati nell'output, ma possono anche introdurre un carico aggiuntivo sull'access point, pertanto è necessario più tempo per un'analisi corretta. Il che, in determinate condizioni, può potenzialmente interrompere il servizio se molti dispositivi client tentano di connettersi allo stesso punto di accesso durante il test o a variabili simili.

Per disabilitare i debug sul punto di accesso della variante AP-COS, su un access point serie 1800 o 2800/3800, una volta completato il processo di test e raccolta dei dati, è possibile eseguire questo comando CLI sull'access point:

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

Serie 2800/3800 | Comandi di debug AP-COS

Dopo aver raccolto l'output iniziale dei comandi show menzionati, è necessario abilitare i debug sugli stessi access point serie 2800/3800 in una sessione Telnet/SSH separata, come mostrato. Assicurarsi di salvare l'intero output in un file di testo.

```
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
```

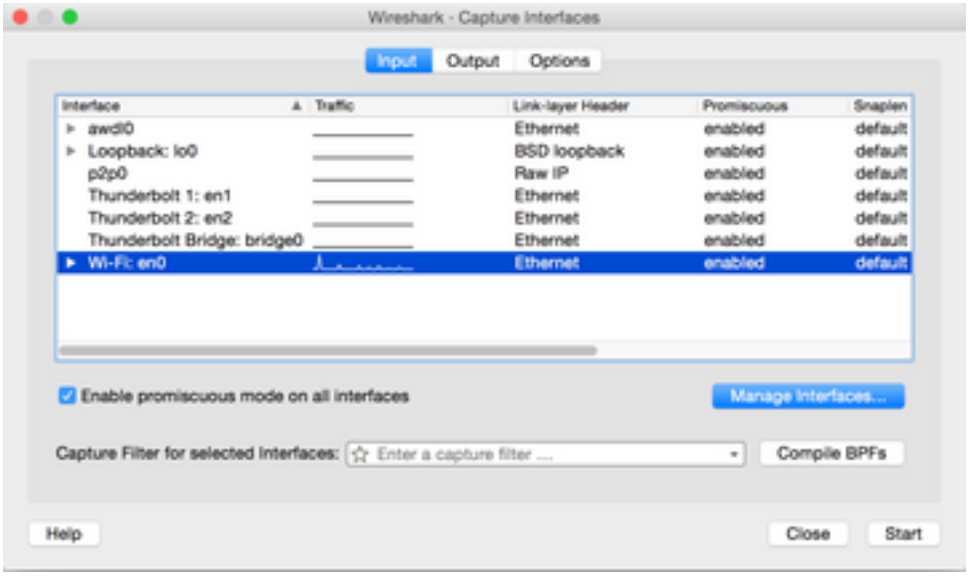
Per disabilitare i debug sull'access point serie 1800/2800/3800 al termine del processo di test e raccolta dei dati, è possibile eseguire questo comando CLI sull'access point:

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

VIII. Acquisizioni di pacchetti sul lato client

Dal dispositivo client in uso, se si tratta di un notebook, MacBook o simile, è necessario raccogliere l'acquisizione del pacchetto in modalità promiscua dall'interfaccia wireless del dispositivo client utilizzato per riprodurre il problema. Utilità comuni come Netmon 3.4 (solo Windows) o Wireshark possono essere facilmente scaricate e utilizzate per raccogliere questa cattura e salvarla in un file *.pcap. Dipende dal dispositivo, ci potrebbero essere anche mezzi per raccogliere un tcpdump o simile dal client in questione, quindi potrebbe essere necessario consultare il produttore del dispositivo client per assistenza a questo proposito.

Di seguito è riportato un esempio di configurazione di un'acquisizione Wireshark per l'interfaccia wireless su un MacBook Pro:



Come per qualsiasi acquisizione di pacchetti, indipendentemente dall'utilità utilizzata per raccoglierli, assicurarsi di salvare il file in un formato pcap (*.pcap, *.pcapng, *.pkt,...). In questo modo, non solo i tecnici Cisco di un reparto possono visualizzare facilmente i file di acquisizione dei pacchetti, ma anche i tecnici di altri fornitori e organizzazioni (Intel, Apple,...). Ciò consente un processo di cooperazione e collaborazione più fluido, che facilita ulteriormente sia Cisco che i fornitori di dispositivi client a collaborare meglio tra loro per individuare e risolvere eventuali problemi di interoperabilità.

IX. Acquisizioni pacchetti OTA (Over-the-Air)

Per risolvere efficacemente eventuali problemi di interoperabilità wireless, è fondamentale raccogliere un pacchetto OTA di qualità per l'acquisizione del problema. Ciò consente l'analisi dettagliata della comunicazione wireless 802.11 effettiva tra il client wireless e le radio del punto di accesso in questione, oltre a fornire un'ulteriore prospettiva dei registri lato client e dell'infrastruttura wireless, e dei debug. Si tratta di un passo fondamentale che deve essere compiuto per ogni test di un potenziale problema di interoperabilità wireless, senza eccezioni.

Tuttavia, spesso il cliente finale non è adeguatamente attrezzato o preparato per raccogliere le acquisizioni di pacchetti OTA. Si tratta di un ostacolo comune che i tecnici wireless spesso devono affrontare e devono collaborare con il cliente per superarlo in diversi modi. Questo articolo dei forum del supporto Cisco può essere un buon punto di partenza per guidare e formare il cliente a riguardo:

sniffing wireless 802.11 / acquisizione pacchetti

Èdi fondamentale importanza che le acquisizioni di pacchetti OTA vengano raccolte in un formato di file pcap (*.pcap, *.pcapng, *.pkt,...) e includano metadati 802.11 (RSSI, canale, velocità dei dati,...). Lo sniffer OTA deve inoltre essere sempre tenuto in prossimità del dispositivo client in questione durante le prove, per garantire una prospettiva accurata del traffico inviato e ricevuto dal/dal dispositivo client sottoposto a prova.

> **Nota**: se i test in questione riguardano un dispositivo client in roaming, in cui più di un canale 802.11 deve essere monitorato in un'acquisizione aggregata di pacchetti. Quindi attualmente

non si consiglia di utilizzare AirMagnet WiFi Analyzer di Fluke Networks.

Il motivo è che le acquisizioni aggregate di pacchetti con l'uso di questa utility vengono attualmente salvate in un formato di file proprietario e non in un formato di tipo pcap che possa essere visualizzato facilmente in Wireshark o altre utility simili. Assicuratevi che il file di acquisizione dei pacchetti OTA sia in un formato non proprietario, in modo che tutte le parti coinvolte e i fornitori coinvolti possano esaminare rapidamente tutti i file di acquisizione in qualsiasi momento e, in ultima analisi, velocizzare qualsiasi tentativo di risoluzione.

in un formato leggibile dall'attuale Wireshark e che include metadati 802.11 (RSSI, canale, velocità dei dati). Per ulteriori informazioni, visitare il sito Web all'indirizzo: https://supportforums.cisco.com/document/75331/80211-wireless-sniffing-packet-capture#sthash.Xhlx5LSS.dpuf
Di seguito sono riportati alcuni metodi comuni per raccogliere un'acquisizione di pacchetti OTA:

- AirPCAP con Wireshark
- MacBook Pro
- OmniPeek Professional, OmniPeek Enterprise,...
- Assistente remoto OmniPeek (ORA)
- Cisco AP in modalità Sniffer

Acquisizioni 802.11n

Per le acquisizioni di pacchetti OTA che coinvolgono client wireless 802.11n, al momento c'è una maggiore flessibilità e facilità d'uso. Ciò è dovuto a una più ampia varietà di adattatori WLAN USB wireless disponibili che possono essere facilmente utilizzati con una serie di strumenti, come OmniPeek e altri.

Prendere nota di come le funzionalità delle schede di rete wireless specifiche utilizzate per raccogliere un'acquisizione OTA 802.11n siano paragonabili a quelle del chipset WLAN effettivamente utilizzato dai dispositivi client che si sta tentando di risolvere. Ad esempio, se il dispositivo client presenta un potenziale problema di interoperabilità wireless che utilizza un chipset 802.11n compatibile con 2 stream spaziali (2SS). Si consiglia quindi di assicurarsi che la scheda di rete wireless utilizzata per raccogliere un pacchetto OTA sia anche una scheda 2S o di livello superiore, con specifiche 802.11n o successive.

Acquisizioni OTA 802.11ac

Per le acquisizioni di 3 stream spaziali (3SS) 802.11ac, potete utilizzare le funzionalità di sniffing nativo di un MacBook Pro modello 2014 o successivo con Mac OS X 10.10.x o superiore. In caso di risoluzione di un dispositivo client 802.11ac a 2 stream spaziali, potete anche utilizzare un MacBook Air per le clip 802.11ac. Il modello Air di MacBooks utilizza chipset WLAN 2SS solo al momento della stesura di questo documento. È possibile fare riferimento all'articolo dei forum di supporto Cisco elencati per istruzioni su come raccogliere le acquisizioni di pacchetti OTA con l'uso di Mac OS X, tramite una varietà di metodi:

Sniffing wireless con Mac OS X 10.6+

Èinoltre possibile utilizzare una serie 2702/2802/3702/3802 o un access point simile in modalità sniffer per raccogliere un'acquisizione corretta del pacchetto 802.11ac con 3SS. È inoltre possibile fare riferimento alla risorsa elencata per un elenco aggiornato delle schede di rete wireless

802.11ac disponibili. Alcuni di essi sono potenzialmente in grado di essere utilizzati con strumenti comuni come OmniPeek e altri per raccogliere un pacchetto di acquisizione 802.11ac (chipset da Ralink, Atheros,...):

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

Èinoltre possibile utilizzare una serie 2702/2802/3702/3802 o un access point simile in modalità sniffer per raccogliere un'acquisizione corretta del pacchetto 802.11ac con 3SS. Per comodità, le istruzioni dettagliate su come configurare un Cisco AP in modalità sniffer e raccogliere un'acquisizione pacchetto OTA sono disponibili nell'articolo dei forum di supporto Cisco:

Cisco AP in modalità Sniffer

Per la risoluzione dei problemi di roaming con un dispositivo client wireless, il problema più comune è raccogliere in modo efficace un pacchetto OTA acquisito su più canali. Questo metodo di monitoraggio simultaneo di più canali 802.11 è ottenuto dalla raccolta di pacchetti OTA aggregati. Per ottenere questo risultato, si consiglia di utilizzare più schede WLAN USB compatibili con 802.11ac con un software di analisi di rete compatibile. Alcune comuni schede WLAN USB compatibili con lo standard 802.11ac includono la scheda Savvius WiFI per OmniPeek (802.11ac), Netgear A6210 o simili.

X. Riepilogo

Di seguito è riportato un breve riepilogo delle informazioni da raccogliere per risolvere in modo efficace un potenziale problema di interoperabilità dei client wireless con un CUWN. Se necessario, questa sezione fungerà da sezione di riferimento rapido.

I. Definizione del problema

- Il problema è limitato a uno specifico modello di punto di accesso e/o di tipo radio (2,4 GHz contro 5 GHz)?
- Il problema si verifica solo su una o più versioni specifiche del software WLC (Wireless LAN Controller)?
- Il problema si verifica solo con versioni specifiche di tipi di client e/o software (versione del sistema operativo, versione del driver WLAN, ecc.)?
- Esistono altri dispositivi wireless che non rilevano questo problema? In caso affermativo, quali?
- Il problema è riproducibile quando il client è collegato a un SSID aperto, una larghezza di canale di 20 MHz e 802.11ac disabilitato? (Il problema si verifica solo in modalità 11n rispetto alla modalità 11ac)
- Se il problema non è riproducibile con un SSID aperto, a quale configurazione di protezione minima è associato il problema? (PSK o 802.1X sulla WLAN)
- Quali erano le precedenti versioni software e di configurazione valide?

II. Configurazione e registri WLC

Raccogliere quanto segue dalla CLI del WLC in questione:

- config paging disattivato

- show run-config

In alternativa, è possibile raccogliere solo questi output in base alle esigenze:

- config paging disattivato
- show run-config no-ap
- show wlan apgroups

Backup della configurazione WLC tramite TFTP, FTP,...(GUI: **Comandi > Upload File > Configurazione**)

Syslog dal WLC

III. Informazioni sul dispositivo client

- Tipo di client (tablet, smartphone, notebook, ecc.)
- Marca e modello del dispositivo
- Versione del sistema operativo
- Modello scheda WLAN
- Versione driver scheda WLAN
- Supplicant used (Windows Zero Config / Auto Config, Intel PROSet,...)
- Sicurezza configurata per l'utilizzo da parte del client wireless e della WLAN (Open, PSK, EAP-PEAP/MSCHAPv2,...)

> **Nota**: tutti i parametri client sono stati modificati rispetto alle impostazioni predefinite fornite dal fornitore in questione. (stato di sospensione, parametri di roaming, U-APSD,...)

IV. Esempio di topologia di rete

Include una rappresentazione e/o dettagli relativi ai dispositivi wireless della rete (stampanti/scanner, WLC, ecc.)

V. Creare un foglio di calcolo per registrare tutti i problemi dei client

Esempio:

Indirizzo MAC	Username	Descrizione del sintomo segnalato	Ora in cui l'utente finale ha osservato il sintomo	Eseguire il ping del gateway predefinito S/N	Stato del segnale WiFi (connesso/tentativo di connessione)	Record ipconfig /all equivalente

L'obiettivo di questo esercizio è quello di aiutare a identificare un modello comune e di mostrare un'immagine più accurata del problema o dei problemi in questione.

VI. Comandi show e debug sul WLC

Raccogli questi debug WLC tramite la CLI:

- **timeout sessioni di configurazione 0**
- **debug client <indirizzo_MAC>**

- **debug dhcp message enable**

Aggiungere i debug aggiuntivi caso per caso:

- **debug aaa detail enable** - da utilizzare in caso di problemi di autenticazione con il server AAA
- **debug aaa events enable** - da utilizzare in caso di problemi di autenticazione con il server AAA
- **debug aaa all enable**: utilizzare questa opzione per problemi di autenticazione. La versione è dettagliata, quindi utilizzarla solo quando necessario (per casi di override AAA e simili)
- **debug mobility handoff** - da utilizzare per problemi di roaming tra WLC

Raccogli l'output dei comandi show del WLC dalla CLI:

- **config paging disattivato**
- **show time**
- **show client detail <mac-address of client>** (annotare lo stato del client sul WLC)
- Eseguire il ping del client dal WLC

Al termine del test, usare questo comando per interrompere tutti i debug correnti sul WLC:

- **debug disable-all**

VII. Comandi show e debug sull'access point

Access point Cisco IOS® leggeri

In questa sezione vengono illustrati in dettaglio i debug richiesti per i modelli serie 1700/2700/3700 o precedenti.

Per evitare il timeout di una sessione AP durante una sessione Telnet/SSH/console, utilizzare i seguenti comandi:

- **cli console debug capwap**
- **config t**
- **console linea 0** - utilizzare per modificare i parametri di timeout della sessione seriale
- **line vty 0 4** - utilizzare per modificare i parametri di timeout della sessione Telnet/SSH
- **exec-timeout 0**
- **session-timeout 0**
- **termine len 0**

Prima di iniziare il test, raccogliere un esempio di questi comandi show sull'access point. Almeno raccogliere due campioni di questo output, sia prima che dopo il completamento dei test con l'uso di questi comandi show dell'access point dalla CLI:

- **termine len 0**
- **mostra orologio**
- **show tech**
- **show capwap client mn**
- **mostra int do1 dfs**
- **show logging (visualizza registri)**
- **altro event.log**
- **show trace dot11_rst formato del tempo di visualizzazione locale**

- show trace dot11_rst
- show trace dot11_bcn formato ora di visualizzazione locale
- show trace dot11_bcn

Raccogliere i seguenti debug AP dalla CLI:

- debug dot11 { d0 | d1 } indirizzo monitor <indirizzo_MAC>
- debug dot11 { d0 | d1 } traccia stampa client mgmt chiavi rxev txev rcv xmt txfail
- mon

Al termine del test, usare questo comando per disabilitare i debug:

- u tutto

AP-COS AP

In questa sezione vengono illustrati in dettaglio i debug richiesti per i access point serie 1800/2800/3800.

Per evitare il timeout di una sessione AP durante una sessione Telnet/SSH/console, utilizzare i seguenti comandi:

- exec-timeout 0

Prima di iniziare il test, raccogliere un esempio dei comandi show sull'access point. Almeno raccogliere due campioni di questo output, sia prima che dopo il completamento dei test con l'uso di questi comandi show dell'access point dalla CLI:

- termine len 0
- mostra orologio
- show tech
- show client statistics <indirizzo_MAC_client>
- show cont nss status
- show cont nss stats
- show log

Per i punti di accesso serie 1800, raccogliere i seguenti debug AP dalla CLI:

- debug dot11 client level events addr <indirizzo-MAC_client>
- debug dot11 errori a livello di client addr <indirizzo-MAC_client>
- debug dot11 client level critical addr <indirizzo-MAC_client>
- debug dot11 client level info addr <indirizzo-MAC_client>
- debug dot11 client datapath eapol addr <indirizzo-MAC_client>
- debug dot11 client datapath dhcp addr <indirizzo-MAC_client>
- debug dot11 client datapath arp addr <indirizzo-MAC_client>
- mon

Per i punti di accesso serie 2800/3800, raccogliere i seguenti debug AP dalla CLI:

- config ap indirizzo-traccia-client add <indirizzo-MAC_client>
- abilita tutti i filtri di traccia client dell'access point di configurazione
- config ap client-trace output console-log enable
- avvio traccia client ap di configurazione

- **mon**

Al termine del test, usare questo comando per disabilitare i debug:

- **arresto traccia client ap di configurazione**

VIII. Acquisizioni lato client

Raccogliere un pacchetto Netmon 3.4 (solo Windows XP o 7) o Wireshark dalla scheda WLAN del dispositivo client.

IX. Acquisizioni OTA

Acquisizioni 802.11n

- AirPCAP con Wireshark
- MacBook Pro
- OmniPeek Professional, Enterprise,...
- Assistente remoto OmniPeek (ORA)
- Cisco AP in modalità Sniffer

Acquisizioni 802.11ac

- Per le acquisizioni 11ac 3SS, è possibile utilizzare un Macbook Pro 2014 o successivo con 10.10.x o superiore (non utilizzare MacBook Air per le acquisizioni 11ac se possibile, in quanto attualmente è un dispositivo 2SS).
- In modalità sniffer, è possibile usare anche un access point Cisco serie 2702, 3702 o simile.
- Per scenari di roaming e con l'utilizzo di software di analisi di rete professionale come OmniPeek di Savvius. Si consiglia di utilizzare più schede WLAN USB compatibili con lo standard 802.11ac, ad esempio la scheda WiFI Savius per OmniPeek (802.11ac), Netgear A6210 o simili.

XI. Appendice A - Suggerimenti e consigli aggiuntivi

Windows

Raccogliere informazioni aggiuntive relative alla connessione wireless corrente e altri dettagli correlati direttamente da un PC Windows. Dalla riga di comando (CMD) di Windows è possibile usare i seguenti comandi relativi alla rete wlan netsh:

```
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
```

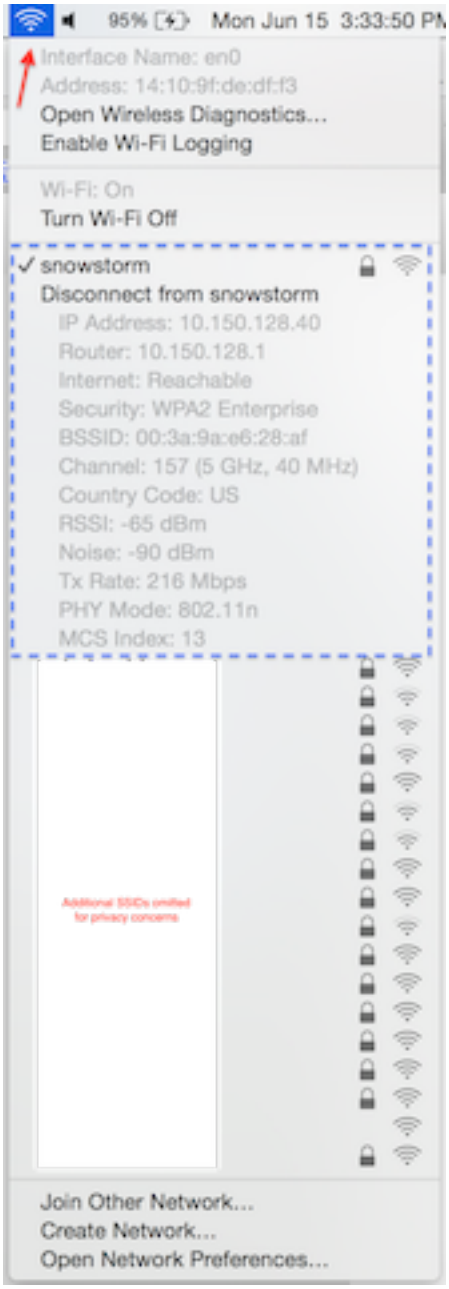
```
         Basic rates (Mbps) : 24 39 156
         Other rates (Mbps) : 18 19.5 36 48 54
    BSSID 2                 : 00:3a:9a:e6:28:a0
         Signal             : 91%
         Radio type         : 802.11n
         Channel            : 6
         Basic rates (Mbps) : 1 2
         Other rates (Mbps) : 5.5 6 9 11 12 18 24 36 48 54

-- More  --
```

macOS (in precedenza OS X)

Per raccogliere l'output equivalente come comando **ipconfig /all** su un PC Windows, è possibile usare il comune comando Linux/Unix di **ifconfig** per elencare le informazioni dettagliate per tutte le interfacce di rete su un MacBook Apple. Se necessario, potete anche specificare di ricevere l'output solo per l'interfaccia wireless nativa per un dato MacBook (en0 o en1, dipende dal modello). Ad esempio:

```
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
```

Per ottenere informazioni rapide ma dettagliate relative alla connessione wireless corrente su un MacBook. È inoltre possibile selezionare l'icona WiFi nell'angolo superiore destro del desktop mentre si tiene contemporaneamente premuto il pulsante di **opzione** sulla tastiera, come mostrato nell'immagine.



Un'altra opzione utile è quella di utilizzare l'utilità della riga di comando nascosta chiamata aeroporto. Si consiglia di utilizzarlo solo con il proprio MacBook o con uno in uso in un ambiente di emulazione. Poiché alcuni amministratori di rete potrebbero non voler concedere l'accesso a questa utility sul MacBook di un utente finale, è necessario prestare la dovuta attenzione. Per continuare, immettere quanto segue in Terminale sul MacBook in questione:

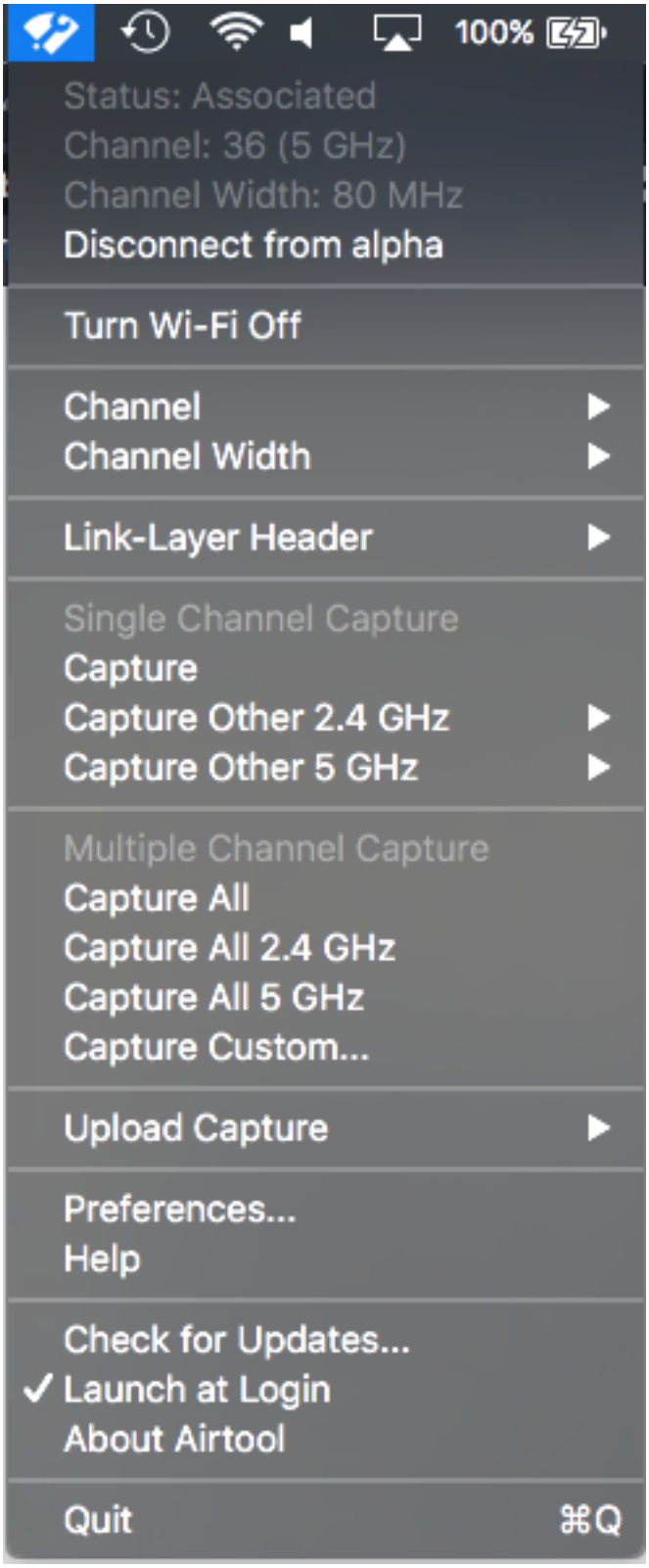
```
sudo ln -s
/System/Library/PrivateFrameworks/Apple80211.framework/Versions/Current/Resources/airport
/usr/local/bin/airport
```

Ora è possibile utilizzare l'utility CLI dell'aeroporto con facilità. Di seguito è riportato un esempio:

```
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
```

Per facilitare ulteriormente il processo di raccolta di un'affidabile, singola acquisizione di pacchetti OTA a 802.11 canali con l'uso delle funzionalità di un MacBook Pro o simili. È possibile utilizzare le funzionalità incorporate in macOS con il metodo Diagnostica wireless > Sniffer o simili, ma è possibile utilizzare anche un'utilità di terze parti chiamata Airtool (OS X 10.8 e versioni successive). Il vantaggio è un'interfaccia semplice per raccogliere rapidamente un pacchetto OTA acquisizione, che viene salvato direttamente sul desktop con pochi clic attraverso l'interfaccia utente dell'app direttamente dalla barra dei menu superiore sullo schermo.



Ulteriori informazioni e link per il download di Airtool sono disponibili al seguente indirizzo:

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

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).