CUWN にかかわるワイヤレス クライアントの相互運用性の問題に関するトラブルシューティング ガイド

目次

概要

この資料は Cisco Unified Wireless Network（CUWN）ソリューションと起こるとき最初に効果的にそのようなワイヤレス相互運用性の問題をか調査し、解決するために集められるどんな情報ニーズ詳しく記述します。 そのような包括的なアプローチのための必要はワイヤレス クライアント デバイスおよび Access Point（AP）無線の数および組み合わせの増加とますます重要になります。

前提条件

要件

次の項目に関する知識が推奨されます。

- Ciscoワイヤレス APS
- ワイヤレス LAN コントローラ（WLC）
- 関連ネットワークデバイス

使用するコンポーネント

このドキュメントは、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。 稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

> **注:** この資料のための意図されていた聴衆は既にこれらのトピックの使用、設定およびトラブルシューティングについて詳しく知っている管理者およびベテランの無線ネットワークエンジニアです。

背景説明

存在 し、成長し続けなさいさまざまなクライアントデバイスを与えられてことが分るためによく

あります。 いろいろな問題はに関して確立しましたり、維持します単に起こりか、または無線ネットワークへの接続からほとんどを抜き出し、インフラストラクチャをサポートできます。

これは頻繁にクライアントデバイスや無線インフラストラクチャー自体の方の簡単なコンフィギュレーション問題に来ることができます。 ただし、場合によってはこれはそれを（すなわち要求元、WLAN アダプタ、ワイヤレス ドライバ、等）サポートする、および/または疑わしい APS ことができますコンポーネントおよび特定のクライアントデバイスに関して相互運用性の問題に帰因させる。 ワイヤレス エンジニアとして、そのような相互運用性の問題は識別する機会を提起し解決し、可能性としては複雑なチャレンジを解決します。

説明されているものがへのこの技術情報でその他の情報はそのような必要条件を定めるかもしれない無限数の変数を与えられて要求され、ケース バイ ケースで集められるために必要とされるかもしれません。 ただし、ここに詳述される情報は潜在的な無線クライアント 相互運用性の問題に対処する一般的 なガイドラインです。

I. 問題の定義

断固になるために効果的にインテントにおける問題にアプローチする第一歩は正確に手もと問題を定義することです。 これを行うために、これらの質問の少くともそれを頼まれます確認すれば返事は明確に文書化されています:

- 問題は APS や無線型（すなわち 2.4 GHz vs 5 GHz）の特定のモデルに制限されますか。
- 問題は WLC ソフトウェアの特定のバージョンでだけ観察されますか。
- ありますクライアントのタイプやソフトウェア（すなわち OS バージョン、WLAN ドライバ バージョン、等）の特定のバージョンだけと直面する問題は
- この問題に直面しない他のどのワイヤレス デバイスもありますか。 その場合、何ですか。
- ディセーブルにされるクライアントが 20 MHz のチャネル幅と開いた SSID のような簡単だったワイヤレス設定、および 802.11ac に接続される間、問題は再生可能ですか。（すなわち問題を起こります 802.11n モードで vs 802.11ac モードだけか。します）。
- 問題がどんな最小セキュリティとコンフィギュレーションで開いた SSID と再生可能、問題ではない場合見られますか。（WLAN のすなわち PSK か 802.1X）。
- 前の運用コンフィギュレーションおよびソフトウェア バージョンとは何か。

II. WLC 設定および概要ログ

実行構成

例外なしで、それは顧客、特定の設定および他のそのような詳細によって使用される機能の詳しい確認のための顧客の WLC 設定を集める絶対必要です。 これを行うために、疑わしい WLC に Telnet/SSH セッションを設定し、テキストファイルにこれらの CLI コマンドの出力を保存して下さい:

```
config paging disable

show run-config
```

完全な実行構成出力は、加入された APS および関連する RF 情報に関して詳細な情報が含まれているので、先祖など常に好まれます 場合によってはおよび状況、のようなけれども加入される多数の APS の WLC と当初働く時（2500+ APS のすなわち 8510 WLC）。 APS の数がある完了するために実行構成は 30 分または多くを奪取 するかもしれませんことを完全の示すので最初に速

い確認のためのそのような AP 情報なしで WLC のちょうど設定を集めることを好むかもしれません。 ただし後で出力される完全な実行構成を集めるために、それはまだ必要であるかもしれません。

これを行うために、テキストファイルにオプションでこれらの CLI コマンドの出力を集めることができます:

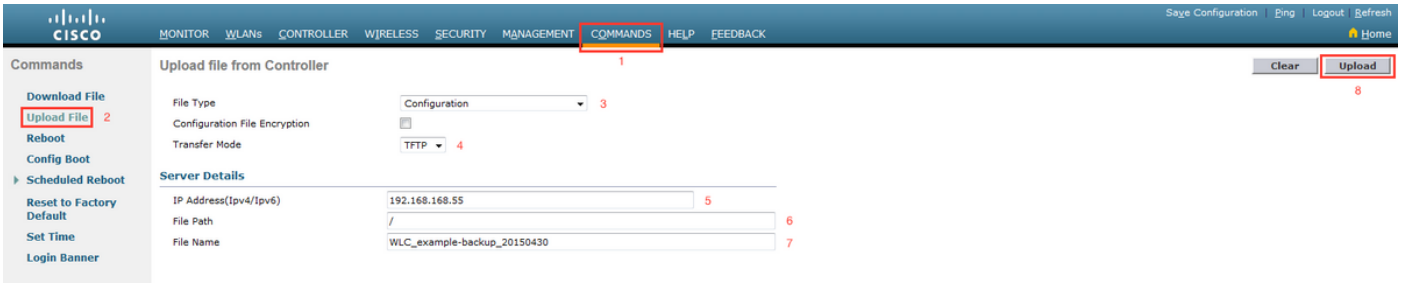
```
config paging disable

show run-config no-ap

show wlan apgroups
```

WLC コンフィギュレーション ファイル

提示実行構成に加えてまたは実行**構成非 ap** 出力を、またそれ WLC 設定の完全バックアップを同様に集めるために推奨されます**示して下さい**。 これは支援 Cisco ラボ 環境の顧客の問題を試み、再現 するためにラボが TAC/HTTS および BU 両方拡大によって行なわれる必要を作り直す場合、です。 WLC のバックアップは TFTP または FTP の使用と、疑わしい WLC の GUI か CLI によって TFTP/外部 FTP サーバにコンフィギュレーション ファイルを保存する集めることができます。 下記の例は TFTP の使用を用いる WLC のバックアップを、保存するために GUI および CLI 両方の使用方法を表示したものです:

GUI

コマンド > イメージに示すように**アップロード ファイル** > **設定** > **アップロード**。



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
```

WLC からの Syslogs

現時点で、また必要に応じて追加確認のための WLC から現在の口グを集めたいと思います。 理想的には報告された問題が再現 されるという、無線クライアントのテストの直後のこれらの口グを集めたいと思います。 顧客が外部のsyslog サーバに WLC 口グをエクスポートする場合、そこにからそれらを取得したいと思います。 さもなければ、msglog を保存することができ、この CLI セッションを保存することによって WLC でロ一カルで保存された traplog は現在別のテキストファイルに出力しました:

```
config paging disable

show msglog

show traplog
```

III.クライアントデバイス 詳細および情報

次のステップは使用中の潜在的なワイヤレス相互運用性の問題に直面するクライアント デバイスに関して同様に多くの情報および仕様を収集することです。 そのような情報はこれらに含む、必ずしも制限する必要があります:

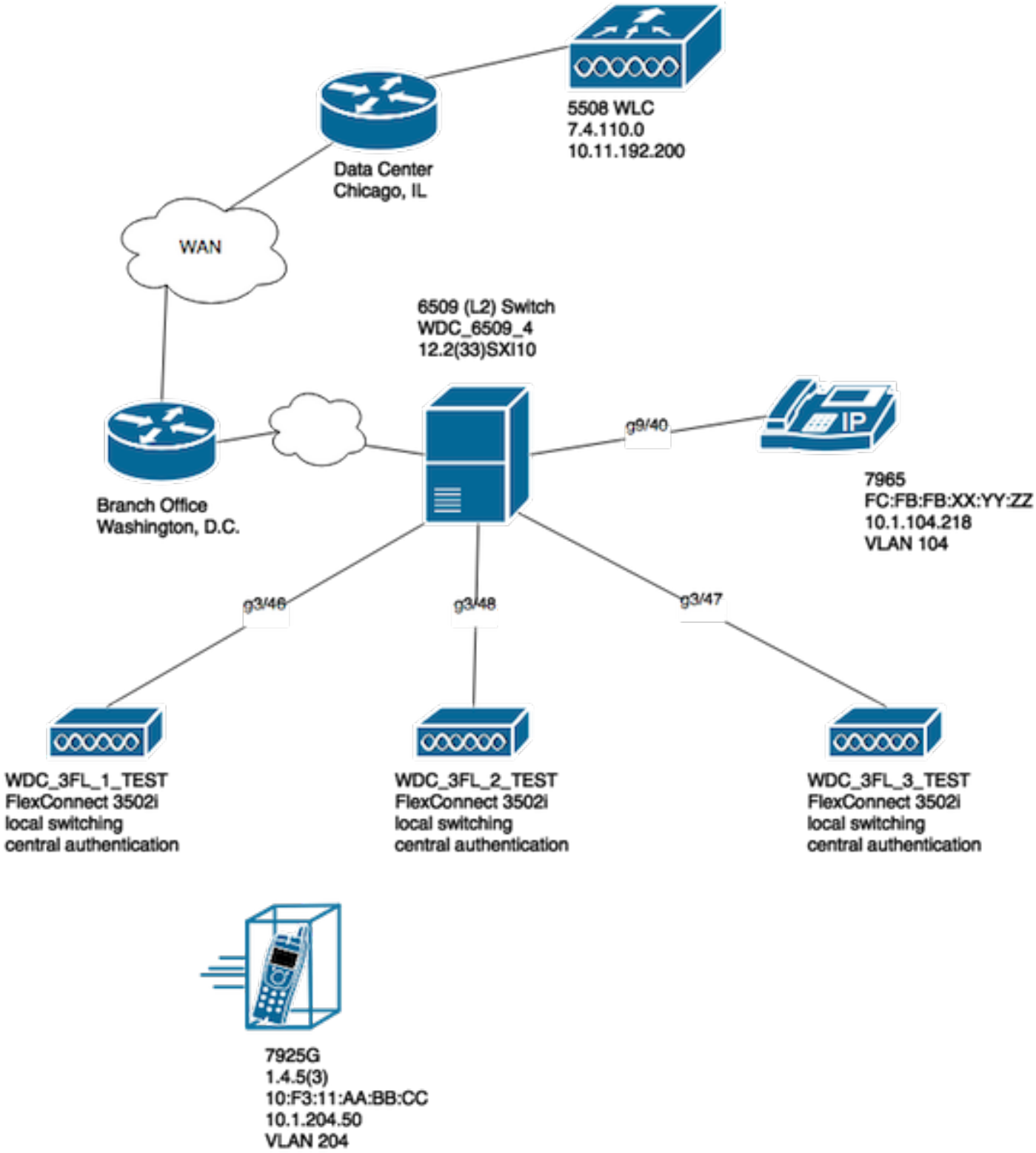
- クライアントのタイプ（すなわちタブレット、smartphone、ノート PC、等）
- デバイスは作り、模倣します
- OS バージョン
- WLAN アダプタ モデル
- WLAN アダプタ ドライババージョン
- 使用される要求元（すなわち Windows ゼロ構成/自動設定、Intel PROSet、等）
- 無線クライアントによって使用のために設定されるセキュリティおよび WLAN （すなわち、PSK、EAP-PEAP/MSCHAPv2、等開いて下さい）
- 疑わしいベンダーが提供するデフォルト設定から変更されたクライアント パラメータに注意して下さい（すなわちスリープ状態、ローミング パラメータ、U-APSD、等）。

注: WLAN 関連するコンフィギュレーションのスクリーン ショットが含まれているクライアント デバイスに関するその他の情報かメモはまた必要に応じて、等含んでいる必要があります。

IV.ネットワーク トポロジ

更にトラブルシューティングの作業および原因解析（RCA）プロセスを促進するために、詳しく、完全なネットワーク トポロジ ダイアグラムを提供することを常に推奨します。 ネットワーク トポロジ ダイアグラムはどんなクライアント VLAN 使用中でであって下さいかだけでなく、ネットワークおよび無線インフラストラクチャーについての詳細を含む必要がありますがまた疑わしい無線デバイスにネットワーク（すなわちプリンタ/スキャナー、等）かおよび相関的な位置の内で互い動作する把握を提供します。

いくつかのツール（すなわち Microsoft Visio、draw.io、等）およびいろいろな形式はそのようなネットワークダイアグラムを作成するのに使用することができます。 重要な側面は適切な情報がすべての複雑なパーティおよびベンダーが確認に提供するダイアグラムで明確に示されるように単にすることです。 基本をキャプチャ する ネットワーク例ネットワーク· トポロジ、イメージに示すようにインフラストラクチャおよびクライアントデバイス両方に関する有用な情報。



V. トラック追加詳細および仕様

エンドユーザが問題にとの直面すること適切な情報がクライアント デバイスが付いているあらゆるテストの時に収集されるようにするのを助けるため。 または類似した優先にこの例のようなテストの時に、観察されるすべてのクライアント問題および関連詳細を記録するためにスプレッドシートを作成することを推奨します:

MAC アドレス　Username 表示された現象の説明 時間エンドユーザによって観察される現象　Pi
ル
ウ

xxyy.aabb.0011 test_user1 断続的にアクセス ポ　AP3 からの失われたネットワーク接続およびワイ　N

イントからの切断。　ヤレス アソシエーション。

この演習の目標は文書化し、対象の一般的なパターンの判別を、また問題の正確な情報を手もとに得るのを助けることです。 このスプレッドシートがデータ収集に使用するために準備されればテストを始めて現在準備ができています。 いくつかの追加、けれども重要な考慮事項は次の通りです:

注: ログとより容易な相関の同じ NTP サーバに同期されるすべてのデバッグおよびパケットキャプチャによって集められる必要はある特定のテスト用のおよび同時に奪取 する必要があります。

注: 問題が観察されるとき、そして問題が回復ようであるとき正確なタイムスタンプをの提供します (該当する場合) 。

注: AP および WLC 両方のクライアントのMACアドレスごとにフィルタリングされるデバッグを常に収集して下さい。

注: 同じ Telnet/SSH/console セッション内の AP の show および debug コマンドを、これら別のセッションでそれに応じて別々にされるべきです実行しないで下さい。

注: AP デバッグはコンソールが有効であるには一般的に余りにも遅いので Telnet/SSH で vs コンソール行われるために好まれます。

VI. WLC - Show および debug コマンド

潜在的な無線クライアント 相互運用性の問題を再現 し、解決するためにテストが行なわれるときデバッグおよび追加ログが使用中の無線インフラストラクチャーから集められることは絶対必要です。 これら二つのセクションは WLC および AP から集める必要がある最初のデバッグ 出力および特定の ログをそれぞれ詳しく説明できます。

WLC Debug コマンド

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

手もと問題の性質に関してまたこれらの WLC デバッグをケース バイ ケースで追加できます:

- **デバッグ AAA 詳細 イネーブル**- AAAサーバにおいての認証 関連 問題がある場合これを使用して下さい
- **AAA イベント イネーブルをデバッグして下さい**- AAAサーバにおいての認証 関連 問題がある場合これを使用して下さい
- **debug aaa all enable** - auth 問題のためにこれを使用して下さい; このデバッグのための出力は冗長です従ってだけ絶対に必要な場合だけそれを使用して下さい（すなわち AAA 上書きするケース、等のために）
- **デバッグ モビリティ ハンドオフ**-そこに WLCs 間の問題をローミングしている時使用して下さい

問題が疑わしい無線クライアントおよびセクションで前に説明されている情報すべてとおよび再現 されればこれの後で集められ、文書化されています。 これらの CLI コマンドを実行するために、WLC のデバッグをディセーブルにして下さい。

```
debug disable-all
```

WLC Show コマンド

```
config paging disable

show time

show client detail <MAC_address>

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

以前に述べられるように、1 つの Telnet/SSH セッションの WLC デバッグを実行し、WLC に別の Telnet/SSH のこれらの show コマンドのための出力を集めるために確認して下さい。 コマンドがこれらで詳しいセクションを出力する AP debug および show を収集するために同じをして下さい。

VII. AP - Show および debug コマンド

軽量 Cisco IOS アクセス ポイント

2600、2700、3700 または前モデル Ciscoアクセスポイントのようなテストに、関連するあらゆる lightweight IOS AP のデバッグを開始する前に。 クライアント テスト時最初に疑わしい AP に Telnet/SSH/console セッションの時にタイムアウトを避けるために AP のこれらの CLI コマンドを実行して下さい:

```
debug capwap console cli

config t

line vty 0 4

exec-timeout 0

session-timeout 0
```

またコンソール接続を使用し、シリアル/コンソール接続のための exec およびセッション タイムアウトをそれに応じて無効に するために**行コンソール 0** によって **line vty 0 4** 文を代りに取り替

えるように次の手順に従うことができます。

- 行コンソール 0 -シリアル セッション タイムアウト パラメータを修正するのに使用して下さい
- line vty 0 4 - Telnet/SSH セッション タイムアウト パラメータを修正するのに使用して下さい

AP Show コマンド

テストを始める前に、最初に AP のこれらの show コマンドのサンプルを収集して下さい。 二度疑わしい無線クライアントを含む各テスト用のこれらの show コマンドの出力を少なくとも集める必要があります; テストの前後の両方は完了しました。

```
term len 0

show clock

show tech

show capwap client mn

show int do1 dfs

show logging

more event.log

show trace dot11_rst display time format local

show trace dot11_rst

show trace dot11_bcn display time format local

show trace dot11_bcn
```

AP Debug コマンド

前述 show コマンドの最初の出力を集めたら、示されているように今別途の Telnet/SSH セッションの同じアクセス ポイントのデバッグをイネーブルにすることができます。 テキストファイルに全体の出力を保存するために確認して下さい。

```
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
```

凡例

フラグ	説明
d0	2.4 GHz 無線（slot0）
d1	5 GHz 無線（1）スロット
mgmt	トレース管理パケット
Ba	トレース ブロック ACK 情報
rcv	トレース受け取り パケット
キー	トレース一定キー

rxev　トレースはイベントを受け取りました
txev　トレース送信イベント
txrad　無線で送るべきトレース送信
xmt　トレース送信パケット
txfail　トレース送信 障害
レート トレース レート変更

テストおよびデータ収集 プロセスが完了すれば AP のデバッグをディセーブルにするために、AP のこの CLI コマンドを実行できます:

```
u all
```

AP-COS アクセス ポイント

802.11ac ウェーブ 2 1800、2800 および 3800 モデル アクセス ポイントのような可能なアクセス ポイントおよびそれ以降に関しては。 これらの新しいモデル APS は AP-COS と言われるアクセス ポイント プラットフォームのための全く新しいオペレーティング システムをもたらします。 上で詳述されてのでそのように、まだ従来の軽量 Cisco IOS で以前に使用されるようにすべてのコマンドがアクセス ポイントを適用されます基づかせていませんでした。 解決するとき問題がさまざまなクライアント STA デバイスおよび AP-COS モデル APS と相互運用性の問題を含む場合、これらの情報は同等のテストに関連する AP-COS アクセス ポイントから収集する必要があります。

開始する前にあらゆる AP-COS のどのデバッグでもテストに関連する AP を模倣します。 クライアント テスト時タイムアウトを疑わしい AP に Telnet/SSH/console セッションの時に避けるために最初にこれらの AP の CLI コマンドを実行して下さい:

```
exec-timeout 0
```

AP-COS Show コマンド

テストを始める前に、最初に AP のこれらの show コマンドのサンプルを収集して下さい。 二度疑わしい無線クライアントを含む各テスト用のこれらの show コマンドの出力を少なくとも集める必要があります; テストの前後の両方は完了しました。

```
term len 0

show clock show tech

show client statistics <client_MAC-address>

show cont nss status

show cont nss stats

show log
```

1800 シリーズ | AP-COS Debug コマンド

これらのデバッグはアクセス ポイントの 18xx シリーズに特定です。 これは 2800/3800 シリーズ アクセス ポイントで見つけられるそれらと APS の 1800 シリーズに使用するチップセットによってが異なるこうして比較するとこのシナリオに別の一組のデバッグが必要となります事実が原因であり。 2800/3800 シリーズ APS 用の対応するデバッグは次の セクションでカバーされます

。

前述 show コマンドの最初の出力を集めたら、示されているように今別途の Telnet/SSH セッションの同じ 1800 のアクセス ポイントのデバッグをイネーブルにして下さい。 テキストファイルに全体の出力を保存するために確認して下さい。

```
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>
```

場合によっては、また更にクライアント 相互運用性の問題を解決することを 18xx AP の追加デバッグが可能にする必要があるかもしれません。 ただし、これはされた対応するサービス リクエスト/ケースのために Cisco TAC エンジニアが要求する if/as だけであるはずです。

追加デバッグがだけでなく、出力ではるかに冗長であるかもしれませんが、のでまた AP の追加ロードを導入できます同様にそれ故に適切な分析のために追加を時間を計る必要とする。 特定の条件下で可能性としてはサービスを破壊する場合があるかどれが多くのクライアントデバイスがテストか同じような変数の下で同じ AP に接続されるように試みる場合。

AP-COS バリアント アクセス ポイントのデバッグをディセーブルにするため- 1800 または 1800 シリーズ AP でかどうか-一度テストおよびデータ収集 プロセスは、AP のこの CLI コマンドを実行できます完了します:

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

2800/3800 シリーズ | AP-COS Debug コマンド

前述 show コマンドの最初の出力を集めたら、示されているように今別途の Telnet/SSH セッションの同じ 2800/3800 のアクセス ポイントのデバッグをイネーブルにして下さい。 テキストファイルに全体の出力を保存するために確認して下さい。

```
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
```

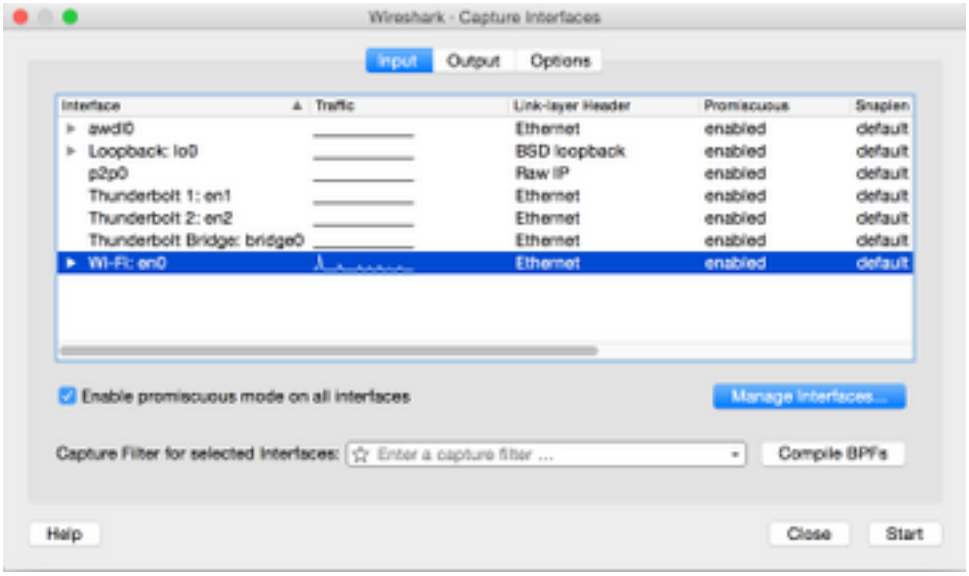
テストおよびデータ収集 プロセスが完了すれば 1800/2800/3800 シリーズ AP のデバッグをディセーブルにするために、AP のこの CLI コマンドを実行できます:

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

VIII.クライアント側パケットキャプチャ

使用中のクライアントデバイスからノート PC、MacBook または類似したなら、使用されるクライアントデバイスのワイヤレス インターフェイスから問題を再現 するのに混合モード パケット キャプチャを集めて下さい。 Netmon 3.4 （ Windows だけ ）または Wireshark のようなよくあるユーティリティが容易にダウンロードされ、このキャプチャを集め、*.pcap ファイルにそれを保存するのに使用することができます。 それはデバイスによって決まります、また疑わしいクライアントから tcpdump をまたは類似した集める手段（ 方法 ）があるかもしれません従って支援のためのクライアントデバイス 製造業者とこの点で相談する必要があるかもしれません。

プロ MacBook のワイヤレス インターフェイスのための Wireshark キャプチャを設定する例はここにあります:



あらゆるパケットキャプチャと同様に、どんなに関係なくユーティリティがそれを集めるのに使用されているか pcap ファイルフォーマット（ すなわち *.pcap、*.pcapng、*.pkt、等 ）のファイルを保存するために確認して下さい。 これはだけでなく、あらゆる部門の Ciscoエンジニアが同様にパケットキャプチャ ファイル、他の開発元からのエンジニアおよび組織を簡単に表示することができるようにすることです（ すなわち Intel、Apple、等 ）。 これは潜在的な相互運用性の問題を調査し、解決するために協力するように更に Cisco およびクライアントデバイス ベンダーを両方よりよく促進するコラボレーション プロセス可能にします、およびシームレス協同を。

IX。 Overthe エア（ OTA ）パケットキャプチャ

効果的に可能性かワイヤレス相互運用性の問題を存在 することを解決するために、問題の品質 OTA パケットキャプチャを集めることは重大です。 これは無線クライアント間の実際の 802.11 ワイヤレス通信の詳細な分析を可能にし、に加えて疑わしいアクセス ポイント無線はクライアント側および無線インフラストラクチャー ログ、デバッグ、先祖などにそれ以上の観点を与えますこれは例外なしに潜在的なワイヤレス相互運用性の問題の各テスト用の堪能の必要がある極めて重要な手順です。

ただし、頻繁にエンド カスタマをきちんと装備されていませんでしたりまたは OTA パケットキャプチャを集めるために準備されません時間を計ります。 これはいろいろな方法でこれを克服するためにワイヤレス頻繁のエンジニア フェイスが顧客と、および彼らはたらかせる必要があるよくある障害です。 Ciscoサポート フォーラムからのこの技術情報はよい開始点として顧客のそれに応じてガイドし、教育を助けるのに動作できます:

802.11 ワイヤレス/パケットキャプチャ スニッフィング

OTA パケットキャプチャが pcap ファイルフォーマット（すなわち *.pcap、*.pcapng、*.pkt、等）で集められるもち、802.11 メタデータ（すなわち RSSI、チャネル、データ レート、等を）含まれています優先する重要性を。 OTA スニファーはまたクライアントデバイスへの近似性で疑わしいテストされるクライアントデバイスに出入して送信 され、受信されるトラフィックの正確な観点を確認するためにテストの間にいつも保存するはずです。

> **注:** 疑わしいテストがクライアントデバイス ローミング シナリオを含む場合、複数の 802.11 チャネルが集約されたパケットキャプチャで監視される必要があるという。 それから現在肝蛭ネットワークからの AirMagnet WiFi アナライザを使用することを推奨しません。

この理由はこのユーティリティの使用を用いる集約されたパケットキャプチャが独自のファイルフォーマットで現在保存される、およびない Wireshark か他の同じようなユーティリティで容易に表示することができる pcap 形式形式で原因ですというファクトが。 ように OTA パケットキャプチャある非プロプライエタリ ファイルフォーマットにして下さい、これは含まれるすべてのパーティおよびベンダーが容易にするのをキャプチャ ファイルをいつも検討できる助け最終的にように解決努力の促進を助けます。

現在の Wireshark によって読解可能である、802.11 メタデータ（RSSI、チャネル、データ レート）が含まれ形式で-多くをで参照して下さい:
https://supportforums.cisco.com/document/75331/80211-wireless-sniffing-packet-capture#sthash.Xhlx5LSS.dpuf
OTA パケットキャプチャを集めるいくつかの共通のメソッドはここにあります:

- Wireshark の AirPCAP
- プロ MacBook
- OmniPeek 専門家、OmniPeek 企業、先祖など
- OmniPeek リモート アシスタント（ORA）
- スニファー モードの Cisco AP

802.11n キャプチャ

OTA パケットキャプチャに関しては 802.11n 無線クライアントを含む、現在より多くの柔軟性および使い易さがあります。 これは OmniPeek および他のようないくつかのツールによって容易に、使用できる利用可能なワイヤレス USB WLAN アダプタの多種多様が原因です。

802.11n OTA キャプチャを集めるのに使用される解決するように試みるクライアント デバイスによって使用される実際の WLAN チップセットの機能で特定のワイヤレスアダプタの機能がどのようにに関して比較するかメモを奪取 して下さい。 たとえば、クライアントデバイスが 2 空間的なストリーム（2SS）可能な 802.11n チップセットを使用する潜在的なワイヤレス相互運用性の問題に直面する場合。 それから強く推奨されています、OTA パケットキャプチャを集めるのに使用されるワイヤレスアダプタがまた 2SS またはよりよいアダプタである 802.11n かより新しい仕様とことを確認するために。

802.11ac OTA キャプチャ

3 人の空間的なストリーム（3SS） 802.11ac キャプチャの場合、またはより高く Mac OS X 10.10.x を実行する 2014 モデル MacBook プロまたはそれ以降のネイティブ スニッフィング機能を使用できます。 2 空間的なストリーム 802.11ac クライアントデバイスを解決している場合、また 802.11ac キャプチャのために MacBook 工アを使用できます。 MacBooks 使用 2SS この書

き込みの時の WLAN チップセットだけのエア モデル現在。 いろいろな方式によって Mac OS X の使用を用いる OTA パケットキャプチャを、集める方法に関する説明に関しては下記の Ciscoサポート フォーラム技術情報を参照できます:

Mac OS X 10.6+ の使用とのワイヤレス スニッフィング

またスニファー モードで 2702/2802/3702/3802 シリーズか 3SS の適切な 802.11ac パケットキャプチャを集めるのに同じような AP を使用できます。 また利用可能な 802.11ac ワイヤレスアダプタの現在の一覧のための下記のリソースを参照できます。 可能性としては OmniPeek および他のような普通 工具によって 802.11ac パケットキャプチャであるかもしれないいくつか（Ralink、Atheros、等からのすなわちチップセット）を集めるのに使用こと:

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

またスニファー モードで 2702/2802/3702/3802 シリーズか 3SS の適切な 802.11ac パケットキャプチャを集めるのに同じような AP を使用できます。 利便性の場合スニファー モードの Cisco AP を設定し OTA パケットキャプチャを集める、方法に関するステップバイステップの説明は下記の Ciscoサポート フォーラム技術情報で見つけることができます:

スニファー モードの Cisco AP

ワイヤレス クライアント デバイスでローミング シナリオを解決するために、よくあるチャレンジは効果的にマルチチャネルを渡る OTA パケットキャプチャを集めることです。 同時に複数の 802.11 チャネルを監視するこの方式は集約された OTA パケットキャプチャの収集によって実現します。 これを実現させるために互換性のあるネットワーク解析ソフトウェアと複数、互換性のある 802.11ac 可能な USB WLAN アダプタを使用するために推奨します。 一部のよくある 802.11ac 可能な USB WLAN アダプタは OmniPeek（802.11ac）、Netgear A6210 のための Savvius WiFI アダプタが、か類似した含まれています。

X. 要約

効果的に CUWN で潜在的な無線クライアント 相互運用性の問題を解決するために収集される必要がある情報の簡潔な再生タイヤはここにあります。 このセクションは必要に応じてクイックレファレンス セクションとして、動作するように意図されています。

I. 問題の定義

- 問題はアクセス ポイントや無線型（2.4 GHz vs 5 GHz）の特定のモデルに制限されますか。
- 問題はワイヤレス LAN コントローラ（WLC）ソフトウェアの特定のバージョンでだけ観察されますか。
- ありますクライアントのタイプやソフトウェア（すなわち OS バージョン、WLAN ドライババージョン、等）の特定のバージョンだけと直面する問題は
- この問題に直面しない他のどのワイヤレス デバイスもありますか。 その場合、何ですか。
- ディセーブルにされるクライアントが 20 MHz の開いた SSID、チャネル幅、および 802.11ac に接続される間、問題は再生可能ですか。（すなわち問題を起こります 11n モードで vs 11ac モードだけします）
- 問題がどんな最小セキュリティとコンフィギュレーションで開いた SSID と再生可能、問題ではない場合見られますか。（WLAN のすなわち PSK か 802.1X）
- 前の運用コンフィギュレーションおよびソフトウェア バージョンとは何か。

II. WLC 設定およびログ

疑わしい WLC の CLI からこれを集めて下さい:

- 構成ページング ディセーブル
- show run-config

また、また必要に応じて出力されるちょうどこれらを集めることができます:

- 構成ページング ディセーブル
- 実行構成非 ap を示して下さい
- show wlan apgroups

TFTP、FTP、等 (GUI による WLC 設定のバックアップ: **コマンド > アップロード ファイル > 設定**)

WLC からの Syslogs

III.クライアントデバイス情報

- クライアントのタイプ (すなわちタブレット、smartphone、ノート PC、等)
- デバイスは作り、模倣します
- OS バージョン
- WLAN アダプタ モデル
- WLAN アダプタ ドライババージョン
- 使用される要求元 (すなわち Windows ゼロ構成/自動設定、Intel PROSet、等)
- 無線クライアントによって使用のために設定されるセキュリティおよび WLAN (すなわち、PSK、EAP-PEAP/MSCHAPv2、等開いて下さい)

  注: 疑わしいベンダーが提供するデフォルト設定から変更されるクライアント パラメータ。(すなわちスリープ状態、ローミング パラメータ、U-APSD、等)

IV.ネットワーク トポロジ ダイアグラム

これはネットワーク (すなわちプリンタ/スキャナー、WLCs、等) にワイヤレス デバイスに関して表示や詳細を含める必要があります

V. すべてのクライアント問題を記録するためにスプレッドシートを作成して下さい

例：

MAC アドレス	username	表示された現象の説明	時間	エンドユーザによって観察される現象	Ping デフォルト ゲートウェイ Y/N	WiF ます

この演習の目標は一般的なパターンを識別し、手もと問題の正確な情報の展示を助けることです。

VI. WLC の Show および debug コマンド

CLI によってこれらの WLC デバッグを収集して下さい:

- **構成セッション タイムアウト 0**
- **デバッグ クライアント <MAC_address>**
- debug dhcp message enable

基礎に追加デバッグを場合次第で追加して下さい:

- **AAA 詳細 イネーブルをデバッグして下さい**- AAAサーバにおいての認証 関連 問題がある場合これを使用して下さい
- **AAA イベント イネーブルをデバッグして下さい**- AAAサーバにおいての認証 関連 問題がある場合これを使用して下さい
- debug aaa all enable - auth 問題のためにこれを使用して下さい; これは冗長です従ってだけ必要な場合だけそれを使用して下さい（すなわち AAA 上書きするのために等を包装します）
- **デバッグ モビリティ ハンドオフ**- WLCs 間の問題をローミングした場合使用して下さい

CLI によって WLC show コマンドのための出力を集めて下さい:

- **構成ページング ディセーブル**
- show time
- **client> のクライアント 詳細 <mac アドレスを示して下さい**（WLC のクライアント ステートに注意して下さい）
- WLC からクライアントを ping して下さい

テストが完了した、WLC のすべての現在のデバッグを停止するこのコマンドを使用して下さい:

- **ディセーブルすべてをデバッグして下さい**

VII. AP の Show および debug コマンド

軽量 Cisco IOS APS

このセクションが 1700/2700/3700 シリーズか前モデル アクセス ポイントに必要なデバッグを詳述します。

AP セッション タイムアウトを Telnet/SSH/console セッションの時に避けるために、これらのコマンドを使用して下さい:

- **capwap コンソール cli をデバッグして下さい**
- config t
- **行コンソール 0** -- シリアル セッション タイムアウト パラメータを修正するのに使用して下さい
- line vty 0 4 -- Telnet/SSH セッション タイムアウト パラメータを修正するのに使用して下さい
- exec-timeout 0
- **セッション タイムアウト 0**
- **条件は 0 を len**

テストを開始する前に、AP のこれらの show コマンドのサンプルを収集して下さい。 少くとも CLI によってこれらの AP show コマンドの使用を用いるテストの完了の前後にこの出力の 2 つのサンプルを、両方集めて下さい:

- 条件は 0 を len
- show clock
- show tech
- show capwap client mn
- int do1 dfs を示して下さい
- show logging
- より多くの event.log
- トレース dot11_rst ディスプレイ時刻形式ローカルを示して下さい
- トレース dot11_rst を示して下さい
- トレース dot11_bcn ディスプレイ時刻形式ローカルを示して下さい
- トレース dot11_bcn を示して下さい

CLI によってこれらの AP デバッグを収集して下さい:

- dot11 {d0 をデバッグして下さい | d1}モニタ アドレス <MAC_address>
- デバッグ dot11 {d0 | d1}トレース プリント クライアント mgmt は rxev txev rcv xmt txfail Ba をキー入力します
- term mon

テストが完了した、デバッグを無効に するこのコマンドを使用して下さい:

- u すべて

AP-COS APS

このセクションが 1800/2800/3800 シリーズ APS に必要なデバッグを詳述します。

AP セッション タイムアウトを Telnet/SSH/console セッションの時に避けるために、これらのコマンドを使用して下さい:

- exec-timeout 0

テストを開始する前に、AP の下記の show コマンドのサンプルを収集して下さい。 少くとも CLI によってこれらの AP show コマンドの使用を用いるテストの完了の前後にこの出力の 2 つのサンプルを、両方集めて下さい:

- 条件は 0 を len
- show clock
- show tech
- クライアント統計 <client_MAC-address> を示して下さい
- cont nss ステータスを表示して下さい
- cont nss 統計を示して下さい
- show log

1800 シリーズ アクセス ポイントに関しては、CLI によってこれらの AP デバッグを収集して下さい:

- dot11 クライアント レベル イベント アドレス <client_MAC-address> をデバッグして下さい
- dot11 クライアント レベル エラー アドレス <client_MAC-address> をデバッグして下さい
- dot11 クライアント レベル重要なアドレス <client_MAC-address> をデバッグして下さい
- dot11 クライアント レベル ヒント アドレス <client_MAC-address> をデバッグして下さい
- dot11 クライアント datapath eapol アドレス <client_MAC-address> をデバッグして下さい

- **dot11 クライアント datapath dhcp アドレス <client_MAC-address> をデバッグして下さい**
- **dot11 クライアント datapath arp アドレス <client_MAC-address> をデバッグして下さい**
- **term mon**

2800/3800 シリーズ アクセス ポイントに関しては、CLI によってこれらの AP デバッグを収集して下さい:

- **構成 ap クライアント トレース アドレスは <client_MAC-address> を追加します**
- **構成 ap クライアント トレース フィルタはすべて有効に なります**
- **構成 ap クライアント トレース出力 console log イネーブル**
- **構成 ap クライアント トレース開始**
- **term mon**

テストが完了した、デバッグを無効に するこのコマンドを使用して下さい:

- **構成 ap クライアント トレース停止**

VIII.クライアント側キャプチャ

クライアントデバイスの WLAN アダプタから Netmon 3.4 （Windows XP か 7 のみ）または Wireshark プロミスキャス パケットキャプチャを集めて下さい。

IX. OTA キャプチャ

802.11n キャプチャ

- Wireshark の AirPCAP
- プロ MacBook
- OmniPeek 専門家、企業、先祖など
- OmniPeek リモート アシスタント（ORA）
- スニファー モードの Cisco AP

802.11ac キャプチャ

- 11ac 3SS キャプチャの場合、それが 2SS 現在デバイスだけであるので）またはより高く 10.10.x を実行する 2014 Macbook プロまたはそれ以降を使用できます（11ac もし可能なら のために MacBook エアをキャプチャ します使用しないで下さい。
- またスニファー モードで 2702、3702 または同じような Cisco AP を使用できます。
- を用いるローミング シナリオに関してはおよび Savvius からの OmniPeek のような専門ネットワーク解析ソフトウェアの使用。 OmniPeek （802.11ac）、Netgear A6210 のために Savvius WiFI アダプタのような複数、互換性のある 802.11ac 可能な USB WLAN アダプタを、か類似した使用するために推奨します。

XI. 付録 A -追加助言およびトリック

Windows

その他の情報および Windows PC から他の関連詳細を直接現在の無線接続に関して集めるため。 Windows コマンド・ライン（CMD）のこれらの netsh wlan 関連のコマンドを利用できます:

```
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
```

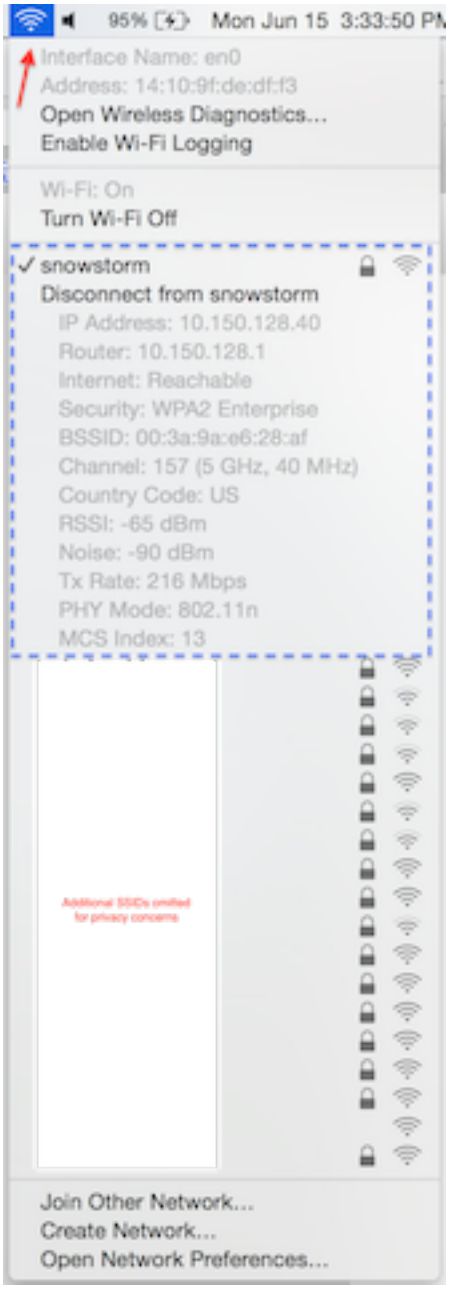
```
Interface name : Wireless Network Connection
There are 21 networks currently visible.

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（以前の X）OS

同等の出力を Windows PC の **ipconfig /all** コマンドとして集めるために、Apple MacBook のネットワーク インターフェイスすべてのための詳細な情報をリストする代りに **ifconfig** のよくある Linux/Unix コマンドを使用できます。 ある特定の MacBook のちょうどネイティブ ワイヤレス インターフェイスのための出力が表示されるために必要に応じて、また規定できます（en0 か en1、モデルによって決まります）。 この例のような:

```
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
```

速いしかし詳細な情報を MacBook の現在の無線接続に関して得るため。 イメージに示すように同時にキーボードの **Option ボタンを**保持する間、またデスクトップの右上隅の WiFi アイコンを選択できます。



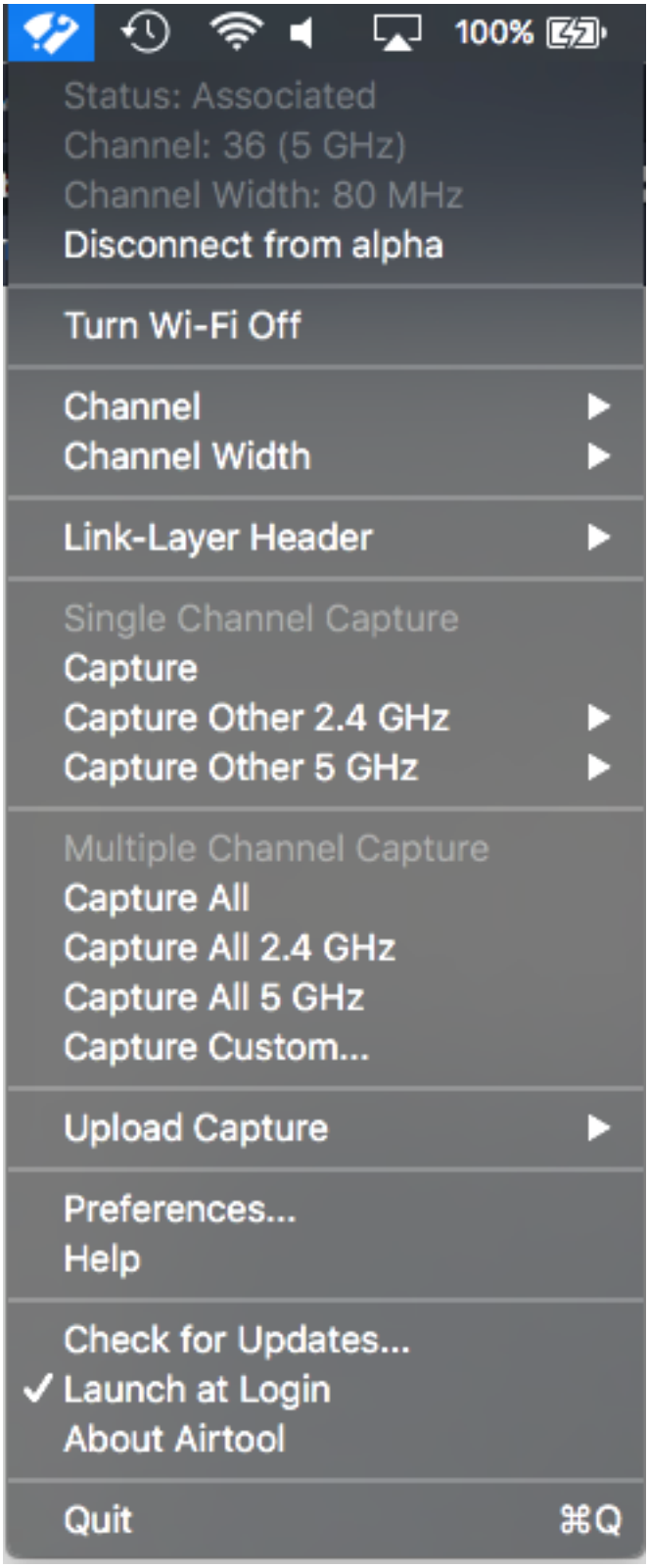
もう一つの有用なオプションは非表示コマンド・ライン ユーティリティによって呼出される空港を利用することです。 それは強く推奨されていますラボ 環境で使用中のあなた自身の MacBook か 1 とこれを利用するためにただ。 いくつかのネットワーク管理者がエンドユーザの MacBook のこのユーティリティへの対するアクセス権の付与に希望しないかもしれませんでしたり従ってので注意の適切なレベルをそれに応じて使用して下さい。 続行するために、疑わしい MacBook のターミナルでこれを入力して下さい:

```
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
```

この場合空港 CLI ユーティリティを容易に頼むことができます。 これが含まれている例:

```
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
```

プロか類似した MacBook の機能の使用を用いる信頼できる、単一 802.11 チャネル OTA パケットキャプチャを集めるために更にプロセスを楽にするため。 以前に説明されている通りワイヤレス診断 > スニファー方式または類似したの使用を用いる macOS の embeded 機能にてこ入れできますオプションで Airtool と同様に呼ばれるサード・パーティ ユーティリティを使用できます（OS X 10.8 およびそれ以降）。 利点はすぐに画面の上メニューバーからのアプリケーション UI 権限によってちょうど少数のクリックのデスクトップに直接保存される OTA パケットキャプチャを集める単一のインターフェイスです。



Airtool へのより詳しい 情報およびダウンロード リンクはこの URL で見つけることができます:

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