Cisco Wireless LAN Controller（WLC）の設定に関するベスト プラクティス

最終更新日：2017 年 8 月
リリース：Cisco Wireless LAN Controller（WLC）の設定に関するベスト プラクティス（リリース 8.1）

概要

モビリティによって、ワイヤレス ネットワーク リソースへの期待や、ユーザによる認識が急速に変化してきました。ワイヤレスはユーザがネットワークにアクセスする場合の推奨オプションとなっており、多くの場面では唯一実用的なオプションでもあります。このドキュメントでは、一般的なワイヤレス LAN コントローラ（WLC）インフラストラクチャに共通するベスト プラクティスに関して、設定のヒントを紹介します。ここでは、大部分のワイヤレス ネットワークの実装に適用できる重要な注意事項も含んでいます。

注：ネットワークはすべて同じではありません。したがって、ヒントの一部は設置時に適用できない場合があります。稼働中のネットワークに変更を加える前に必ず確認してください。

前提条件

要件

次の項目に関する知識が推奨されます。

- ワイヤレス LAN コントローラ（WLC）と Lightweight アクセス ポイント（LAP）の基本動作の設定方法に関する知識
- Control And Provisioning of Wireless Access points（CAPWAP）プロトコルとワイヤレス セキュリティ方式に関する基礎知識

使用されるコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- ソフトウェア リリース 8.1 以降が動作する Cisco WLC
- Cisco 802.11n および 11ac シリーズ AP

注：WLC に関する事項はすべてソフトウェア リリース 8.1 以降に基づいています。

注：このドキュメントの情報は、特定のラボ環境に置かれたデバイスに基づいて作成されました。このドキュメントで使用されるデバイスはすべて、初期設定（デフォルト）の状態から作業が開始されています。ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

Cisco WLC 設定に関するベスト プラクティス

ネットワーク設計

次のセクションでは、ネットワーク設計のベスト プラクティスを列挙します。

AP 接続スイッチ ポートでの PortFast の使用

ローカル モードの AP については、PortFast を使用してスイッチ ポートを設定します。PortFast を設定するには、ポートを「ホスト」ポートとして接続するように設定するか（switchport host コマンド）、または直接 portfast コマンドを使用します。これにより、AP の参加プロセスが高速になります。CAPWAP AP は VLAN 間をブリッジしないため、ループが発生するリスクはありません。

注：ローカル モードの AP については、ラウンドトリップ遅延がアクセス ポイントとコントローラ間で 20 ミリ秒（ms）を超えないようにします。

インターフェイス ソース（DHCP、SNMP、RADIUS、Multicast など）

CPU 起点のトラフィック（SNMP トラップ、RADIUS 認証要求、マルチキャスト転送など）の多くは、設計上の理由から、コントローラの管理アドレスから送信されます。

- このルールのデフォルトの例外は DHCP 関連トラフィックです。各 SSID で [radius interface overwrite] を有効にすると、この WLAN の RADIUS パケットがダイナミック インターフェイスから送信されます。ただ、これにより Bring Your Own Device（BYOD）フローと認可変更（CoA）に問題が発生します。
- 各 SSID で [radius interface overwrite] を有効にすることは、ファイアウォール ポリシーの設定やネットワーク トポロジを設計するときに重要です。非対称ルーティング問題が発生する可能性があるため、コントローラから到達可能なサーバ（例えば RADIUS サーバなど）として同じサブネットワークでダイナミック インターフェイスの設定を避ける必要があります。
- RADIUS は RADIUS オーバーライド機能を使用して、ダイナミック インターフェイスをソースにできます。特定のトポロジで必要な場合のみ使用してください。

推奨スイッチポート モードと VLAN プルーニング

ローカル モードの AP については、スイッチポートを必ず「アクセス モード」に設定してください。FlexConnect モードの AP（ローカル スイッチングを実行）、および WLC に接続されるトランク モードのスイッチポートについては、必ず VLAN をプルーニングして、FlexConnect AP および WLC に設定された VLAN のみを許可します。また、これらのトランクに **switchport nonegotiate** コマンドを入力して、スイッチポートでダイナミック トランキング プロトコル（DTP）を無効化することでフレーム処理（AP/WLC では DTP をサポートしないため不要）を回避できます。DTP をサポートできないデバイスとネゴシエートを試行するスイッチでもリソースが無駄になる場合があります。

ネットワーク接続

次の設定を変更した場合、コントローラをリロードすることを推奨します。

- 管理アドレス
- SNMP 設定
- HTTPS 暗号化設定
- LAG モード（有効/無効）

管理インターフェイスへの VLAN タギングの使用

HA シナリオで唯一サポートされているモードであるため、シスコでは WLC の管理インターフェイスに VLAN タギングを使用することを推奨します。タグ付けされていないインターフェイスでは、管理インターフェイスで送受信されるパケットは、WLC の接続先トランク ポートのネイティブ VLAN と見なされます。しかしながら、管理インターフェイスに別の VLAN を割り当てる場合は、次のコマンドを使用して適切な VLAN にタグ付けします。

(Cisco Controller) >config interface vlan management <vlan-id>

対応する VLAN がスイッチポートで許可され、トランク（ネイティブ以外の VLAN）によってタグ付けされていることを次のように確認します。

- コントローラに接続されているすべてのトランク ポートについては、使用されていない VLAN をフィルタします。

  たとえば Cisco IOS スイッチで、管理インターフェイスが VLAN 20 にあり、VLAN 40 と VLAN 50 は 2 つの WLAN にそれぞれ使用されている場合、次の設定コマンドをスイッチ側で使用します。

  Switch# switchport trunk allowed vlans 20,40,50

  - インターフェイスを 0.0.0.0 アドレス（未設定のサービス ポートなど）のままにすることはできません。コントローラの DHCP 処理に影響を与える場合があります。

  確認するには次のコマンドを実行します。

```
(Cisco Controller) >show interface summary
Interface Name        Port  Vlan Id   IP Address       Type     Ap Mgr
--------------------  ----  --------  ---------------  -------  ------
ap-manager            LAG   15        192.168.15.66    Static   Yes
example               LAG   30        0.0.0.0          Dynamic  No
management            LAG   15        192.168.15.65    Static   No
service-port          N/A   N/A       10.48.76.65      Static   No
```

  - コントローラのすべてのポートに対して、接続しているスイッチ側に同じレイヤ 2 設定がない場合、リンク アグリゲーション（LAG）は使用できません。たとえば、あるポートで VLAN をフィルタし、それ以外のポートではフィルタしない、ということは避ける必要があります。

  - LAG を使用するときは、トラフィックは同じデータ プレーンに到達する必要があります。ネットワークから着信するトラフィックに関するロード バランシングの決定については、コントローラはスイッチに依存します。コントローラでは、AP に属するトラフィックは常に同じデータ プレーンに入ると想定されます。5500 コントローラは、トラフィックが常に同じデータ プレーンに到達する単一データ プレーンの例です。

  - WISM2 と 8500 は、2 つのデータ プレーンがある WLC です。可能な限り、トラフィックは同じデータ プレーンに到達する必要があります。通常、データ プレーン間でフレームを移動するための帯域幅は十分にあります。しかしながら、帯域幅が制限されている場合、トラフィックはドロップされる場合があります。

  EtherChannel ロード バランシング メカニズムを確認するには、次のコマンドを実行します。

  Switch#show etherchannel load-balance

```
EtherChannel Load-Balancing Configuration:
src-dst-ip
EtherChannel Load-Balancing Addresses Used Per-Protocol:
Non-IP: Source XOR Destination MAC address
IPv4: Source XOR Destination IP address
IPv6: Source XOR Destination IP address
```

  スイッチの設定（IOS）を変更するには、次のコマンドを実行します。

  Switch(config)#port-channel load-balance src-dst-ip

Cisco IOS ソフトウェア リリース 12.2(33)SXH6 以降には、負荷分散で VLAN を除外する PFC3C モード シャーシのオプションがあります。**port-channel load-balance src-dst-ip exclude vlan** コマンドを使用して、この機能を有効にします。この機能を使用すると、LAP に属するトラフィックは同じポートに入ります。

- LAG は VSS、スタック スイッチ（3750/2960）、または Nexus VPC を使用していて、IP パケットのフラグメントが同じポートに送信される限り、動作する必要があります。つまり、複数のスイッチを使用する場合、ロード バランシングの決定に関して、ポートは同じ L2「エンティティ」に属する必要があるということです。
- WLC を複数のスイッチに接続するには、各物理ポートに AP マネージャを作成して、LAG を無効にする必要があります。これにより、冗長性と拡張性を実現します。
- 古いソフトウェア バージョンで許可されていても、AP 管理インターフェイスにバックアップ ポートを作成することはできません。冗長性は、このドキュメントで既述のとおり、複数の AP 管理インターフェイスによって実現されます。

マルチキャスト転送モードの使用

より少ない帯域幅の使用率でパフォーマンスを最大化するにはマルチキャスト フォワーディング モードを使用します。多数の IPv6 クライアント、ビデオストリームや mDNS プロキシを使用しない Bonjour のような負荷の大きいマルチキャスト アプリケーションが使用されるネットワークでは、マルチキャスト モードにすることで大幅な改善が見込めます。

コントローラでマルチキャスト モードを確認するには、次のコマンドを実行します。

(Cisco Controller) >show network summary

```
RF-Network Name.............................rfdemo
Web Mode....................................Enable
Secure Web Mode.............................Enable
Secure Web Mode Cipher-Option High..........Disable
Secure Web Mode Cipher-Option SSLv2.........Disable
Secure Web Mode RC4 Cipher Preference.......Disable
OCSP........................................Disabled
OCSP responder URL..........................
Secure Shell (ssh)..........................Enable
Telnet......................................Enable
Ethernet Multicast Forwarding...............Enable
Ethernet Broadcast Forwarding...............Enable
```

IPv4 AP Multicast/Broadcast Mode.....Multicast Address : 239.0.1.1

```
IGMP snooping...............................Enabled
IGMP timeout................................60 seconds
IGMP Query Interval.........................20 seconds
MLD snooping................................Enabled
```

WLC コマンド ラインで multicast-multicast 動作を設定するには、次のコマンドを実行します。

(Cisco Controller) >config network multicast mode multicast 239.0.1.1

(Cisco Controller) >config network multicast global enable

- マルチキャスト アドレスはコントローラによって使用され、トラフィックをアクセス ポイント（AP）に転送します。マルチキャスト アドレスについて、他のプロトコルがネットワーク上で使用中の別のアドレスに一致しないことを確認します。たとえば、224.0.0.251 を使用する場合、いくつかのサード パーティ製のアプリケーションが使用する mDNS と競合します。コントローラが使用するマルチキャスト アドレスについては、プライベート アドレスの範囲（239.0.0.x と 239.128.0.x を除外した 239.0.0.0 ～ 239.255.255.255）にすることを推奨しています。また、マルチキャスト IP アドレスが 各々の WLC で別々の値に設定されていることを確認します。他の WLC の AP とマルチキャスト通信する WLC は必要ありません。
- AP が管理インターフェイスで使用されるサブネットと別のサブネット上にあり、AP マルチキャスト モードが有効な場合、ネットワーク インフラストラクチャで管理インターフェイス サブネットと AP サブネット間のマルチキャスト ルーティングを使用できる必要があります。

内部 DHCP の無効化

コントローラには、内部 DHCP サーバを提供する機能があります。この機能は非常に限定的で、たとえばラボ環境などでの簡単なデモや POC 検証のために使用されるのが大半です。企業の実稼動ネットワークではこの機能を使用しないことを推奨します。

show interface detailed management コマンドを使用して、内部 DHCP サーバが使用されているかどうかを確認します。プライマリ DHCP サーバ アドレスは、管理 IP アドレスと同じです。次の例を参照してください。

(Cisco Controller) >show interface detailed management

```
Interface Name.............................. management
MAC Address................................. e0:2f:6d:5c:f0:40
IP Address.................................. 10.10.10.2
IP Netmask.................................. 255.255.255.0
IP Gateway.................................. 10.10.10.1
External NAT IP State....................... Disabled
External NAT IP Address..................... 0.0.0.0
Link Local IPv6 Address..................... fe80::e22f:6dff:fe5c:f040/64
STATE ...................................... NONE
Primary IPv6 Address........................ ::/128
STATE ...................................... NONE
Primary IPv6 Gateway........................ ::
Secondary IPv6 Address...................... ::/128
STATE ...................................... NONE
Secondary IPv6 Gateway...................... ::
VLAN........................................ 10
Quarantine-vlan............................. 0
Active Physical Port........................ 1
Primary Physical Port....................... 1
Backup Physical Port........................ Unconfigured
DHCP Proxy Mode............................. Global
Primary DHCP Server......................... 10.10.10.2
```

内部 DHCP サーバ（管理 IP アドレス）を実稼働 DHCP サーバに変更するには、次のコマンドを実行します。

(Cisco Controller) >config interface dhcp management primary <primary-server>

既存の内部 DHCP スコープを無効化またはクリーンアップすることを推奨します。

(Cisco Controller) >show dhcp summary

```
Scope Name                    Enabled          Address Range
Scope1                         Yes           10.10.10.100 -> 10.10.10.150
```

DHCP スコープを無効にするには、次のコマンドを実行します。

(Cisco Controller) >config dhcp delete-scope <scope name>

または

(Cisco Controller) >config dhcp disable <scope name>

高速再起動

次のようなシナリオのためにネットワークとサービスのダウンタイムを短縮し、有用性を向上させるには、**reset system** の代わりに **restart** を使用することを推奨します。

- LAG モードの変更
- モビリティ モードの変更
- Web 認証証明書のインストール
- 設定のクリア

高速再起動機能は、Cisco WLC 7510、8510、5520、8540、および vWLC リリース 8.1 以降でサポートされています。

コントローラを再起動するには、次のコマンドを実行します。

(Cisco Controller) >restart

```
The system has unsaved changes.
Would you like to save them now? (y/N) y

Updating HBL license statistics file
Done.

Configuration Saved!
System will now restart!
Updating license storage ...  Done.
```

セキュリティ

次のセクションでは、セキュリティのベスト プラクティスを列挙します。

AP の 802.1X 認証

セキュリティを強化するためには、lightweight アクセス ポイント（AP）とシスコ スイッチの間の 802.1X 認証を設定します。AP は 802.1X サプリカントとして動作し、EAP-FAST と匿名 PAC プロビジョニングを使用してスイッチにより認証されます。これはグローバル認証設定で設定できます。

現在コントローラに参加しているすべての AP と今後コントローラに参加する AP のグローバル認証ユーザ名とパスワードを設定するには、次のコマンドを実行します。

(Cisco Controller) >config ap 802.1Xuser add username <ap-username> password <ap-password> all

設定を確認するには、次のコマンドを実行します。

(Cisco Controller) >show ap summary

```
Number of APs.................................... 1
Global AP User Name.............................. globalap
Global AP Dot1x User Name........................ globalDot1x
```

スイッチの認証の設定

下記はスイッチ ポートで 802.1X 認証を有効にする設定例です。

Switch# configure terminal

Switch(config)# dot1x system-auth-control

Switch(config)# aaa new-model

Switch(config)# aaa authentication dot1x default group radius

Switch(config)# radius-server host <ip_addr> auth-port <port> acct-port <port> key <key>

Switch(config)# interface gigabitethernet2/1

Switch(config-if)# switchport mode access

Switch(config-if)# dot1x pae authenticator

Switch(config-if)# dot1x port-control auto

Switch(config-if)# end

ワイヤレス経由での管理（Management over Wireless）アクセス機能の無効化

Cisco WLAN ソリューションの Management over Wireless（ワイヤレス経由での WLC の管理）機能では、Cisco WLAN ソリューション オペレータがワイヤレス クライアントを使用して WLC を監視・設定できます。セキュリティ上の理由のため、Management over Wireless（ワイヤレス経由での WLC の管理）機能を無効にしてください。

Management over Wireless（ワイヤレス経由での WLC の管理）機能を確認するには、次のコマンドを実行します。

(Cisco Controller) >show network summary

```
RF-Network Name.............................default
Web Mode....................................Enable
Secure Web Mode.............................Enable
Secure Web Mode Cipher-Option High..........Disable
Secure Web Mode Cipher-Option SSLv2.........Disable
Secure Web Mode RC4 Cipher Preference.......Disable
…
Mgmt Via Wireless Interface.................Enable
```

Management over Wireless（ワイヤレス経由での WLC の管理）機能を無効にするには、次のコマンドを実行します。

(Cisco Controller) > config network mgmt-via-wireless disable

セキュア Web アクセスの有効化

セキュリティ強化のため、管理アクセスについて HTTPS を有効にして HTTP を無効にします。

ネットワーク サマリーを表示するには、次のコマンドを実行します。

(Cisco Controller) >show network summary

```
RF-Network Name.............................default
Web Mode....................................Enable
Secure Web Mode.............................Enable
Secure Web Mode Cipher-Option High..........Disable
Secure Web Mode Cipher-Option SSLv2.........Disable
```

Web モードを無効にするには、次のコマンドを実行します。

(Cisco Controller) >config network webmode disable

このコマンドにより、「http://ip-address」を使用してコントローラ GUI にアクセスするユーザを拒否します。

セキュア Web モードを有効にするには、次のコマンドを実行します。

(Cisco Controller) >config network secureweb enable

このコマンドにより、「https://ip-address」を使用して、コントローラ GUI へのセキュアなアクセスができるようになります。

セキュア SSH/Telnet

セキュア Web アクセスと同様に、コントローラへの SSH を有効にし Telnet を無効にして、セキュリティを強化します。

ネットワーク サマリーを表示するには、次のコマンドを実行します。

(Cisco Controller) > show network summary

```
Web Mode.....................................Enable
Secure Web Mode..............................Enable
Secure Web Mode Cipher-Option High.....Enable
Secure Web Mode Cipher-Option SSLv2.....Enable
Secure Shell (ssh).....................Enable
Telnet.....................................Enable
```

Telnet を無効にするには、次のコマンドを実行します。

(Cisco Controller) > config network telnet disable

SSH を有効にするには、次のコマンドを実行します。

(Cisco Controller) >config network ssh enable

ローカル管理パスワード ポリシー

強力なパスワードを使用する必要があります。パスワード ポリシーを使用すると、コントローラおよびアクセス ポイントの追加の管理ユーザ用に新しく作成されたパスワードに対して、強力なパスワード チェックを実行できます。新規パスワードには次の要件が適用されます。

- コントローラが旧バージョンからアップグレードされた場合、たとえパスワード強度が低下するとしても、古いパスワードはすべて維持されます。システムのアップグレード後、強力なパスワード チェックが有効になると、それ以降は強力なパスワード チェックが適用され、以前に追加されたパスワードの強度のチェックまたは変更は行われません。
- [Password Policy] ページで設定された内容によっては、ローカル管理ユーザおよびアクセス ポイント ユーザの設定が影響を受けます。

強力なパスワード チェックを確認するには、次のコマンドを実行します。

(Cisco Controller) >show switchconfig

```
….
Strong Password Check Features
   case-check.....................................Enabled
   consecutive-check..............................Enabled
   default-check..................................Enabled
   username-check.................................Enabled
   position-check.................................Disabled
   case-digit-check...............................Disabled
   Min. Password length..........................3
```

```
Min. Upper case chars.....................0
Min. Lower case chars.....................0
Min. Digits chars.........................0
Min. Special chars........................0
```

AP と WLC への強力なパスワード チェックを有効にするには、次のコマンドを実行します。

(Cisco Controller) >config switchconfig strong-pwd {case-check | consecutive-check | default-check | username-check | all-check} {enable | disable}

コマンドの設定値は次のとおりです。

- **case-check**：3 回連続の同じ文字の使用を確認します。
- **consecutive-check**：デフォルト値またはその変種の使用を確認します。
- **default-check**：ユーザ名またはそれを逆にした文字の使用を確認します。
- **all-checks**：強力なパスワード チェックをすべて有効または無効にします。

ユーザ ログイン ポリシー

ユーザ ログイン ポリシーは、コントローラのローカル ネットユーザの同時ログイン数を制限するために指定します。同時ログイン数を制限できるため、デフォルトの 0（ログインは無制限）より大きな値の設定を推奨します。

ネットユーザ数の制限を確認するには、次のコマンドを実行します。

(Cisco Controller) >show netuser summary

```
Maximum logins allowed for a given user name.....Unlimited
```

ユーザ ログイン ポリシーを設定するには、次のコマンドを実行します。

(Cisco Controller) >config netuser maxuserlogin 5

Aironet IE の無効化

Aironet IE とは、接続性の向上のためにシスコのデバイスで使用されるシスコ独自の属性です。Aironet IE には、アクセス ポイント（AP）から送信される、WLAN のビーコンやプローブ応答の情報（アクセス ポイント名、負荷、接続クライアント数など）が含まれます。Cisco Client Extensions（CCX）クライアントは、この情報を使用してアソシエートに最適な AP を選択します。

CCX ソフトウェアは、CCX 対応クライアント デバイスの製造業者およびベンダーに対してライセンスされます。これらのクライアント上にある CCX コードにより、サードパーティ製クライアント デバイスは、シスコ製の AP と無線で通信できるようになり、他のクライアント デバイスでサポートしていないシスコの機能もサポートできるようになります。これらの機能は、セキュリティの強化、パフォーマンスの向上、高速ローミング、および電源管理に関連しています。

Aironet IE は CCX ベースのクライアントではオプションです。しかしながら、一部のタイプのワイヤレス クライアントでは互換性問題が発生する場合があります。WGB および Cisco Voice では Aironet IE の有効化を推奨します。しかしながら、一般的な実稼働ネットワークについては、テスト後に無効化することを推奨します。

特定の WLAN で Aironet IE を無効にするには、次のコマンドを実行します。

(Cisco Controller) >config wlan ccx aironet-ie disable <wlan_id>Forwarding

Client Exclusion（クライアントの除外）

ユーザが認証に失敗すると、コントローラによってそのクライアントが除外されます。除外されたクライアントは、除外タイマーが期限切れになるか、または管理者によって除外タイマーが手動で上書きされるまで、ネットワークに接続できません。

Client Exclusion（クライアントの除外）では、単一のデバイスによる認証の試行が検出されます。デバイスが最大数を超えて失敗すると、その端末の MAC アドレスによるアソシエートはそれ以上許可されなくなります。

Cisco WLC は、次の条件が満たされたときにクライアントを除外します。

- 5 回連続で失敗して 802.11 アソシエーション失敗数を超える
- 5 回連続で失敗して 802.11 認証失敗数を超える
- 3 回連続で失敗して 802.1X 認証失敗数を超える
- IP 盗難または IP 再利用（クライアントが取得した IP アドレスがすでに別のデバイスに割り当てられている場合）
- 3 回連続で失敗して Web 認証失敗数を超える

クライアントの除外期間のタイマーを設定でき、Client Exclusion（クライアントの除外）はコントローラまたは WLAN レベルで有効化または無効化できます。

除外ポリシーを確認するには、次のコマンドを実行します。

（Cisco Controller）>show wps summary

```
Auto-Immune
  Auto-Immune.....................................Disabled
  Auto-Immune by aWIPS Prevention.................Disabled
Client Exclusion Policy
  Excessive 802.11-association failures..........Enabled
  Excessive 802.11-authentication failures.......Enabled
  Excessive 802.1x-authentication................Enabled
  IP-theft.......................................Enabled
  Excessive Web authentication failure...........Enabled
  Maximum 802.1x-AAA failure attempts............3
```

5 回連続で失敗して、6 回目の 802.11 アソシエーションの試行でクライアントを除外するようにコントローラを設定するには、次のコマンドを実行します。

(Cisco Controller) >config wps client-exclusion 802.11-assoc enable

5 回連続で失敗して、6 回目の 802.11 認証の試行でクライアントを除外するようにコントローラを設定するには、次のコマンドを実行します。

(Cisco Controller) >config wps client-exclusion 802.11-auth enable

3 回連続で失敗して、4 回目の 802.1X 認証の試行でクライアントを除外するようにコントローラを設定にするには、次のコマンドを実行します。

(Cisco Controller) >config wps client-exclusion 802.1x-auth enable

IP アドレスがすでに別のデバイスに割り当てられている場合、クライアントを除外するようにコントローラを設定するには、次のコマンドを実行します。

(Cisco Controller) >config wps client-exclusion ip-theft enable

3 回連続で失敗して、4 回目の Web 認証の試行でクライアントを除外するようにコントローラを設定するには、次のコマンドを実行します。

(Cisco Controller) >config wps client-exclusion web-auth enable

上記すべての場合に、クライアントを除外するようにコントローラを設定するには、次のコマンドを実行します。

(Cisco Controller) >config wps client-exclusion all enable

ピアツーピア ブロッキング

ピアツーピア ブロッキングは個別の WLAN に対して適用され、各クライアントが、アソシエート先の WLAN のピアツーピア ブロッキング設定を継承します。ピアツーピア ブロッキングにより、トラフィックを向かわせる方法を制御できます。たとえば、トラフィックがコントローラ内でローカルにブリッジされたり、コントローラによってドロップされたり、またはアップストリーム VLAN へ転送されるように選択することができます。

ローカル スイッチングの WLAN にアソシエートしたクライアントに対して、ピアツーピアブロッキングはサポートされています。コントローラはローカル クライアント トラフィックのブリッジを行わないようにします。したがって、セキュリティの強化のためにはピアツーピア ブロッキングの有効化を推奨します。

WLAN のピアツーピア ブロッキング設定を確認するには、次のコマンドを実行します。

(Cisco Controller) >show wlan <wlan_id>

```
WLAN Identifier.................................1
Profile Name....................................test
Network Name (SSID).............................test
Status..........................................Enabled
...
...
...
Peer-to-Peer Blocking Action.....................Disabled
Radio Policy....................................All
```

WLAN のピアツーピア ブロッキングを設定するには、次のコマンドを実行します。

(Cisco Controller) >config wlan peer-blocking { disable | drop | forward-upstream} <wlan_id>

ローカル EAP の無効化

ローカル EAP は、ユーザおよびワイヤレス クライアントのローカル認証をコントローラで可能にする認証方式です。エンタープライズ実稼働環境でローカル EAP を使用することは推奨しません。ローカル EAP の無効化または使用しないことを推奨します。

WLAN がローカル EAP を使用するように設定されているかどうかを確認するには、次のコマンドを実行します。

(Cisco Controller) >show wlan <WLAN id>

```
Radius Servers
Authentication..............................Global Servers
Accounting..................................Global Servers
Interim Update..............................Disabled
Framed IPv6 Acct AVP .......................Prefix
Dynamic Interface...........................Disabled
Dynamic Interface Priority..................wlan
Local EAP Authentication.....................Disabled
Radius NAI-Realm............................Disabled
```

WLAN でローカル認証を無効にするには、次のコマンドを実行します。

(Cisco Controller) >config wlan local-authen disable <WLAN id>

WPA2 + 802.1X WLAN

コントローラおよび AP は Wi-Fi Protected Access（WPA）と WPA2 を同時に使用した SSID で WLAN をサポートしますが、一部のワイヤレス クライアント ドライバではWPAと WPA2 を同時に使用した SSID の設定に対応できないのが一般的です。シスコは、Advanced Encryption Standard（AES）のみを設定した WPA2 の使用を推奨します。しかしながら、IEEE 規格および必須の Wi-Fi Alliance 認定プロセスがあるため、TKIP サポートは今後のソフトウェア バージョンでも必須です。すべての SSID でセキュリティ ポリシーを簡潔にしてください。WPA と Temporal Key Integrity Protocol（TKIP）を設定した WLAN/SSID と WPA2 と Advanced Encryption Standard（AES）を設定した WLAN/SSID を別々に使用してください。TKIP は廃止される可能性があるため、TKIP を WEP と併用するか、TKIP から完全に移行して可能であれば PEAP を使用することを推奨します。

WPA2 と 802.1X を有効にした WLAN を作成するには、次のコマンドを実行します。

(Cisco Controller) >config wlan security wpa enable <WLAN id>

指定した WPA2/802.1X WLAN に RADIUS 認証サーバを設定するには、次のコマンドを実行します。

(Cisco Controller) >config wlan radius_server auth add <WLAN id> <Server id>

指定した WPA2/802.1X WLAN に RADIUS アカウンティング サーバを設定するには、次のコマンドを実行します。

(Cisco Controller) >config wlan radius_server acct add <WLAN id> <Server id>

アイデンティティ設計のヒント：AAA オーバーライドの使用

各ワイヤレス クライアントに個別のセキュリティ ポリシーがあるなどのセキュリティ上の理由から、ワイヤレス クライアントを複数のサブネットワークに分割する必要があり、アイデンティティ ベースのネットワーキング サービスを設計する場合は、AAA オーバーライド機能を使用して WLAN を統合します。AAA オーバーライド機能によってユーザごとの設定を割り当てることができます。たとえば、分割された VLAN の特定のダイナミック インターフェイスにユーザを移動させたり、ユーザごとのアクセス コントロール リスト（ACL）を適用したりできます。

AAA オーバーライドを設定するには、次のコマンドを実行します。

(Cisco Controller) >config wlan aaa-override enable <WLAN id>

WLAN 設定を確認するには、次のコマンドを実行します。

(Cisco Controller) >show wlan <WLAN id>

```
WLAN Identifier.................................1
Profile Name....................................WLAN-1
Network Name (SSID).............................WLAN-1
Status..........................................Disabled
MAC Filtering...................................Disabled
Broadcast SSID..................................Enabled
AAA Policy Override.............................Enabled
Network Admission Control

Security

802.11 Authentication:..........................Open System
FT Support......................................Disabled
Static WEP Keys.................................Disabled
802.1X..........................................Disabled
Wi-Fi Protected Access (WPA/WPA2)...............Enabled
WPA (SSN IE)....................................Disabled
WPA2 (RSN IE)...................................Enabled
TKIP Cipher.....................................Disabled
AES Cipher......................................Enabled
Auth Key Management
802.1x..........................................Enabled
PSK.............................................Disabled
CCKM............................................Disabled
..
```

```
FT-1X(802.11r)..................................Disabled
FT-PSK(802.11r).................................Disabled
PMF-1X(802.11w).................................Disabled
Radius Servers
Authentication..................................10.10.10.60 1812
Accounting......................................10.10.10.60 1813
Interim Update..................................Disabled
Framed IPv6 Acct AVP ...........................Prefix
Dynamic Interface...............................Disabled
```

短い RADIUS タイムアウトの使用

802.1x に対して、大規模または高負荷のネットワークでは最も短い RADIUS タイムアウトを設定することを推奨します。長いタイムアウトを定義すると、RADIUS のキューのフレーム再送が長く維持されます。ネットワークのキャパシティやキューがどの程度ビジーかによりますが、タイムアウトを長くすると、再送障害発生率が高くなる場合があります。タイムアウトが長いと RADIUS サーバのダウンを検出するのに時間が長くかかる可能性があります。認証数が多いほとんどのネットワーク環境では、タイムアウトを短くすることでコントローラのキャパシティ処理が向上します。また、タイムアウトを短くすると、応答しない RADIUS サーバからの WLC の復帰が速くなります。しかしながら、RADIUS NAC（ISE）や遅い WAN 経由での RADIUS については、タイムアウトを長く（5 秒）することを推奨します。

次の例は、デフォルトの RADIUS タイムアウト（2 秒）を示します。この秒数は高速な RADIUS フェールオーバーでは許容可能でも Extensible Authentication Protocol-Transport Layer Security（EAP-TLS）認証には不十分です。この理由は、RADIUS サーバは外部データベース（Active Directory、NAC、SQL など）と通信して、指定されたタイムアウト時間内に応答する必要があるためです。

RADIUS タイムアウトを確認するには、次のコマンドを実行します。

(Cisco Controller) >show radius summary

```
Vendor Id Backward Compatibility................Disabled
Call Station Id Case............................lower
Acct Call Station Id Type.......................Mac Address
Auth Call Station Id Type.......................AP's Radio MAC Address:SSID
Aggressive Failover.............................Enabled
Keywrap.........................................Disabled
Authentication Servers
Idx  Type  Server Address    Port    State    Tout RFC3576
---  ----  ----------------  ------  --------  ----  -------
1    N     10.48.76.50       1812    Enabled   2     Enabled

IPSec -AuthMode/Phase1/Group/Lifetime/Auth/Encr
-----------------------------------------------
Disabled - none/unknown/group-0/0 none/none
```

RADIUS タイムアウトを設定するには、次のコマンドを実行します。

(Cisco Controller) >config radius auth retransmit-timeout 1 <seconds>

EAP Identity Request タイムアウト

コントローラのいくつかのシナリオによっては、EAP Identity Request のデフォルト タイムアウトを増やす必要があります。たとえば、EAP Identity Request に応える際にユーザの操作が必要な、スマート カードのワンタイム パスワード（OTP）を実装する場合です。自律型 AP では、デフォルトのタイムアウトは 30 秒です。自律型をインフラストラクチャ ワイヤレス ネットワークに移行する場合は、EAP Identity Request タイムアウトを変更することも検討してください。

デフォルトのタイムアウトを確認するには、次のコマンドを実行します。

(Cisco Controller) >show advanced eap

```
EAP-Identity-Request Timeout (seconds)...........30
EAP-Identity-Request Max Retries.................2
EAP Key-Index for Dynamic WEP....................0
EAP Max-Login Ignore Identity Response...........enable
EAP-Request Timeout (seconds)....................30
EAP-Request Max Retries..........................2
EAPOL-Key Timeout (milliseconds).................1000
EAPOL-Key Max Retries............................2
EAP-Broadcast Key Interval.......................3600
```

タイムアウト（秒単位）を変更するには、次のコマンドを実行します。

(Cisco Controller) >config advanced eap identity-request-timeout <seconds>

EAPoL キーのタイムアウトと最大再試行回数

推奨される EAPoL タイムアウトは、IP 7920 電話機などの音声クライアントの場合、できるだけ短くする必要があります。最大試行回数は、RF 環境が最適レベル以下で動作している場合、増やす必要があります。

デフォルトのタイムアウトを表示するには、次のコマンドを実行します。

(Cisco Controller) >show advanced eap

```
EAP-Identity-Request Timeout (seconds)...........30
EAP-Identity-Request Max Retries.................2
EAP Key-Index for Dynamic WEP....................0
EAP Max-Login Ignore Identity Response...........enable
EAP-Request Timeout (seconds)....................30
EAP-Request Max Retries..........................2
EAPOL-Key Timeout (milliseconds).................1000
EAPOL-Key Max Retries............................2
EAP-Broadcast Key Interval.......................3600
```

EAPoL タイムアウトを設定するには、次のコマンドを実行します。

(Cisco Controller) >config advanced eap eapol-key-timeout <milliseconds>

EAPoL 再試行回数を設定するには、次のコマンドを実行します。

(Cisco Controller) >config advanced eap eapol-key-retries <retries>

EAP リクエストのタイムアウトと最大再試行回数

クライアント タイプによりますが、一部のデバイスは非常に短いタイムアウトでは動作しない場合があります。しかしながら、その他のデバイスについては、劣悪な RF 環境で高速に復帰できるようタイムアウトを短く、再試行回数を多く設定することを推奨します。PEAP/GTC などの内部 EAP 方式を使用してクライアントが認証を行う場合にも適用できます。

デフォルトのタイムアウトを表示するには、次のコマンドを実行します。

(Cisco Controller) >show advanced eap

```
EAP-Identity-Request Timeout (seconds)...........30
EAP-Identity-Request Max Retries.................2
EAP Key-Index for Dynamic WEP....................0
EAP Max-Login Ignore Identity Response...........enable
EAP-Request Timeout (seconds).....................30
EAP-Request Max Retries...........................2
EAPOL-Key Timeout (milliseconds).................1000
EAPOL-Key Max Retries............................2
EAP-Broadcast Key Interval.......................3600
```

EAP リクエストのタイムアウトを設定するには、次のコマンドを実行します。

(Cisco Controller) >config advanced eap request-timeout <seconds>

EAP リクエストの再試行回数を設定するには、次のコマンドを実行します。

(Cisco Controller) >config advanced eap request-retries <retries>

CCKM タイムスタンプ妥当性検証

CCKM 妥当性検証を 5 秒に変更してピコセルやローミング問題を回避するには、次のコマンドを実行します。

(Cisco Controller) >config wlan security wpa akm cckm timestamp-tolerance 5000 <WLAN id>

TACACS + 管理タイムアウト

再認証が繰り返し試行されたり、プライマリ サーバがアクティブで接続可能なときにコントローラがバックアップ サーバにフォールバックしたりする場合には、TACACS + 認証サーバ、認可サーバ、およびアカウンティング サーバの再送信のタイムアウト値を増やすことを推奨します。ワンタイム パスワード（OTP）を実装する場合に特にこれが当てはまります。

(Cisco Controller) >show tacacs summary

Authentication Servers

```
Idx      Server Address        Port    State   Tout   MgmtTout
---      ---------------       ------  -------  -----  --------
1        10.10.10.60           49      Enabled  5      2


Authorization Servers

Idx      Server Address        Port    State   Tout   MgmtTout
---     ----------------       ------  -------  -----  --------
1       10.10.10.60            49      Enabled  5      2
```

TACACS + 認証再送信タイムアウトを設定するには、次のコマンドを実行します。

(Cisco Controller) >config tacacs auth server-timeout 1 <seconds>

TACACS + 認可再送信タイムアウトを設定するには、次のコマンドを実行します。

(Cisco Controller) >config tacacs athr server-timeout 1 <seconds>

SNMPv3 デフォルト ユーザの変更

SNMPv3 デフォルト ユーザをチェックしてください。デフォルトでは、コントローラでユーザ名が無効または変更するように設定されています。

SNMPv3 デフォルト ユーザを確認するには、次のコマンドを実行します。

(Cisco Controller) >show snmpv3user

```
SNMP v3 User Name    AccessMode  Authentication Encryption
-------------------- ----------- -------------- ----------
default               Read/Write  HMAC-SHA       CFB-AES
```

SNMPv3 デフォルト ユーザを設定するには、次のコマンドを実行します。

(Cisco Controller) >config snmp v3user delete default

(Cisco Controller) >config snmp v3user create nondefault rw hmacsha des authkey <*encrypkey12characters*>

注：SNMP 設定がコントローラと Wireless Control System（WCS）/Network Control System（NCS）/Prime Infrastructure（PI）間で一致していることを確認してください。また、ご自身のセキュリティ ポリシーに一致する暗号化キーおよびハッシュ キーを使用する必要があります。

Network Time Protocol（NTP）の有効化

Network Time Protocol（NTP）はいくつかの機能にとって非常に重要です。ロケーション、SNMPv3、アクセス ポイント認証、MFP のいずれかの機能を使用する場合、コントローラで NTP 同期を使用することは必須です。WLC では認証ありの NTP との同期がサポートされています。

NTP サーバを有効にするには、次のコマンドを実行します。

(Cisco Controller) >config time ntp server 1 10.10.10.1

トラップログのエントリで確認すると、次のように表示されます。

30 Mon Jan 6 08:12:03 2014 Controller time base status – Controller is in sync with the central timebase.

NTP 認証を有効にするには、次のコマンドを実行します。

(Cisco Controller) >config time ntp auth enable <ntp server index>

(Cisco Controller) >config time ntp key-auth add <key index>

802.11r Fast Transition の有効化

802.11r は高速ローミングの IEEE 規格で、この規格ではターゲット AP（つまり、クライアントの次の接続先 AP）との初回認証ハンドシェイクが、クライアントがターゲット AP に接続前であっても実行されます。これは Fast Transition（FT）と呼ばれ、デフォルトで Fast Transition は無効になっています。

注：802.11r 未対応のクライアントは 802.11r が有効な WLAN に接続できません。クライアントが 802.11r 対応（バージョン 6 以降の Apple デバイスなど）であることを確認してください。

802.11r または Fast Transition（FT）を有効にするには、次のコマンドを実行します。

(Cisco Controller) >config wlan security ft enable <WLAN id>

802.1X を使用した FT 認証管理を設定するには、次のコマンドを実行します。

(Cisco Controller) >config wlan security wpa akm ft-802.1X enable <WLAN id>

PSK を使用した FT 認証管理を設定するには、次のコマンドを実行します。

(Cisco Controller) >config wlan security wpa akm ftp-psk enable <WLAN id>

DHCP Required オプション

セキュリティを強化するために、シスコはすべてのクライアントが DHCP サーバから IP アドレスを取得することを推奨します。

WLAN 設定の DHCP Required オプションによって、クライアントとネットワークの間でトラフィックが送受信される前に、WLAN にアソシエーションするたびに DHCP アドレス要求または更新を実行するように強制できます。セキュリティの観点から、これによって使用中の IP アドレスの制御がより厳格になります。ただし、トラフィックの再通過が許可されるまでのローミング時間に影響がでる場合があります。

また、リース時間の期限切れまで DHCP 更新を実行しない実装では一部のクライアントに影響がでる場合があります。クライアント タイプによりますが、たとえば Cisco 7921 や 7925 電話機ではこのオプションを有効にするとローミング時に音声問題が発生する場合があります。これは、コントローラが音声またはシグナリング トラフィックの通過を DHCP フェーズが完了するまで許可しないためです。別の例では、Android および一部の Linux ディストリビューションはリース時間の半ばでのみ DHCP 更新を実行し、ローミングでは実行しない場合があります。クライアント エントリが期限切れの場合、これにより問題が発生する場合があります。

サードパーティ製のプリンタ サーバも影響を受ける可能性があります。一般に、WLAN に Windows 以外のクライアントがある場合にこのオプションを使用しないことを推奨します。DHCP クライアント側の実装方法によりますが、制御を厳格にすると接続問題が発生する可能性があるためです。

WLAN 設定の DHCP Required オプションを確認するには、次のコマンドを実行します。

(Cisco Controller) >show wlan <WLAN id>

```
WLAN Identifier.................................1
Profile Name....................................WLAN-1
Network Name (SSID).............................WLAN-1
Status..........................................Enabled
MAC Filtering...................................Disabled
…
mDNS Status.....................................Enabled
mDNS Profile Name...............................default-mdns-profile
DHCP Server.....................................Default
DHCP Address Assignment Required................Enabled
```

セキュリティ

次のセキュリティ ベスト プラクティスが WLC の [Advanced UI] のベスト プラクティス ページに追加されています

AP の 802.1x

説明：高度なセキュリティ ネットワークの AP で 802.1X を有効にして、ネットワーク セキュリティを強化します。

[Status]：

準拠：AP の 802.1x 認証が有効

非準拠：AP の 802.1x 認証が無効

CLI オプション：
次のコマンドを入力して、AP で 802.1x を有効にします。

(Cisco Controller) >config ap 802.1Xuser add username ap-userpassword password all

CPU ACL

説明：WLC へのアクセス全体を制御します

[Status]：
準拠：設定済み

非準拠：未設定

Client Exclusion（クライアントの除外）

説明：有効にすると、Cisco WLC は特定の条件でクライアントの参加を排除します。[Fix it Now] をクリックするとすべてのイベントで Client Exclusion を有効にします。

[Status]：
準拠：Client Exclusion がすべてのイベントに対して有効

非準拠：Client Exclusion がすべてのイベントに対して無効

CLI オプション：
次のコマンドを入力して、すべてのイベントで Client Exclusion を有効にします。

(Cisco Controller) >config wps client-exclusion all enable

レガシー IDS

説明：有効にすると、ワイヤレス IDS 機能および 17 の組み込みのシグニチャで侵入攻撃を防止できます。[Fix it Now] をクリックするとシグニチャ チェックが有効になります。

このベスト プラクティスが機能するには、少なくとも 1 つの WLAN が有効で、Client Exclusion リストがその WLAN で有効であることを確認します。WLAN で Client Exclusion リストを有効にするには、conf wlan exclusionlist wlan-id enabled コマンドを使用します。

[Status]：
準拠：標準のすべてのシグニチャ チェックが有効

非準拠：標準のすべてのシグニチャ チェックが無効

CLI オプション：
次のコマンドを入力して、シグニチャ チェックを有効にします。

(Cisco Controller) >config wps signature enable

ローカル管理パスワード ポリシー

説明：強力なパスワード ポリシーを適用します。**[Fix it Now]** をクリックして、次の強力なパスワード ポリシーを有効にします。

- case-check：同じ文字が 3 回連続して使用されているかを確認します
- consecutive-check：デフォルト値またはそのバリアントが使用されているかを確認します
- default-check：ユーザ名またはそれを逆にした文字が使用されているかを確認します

- all-checks：強力なパスワード チェックをすべて有効または無効にします
- position-check：古いパスワードからの 4 文字の流用を確認します
- case-digit-check：小文字、大文字、数字、特殊文字の 4 つすべての組み合わせが含まれているかを確認します

[Status]：

準拠：すべての強力なパスワード ポリシーが有効

非準拠：一部のパスワード ポリシーが有効か、すべてのパスワード ポリシーが無効

CLI オプション：

次のコマンドを入力して、すべての強力なパスワード ポリシーを有効にします。

(Cisco Controller) >config switchconfig strong-pwd all-checks enable

最小不正 AP RSSI しきい値

説明：AP が不正 AP を検出し、そのエントリを Cisco WLC に作成する場合の不正 AP の最小 RSSI 値を指定します。推奨値は -80 dBm です。[Fix it Now] をクリックして、最小 RSSI 値を変更し、その下限を -80 dBm にします。

[Status]：

準拠：-80 dBm に設定

非準拠：-80 dBm 未満に設定

CLI オプション：

次のコマンドを入力して、不正 AP の最小 RSSI 値を設定します。

(Cisco Controller) >config rogue detection min-rssi rssi-in-dBm

ピアツーピア

説明：ピアツーピア ブロッキング機能により、クライアント間で同じサブネットにトラフィックをブリッジすることを無効にします。クライアント対クライアント通信が望ましくない高度なセキュリティ ネットワークのみで推奨されます。エンタープライズおよび音声環境では、推奨しません。

[Status]：

準拠：1 つ以上の WLAN でピアツーピア ブロッキングが有効

非準拠：すべての WLAN でピアツーピア ブロッキングが無効

CLI オプション：

次のコマンドを入力して、ピアツーピア ブロッキングを有効にします。

(Cisco Controller) >config wlan peer-blocking drop wlan-id

不正 AP ポリシー

説明：ポリシーを [High] 以上にします。[Fix it Now] をクリックして、不正 AP 検出セキュリティ レベルを [High] に設定します。

[Status]：

準拠：ポリシーを [High] 以上に設定

非準拠：ポリシーを [Custom] に設定

次のコマンドを入力して、不正 AP 検出セキュリティ レベルを [High] に設定します。

(Cisco Controller) >config rogue detection security-level high

SSH/Telnet アクセス

説明：WLC への SSH をデフォルトで有効にします。[Fix it Now] をクリックして、WLC への SSH を有効に、WLC への Telnet を無効にします。

[Status]：

準拠：SSH が有効で Telnet が無効

非準拠：SSH が有効かつ Telnet が有効または SSH が無効かつ Telnet が有効

CLI オプション：

次のコマンドを入力して、SSH を有効にします。

(Cisco Controller) >config network ssh enable

次のコマンドを入力して、Telnet を無効にします。

(Cisco Controller) >config network telnet disable

ユーザ ログイン ポリシー

説明：コントローラのローカル ネット ユーザの同時ログイン数を制限するためにユーザ ログイン ポリシーを指定します。同時ログイン数を制限できるため、デフォルトの 0（ログインは無制限）より大きな値の設定を推奨します。

[Status]：

準拠：設定済み

非準拠：ユーザ ログイン ポリシーはなし

CLI オプション：

次のコマンドを入力して、ネット ユーザの制限を確認します。

(Cisco Controller) >show netuser summary

次のコマンドを入力して、ユーザ ログイン ポリシーを設定します。

(Cisco Controller) >config netuser maxUserLogin count

WPA2 または 802.1X を使用した WLAN

説明：WLAN で 802.1X または WPA セキュリティを使用します。[Fix it] ボタンはありません。WLAN ページへのリンクがあります。Day 0 デフォルトでは、802.1X 必須ではありません。

[Status]：

準拠：少なくとも 1 つの WLAN で 802.1X または WPA を使用している場合に有効

非準拠：無効

WPA2 と AES ポリシーを使用した WLAN

説明：WPA2+AES でセキュリティが向上するため、WPA+AES および TKIP の代わりに WPA2+AES の使用を推奨します。WPA+AES は将来のサポートが保証されないため、使用は推奨されません。

[Status]：

準拠：WPA+WPA2 を設定したすべての WLAN に WPA2+AES セキュリティ ポリシーがある

非準拠：WPA+WPA2 を設定したすべての WLAN に次のセキュリティ ポリシーがある

WPA+AES、WPA2+AES

WPA+AES

CLI オプション：

次の CLI を使用して、WLAN で WPA2+AES を有効にします。

(Cisco Controller) >config wlan security wpa enable wlan-id

ISE RADIUS

次のベスト プラクティスは ISE を AAA サーバとして使用するネットワークに適用可能であり、WLC の [Advanced UI] のベスト プラクティス ページに追加されています。

RADIUS サーバのタイムアウト

説明：RADIUS 認証およびアカウンティング サーバでは、クライアント参加タイムアウト問題が ISE RADIUS サーバで発生することを防止するために、サーバ タイムアウトの最小値を 5 秒に設定します。

[Status]：

準拠：すべての有効な RADIUS 認証およびアカウンティング サーバのタイムアウトが 5 秒以上。

非準拠：少なくとも 1 つの有効な RADIUS 認証およびアカウンティング サーバのタイムアウトが 5 秒未満。

CLI オプション：

次のコマンドを入力して、RADIUS 認証およびアカウンティング サーバのタイムアウトを設定します。

(Cisco Controller) >config radius auth retransmit-timeout RADIUS-Server-ID timeout-in-seconds

(Cisco Controller) >config radius acct retransmit-timeout RADIUS-Server-ID timeout-in-seconds

WLAN ISE 設定

説明：WLAN に Cisco ISE RADIUS サーバに推奨される設定が行われているかどうかを確認できます。

[Status]：

準拠：有効状態の WLAN の少なくとも 1 つに、ISE 設定セット全体が設定されている。

非準拠：有効状態の WLAN のすべてに、ISE 設定セット全体が設定されていない。

CLI オプション：

次のコマンドを入力して、複数の機能を設定する必要があります。

Security

次のコマンドを入力して、AAA サーバで interim update を有効にします。

(Cisco Controller) >config wlan radius_server acct interim-update enable wlan-id

次のコマンドを入力して、AAA サーバの interim interval を 0 秒に設定します。

(Cisco Controller) >config wlan radius_server acct interim-update 0 wlan-id

Advanced

次のコマンドを入力して、Client Exclusion を有効にします。

(Cisco Controller) >config wlan exclusionlist wlan-idenabled

次のコマンドを入力して、セッション タイムアウトを 7200 秒に設定します。

(Cisco Controller) >config wlan session-timeout wlan-id7200

次のコマンドを入力して、Client Exclusion リスト タイムアウトを 180 秒に設定します。

(Cisco Controller) >config wlan exclusionlist wlan-id 180

次のコマンドを入力して、ユーザ アイドル タイムアウトを 3600 秒に設定します。

(Cisco Controller) >config wlan usertimeout 3600 wlan-id

RADIUS のアグレッシブ フェールオーバー

説明：Cisco ISE サーバのクライアント認証で最適なパフォーマンスを得るには、RADIUS アグレッシブ フェールオーバーを無効にします。

[Status]：

準拠：RADIUS アグレッシブ フェールオーバーは無効。

非準拠：RADIUS アグレッシブ フェールオーバーは有効。

CLI オプション：

次のコマンドを入力して、RADIUS アグレッシブ フェールオーバーを無効にします。

(Cisco Controller) >config radius aggressive-failover disable

不正 AP の管理と検出

不正なワイヤレス デバイスは、企業のワイヤレス ネットワークにとって常に脅威となっています。ネットワークの所有者は、不明なデバイスをスキャンするだけでなく、それ以上のことを実施する必要があります。ネットワークの所有者は、不正 AP や侵入者の脅威の検出、無効化、位置の特定、および管理をリアルタイムで自動的に実行できる必要があります。

不正 AP は、正規のクライアントをハイジャックし、プレーン テキスト攻撃、DoS 攻撃、または中間者攻撃を使用することによって、無線 LAN の運用を妨害します。つまり、ハッカーは不正 AP を使用して、パスワードやユーザ名などの機密情報を取得できます。これに成功すると、ハッカーは一連の Clear To Send（CTS）フレームを送信できるようになります。このフレームでは AP を模倣し、特定のワイヤレス LAN クライアント アダプタに送信を通知し、他のすべてのアダプタには待機を通知します。その結果、正規のクライアントは、無線 LAN リソースに接続できなくなります。このため、無線 LAN のサービス プロバイダーは、その無線周波数帯で不正 AP を禁止する方法を探し求めています。

ベスト プラクティスは、不正 AP 検出を使用して、たとえば、ある企業の環境内でセキュリティ リスクを最小限に抑えることです。しかしながら、OEAP 環境、オープンエアーの会場やスタジアム、市全域、屋外など、不正 AP 検出が不要な特定のシナリオがあります。屋外のメッシュ AP を使用して不正 AP を検出しても、分析するリソースが増えるばかりでメリットはほとんどありません。さらに、不正 AP の自動封じ込めを評価する（または完全に止める）ことがきわめて重要です。これは、不正 AP の自動封じ込めを動作させておくと法的な問題や責任が生じる可能性があるためです。

次のセクションでは一部のベスト プラクティスを列挙しており、これにより AP 不正 AP リストの運用と管理の効率が向上します。

不正 AP 管理の詳細については、次のドキュメントを参照してください。

http://www.cisco.com/c/en/us/td/docs/wireless/technology/roguedetection_deploy/Rogue_Detection.html

悪意のある不正 AP ルールの適切な定義

日常的に悪意のある不正 AP ルールを定義して、早急な注意と軽減プランが必要な「major」および「critical」の不正 AP アラームに優先順位を付けます。

「major」または「critical」な不正 AP アラームは [Malicious] と分類され、ネットワーク上で検出されます。

各不正ルールは単一または複数の条件（必須または推奨）から構成されます。悪意のある不正 AP ルールは次のとおりです。

- 管理対象 SSID（必須）：ワイヤレス インフラストラクチャと同じ管理対象 SSID を使用する不正 AP はすべて [Malicious] とマークされる必要があります。管理者はこの脅威を調査し、軽減する必要があります。
- 最小 RSSI > -70 dBm（推奨）：この基準は通常、不明な不正 AP が設備の境界の内側にあることを示し、ワイヤレス ネットワークに対する干渉の原因となる可能性があります。

  このルールは、エンタープライズ環境に独自の隔離された建物とセキュアな境界がある場合にのみ推奨します。

  このルールは、小売業の店舗や、無線利用者からの Wi-Fi シグナルが混在している（さまざまなテナントによって共有される）場所には推奨されません。
- ユーザが設定した SSID/サブストリング SSID（推奨）が、実稼働 SSID（管理対象 SSID）の文字の別のバリエーションまたは組み合わせを使用している SSID をモニタします。

次の項目一覧に、悪意のある不正 AP ルールにおける条件一致の場合の推奨アクションを示します。

- 悪意のある不正 AP が [Must] 条件と一致する場合、[Contain] をアクションとして設定します。
- 各ルールに条件を 1 つのみ設定し、ルール名は関連付けた条件が直感的にわかるものにします。管理者による識別とトラブルシューティングを容易にするためです。
- 悪意のある不正 AP が [Optional] 条件と一致する場合、[Contain] をアクションとして設定することは、法的な問題があるため推奨しません。代わりに、[Alert] をアクションとして設定します。

注：不正な AP の封じ込めには法的意味合いがあります。しかしながら、自分の実稼働 SSID と同じ SSID を使用する不正な AP は、正規のワイヤレス クライアントを誘導する潜在的脅威を軽減する場合、自動封じ込めの例外になる可能性があります。

フレンドリーな不正 AP リストの定期的な特定および更新

定期的（毎週または毎月）に「未分類」の不正 AP リストのフレンドリーな不正 AP のリサーチと調査を行って、削除します。

次はフレンドリーな不正 AP の例です。

- 既知の内部の（設備の境界内など）フレンドリーな不正 AP やフレンドリーな不正 AP リストに含まれる既知の AP MAC アドレス。
- 既知の外部の（ベンダーが共有する会場や近隣の業者など）のフレンドリーな不正 AP。

未分類の不正 AP のための最善策

デフォルトでは定義された分類ルールと一致しない場合、不正 AP アラームは重大度が [Minor] の [Unclassified] と表示されます。このリストは増大するため、PI での管理が困難になります。たとえば、一時的な不正 AP（モバイル WiFi ルータなど）は短期間のみ検出されます。有線ネットワークで検出されない場合、このような一時的な不正 AP を毎日モニタする必要はありません。毎日のモニタではなく、以下を実行します。

- 自動スイッチポート トレースなどの自動不正 AP 軽減メカニズムを実行します。有線ネットワーク上でトレースされた場合、重大なアラートが上がります。
- 未分類の不正 AP のレポートを毎月または四半期ごとに生成し、この中から未知のフレンドリーな不正 AP の可能性があるものを特定します。

自動スイッチポート トレース（SPT）を不正 AP 軽減スキームとして実行

不正 AP 軽減のために自動 SPT を実行する、つまり不正 AP の無線 MAC アドレス（無線経由で取得）を有線ネットワーク側のイーサネット MAC アドレスと関連付けることを推奨します。潜在的な一致が見つかったら、PI に [Found On Network] とレポートされます。

- 自動 SPT を開始すると、すべての既知のスイッチ上のすべての既知のイーサネット MAC アドレスを参照して各不正 AP の無線 MAC アドレスを調査します。
- 重大度 [Minor] のアラームに対して自動 SPT を有効にすると、軽減スキームがすでにあるため管理者の業務が簡単になります。

AP で検出される不正 AP を確認するには、次のコマンドを実行します。

(Cisco Controller) >show rogue ap summary

```
Rogue Detection Security Level...................custom
Rogue Pending Time...............................180 secs
Rogue on wire Auto-Contain.......................Disabled
Rogue using our SSID Auto-Contain................Disabled
Valid client on rogue AP Auto-Contain............Disabled
Rogue AP timeout.................................1200
Rogue Detection Report Interval..................10
Rogue Detection Min Rssi.........................-128
Rogue Detection Transient Interval...............0
Rogue Detection Client Num Thershold.............0
Total Rogues(AP+Ad-hoc) supported................2000
Total Rogues classified..........................41

MAC Address        Classification     # APs # Clients Last Heard
-----------------  -----------------  ----- --------- -----------------------
00:0d:67:1e:7c:a5  Unclassified       1     0         Thu Feb  6 22:04:38 2014
00:0d:67:1e:7c:a6  Unclassified       1     0         Thu Feb  6 22:04:38 2014
00:0d:67:1e:7c:ac  Unclassified       2     0         Thu Feb  6 22:04:38 2014
```

不正 AP の設定

AP における不正 AP の設定を確認するには、次のコマンドを実行します。

(Cisco Controller) >show ap config general <AP Name>

```
Cisco AP Identifier..............................4
Cisco AP Name....................................AP1140
Country code.....................................Multiple Countries:PT,US
Regulatory Domain allowed by Country.............802.11bg:-AE    802.11a:-AE
AP Country code..................................US  - United States
AP Regulatory Domain.............................802.11bg:-A    802.11a:-A
..
AP Link Latency..................................Disabled
Rogue Detection..................................Enabled
```

AP における不正 AP 検出を有効にするには、次のコマンドを実行します。

(Cisco Controller) >config rogue detection enable <Cisco AP>

最小 RSSI

弱い RSSI の不正 AP について、ネットワーク管理者は有益な情報が得られません。また、弱い RSSI の不正 AP は、強いシグナルの不正 AP ほどワイヤレス ネットワークにとって脅威ではありません。弱いシグナルの不正 AP が多すぎると、Prime Infrastructure GUI に情報があふれ、不正 AP の軽減が困難になります。AP が不正 AP に対しレポートする必要がある最小 RSSI 値（**不正 AP 分類の最小 RSSI**）を制限すると、この問題を回避できます。

最小 RSSI -70 dBm に基づく不正 AP の検出を設定するには、次のコマンドを実行します。

(Cisco Controller) >config rogue detection min-rssi -70

不正 AP 検出のセキュリティレベルを [Low]（自動封じ込めなし）に設定するには、次のコマンドを実行します。

(Cisco Controller) >config rogue detection security-level low

不正 AP のルール

追加の条件セットの不正 AP のルール（例：rule1）を作成するには、次のコマンドを実行します。

(Cisco Controller) >config rogue rule add ap priority 1 classify malicious notify all state alert rule1

ルールを有効化するには、次のコマンドを実行します。

(Cisco Controller) >config rogue rule enable rule1

ルール サマリーを確認するには、次のコマンドを実行します。

(Cisco Controller) >show rogue rule summary

```
Priority   Rule Name  Rule state Class Type Notify  State   Match   Hit Count
-------- ------------------------------- ----------- ----------- -------- -------- ------
1          rule1      Enabled    Malicious    All   Alert    Any    0
```

最大 6 つの条件を 1 つの不正 AP のルールに追加できます。次の CLI 例については、不正 AP の管理のセクションの不正 AP の管理と検出、23 ページを参照してください。

条件ベースのルールを追加すると、ネットワークでスプーフィングを行う人物の検出が簡単になります。管理対象 SSID に基づいて条件ルールを設定するには、次のコマンドを実行します。

(Cisco Controller) >config rogue rule condition ap set managed-ssid rule1

特定の SSID 名に基づいて条件を追加するには、次のコマンドを実行します。

(Cisco Controller) >config rogue rule condition ap set ssid <SSID_name> rule1

最小 RSSI（-70 dBm など）に基づいて条件を追加するには、次のコマンドを実行します。

(Cisco Controller) >config rogue rule condition ap set rssi -70 rule1

不正 AP が検出された期間（秒単位：120 秒など）に基づいて条件を追加するには、次のコマンドを実行します。

(Cisco Controller) >config rogue rule condition ap set duration 120 rule1

不正 AP のルール条件を確認するには、次のコマンドを実行します。

(Cisco Controller) >show rogue rule detailed rule1

```
Priority.....................................1
Rule Name.....................................rule1
State.....................................Disabled
Type.....................................Malicious
Notify.....................................All
State .....................................Alert
Match Operation.............................Any
Hit Count.....................................0
Total Conditions.............................3
Condition 1
type.....................................Duration
value (seconds).............................120
Condition 2
type.....................................Managed-ssid
value.....................................Enabled
Condition 3
type.....................................Rssi
value (dBm).....................................-70
```

Wi-Fi Direct

Wi-Fi Direct を使用すると、Wi-Fi デバイスが即座に相互接続するため、コンテンツの印刷、同期、共有などの際に便利です。デバイスがインフラストラクチャ ネットワークとパーソナル エリア ネットワーク（PAN）両方に同時に接続する場合、ワイヤレス ネットワークにセキュリティ上の懸念が発生する場合があります。シスコは、セキュリティ ホール防止のために Wi-Fi Direct クライアントの無効化を推奨します。

Wi-Fi Direct クライアントの WLAN へのアソシエーションを無効にするには、次のコマンドを実行します。

(Cisco Controller) >config wlan wifidirect not-allow <WLAN-id>

不正 AP のチャネル スキャニング

ローカル/FlexConnect モード/モニタ モードの AP については、RRM 設定のオプションがあります。このオプションにより、ユーザは不正 AP スキャン対象のチャネルを選択できます。設定に応じて、AP は **[all channel]/[country channel]/[DCA channels]** で不正 AP をスキャンします。次にこれらのチャネルの特長を示します。

- セキュリティを強化する場合は、**[all channel]** を選択します。
- システムができるだけ小規模にスキャンを行い、パフォーマンスを重視する場合は、**[DCA channels]** を選択します。
- パフォーマンスとセキュリティのバランスを重視する場合は、**[country channel]** を選択します。

[all channels] の不正 AP 検出に 5 GHz チャネル スキャニングを設定するには、次のコマンドを実行します。

(Cisco Controller) >config advanced 802.11a monitor channel-list all

設定済み Country Code で 2.4 GHz モニタ チャネル スキャニングを設定するには、次のコマンドを実行します。

(Cisco Controller) >config advanced 802.11b monitor channel-list country

一時的な不正 AP 間隔

一時的な間隔値を使用することで、AP が不正 AP をスキャンする間隔を制御できます。AP は、それぞれの一時的間隔値に基づいて、不正 AP のフィルタリングも実行できます。

この機能には次の利点があります。

- AP からコントローラへの不正 AP レポートが短くなる。
- 一時的不正 AP エントリをコントローラで回避できる。
- 一時的な不正 AP への不要なメモリ割り当てを防止します。

一時的な不正 AP 間隔を 2 分（120 秒）に設定するには、次のコマンドを実行します。

(Cisco Controller) >config rogue detection monitor-ap transient-rogue-interval 120

アドホック不正 AP 検出の有効化

一般的な不正 AP 検出と同様に、アドホック不正 AP 検出はセキュリティが正当と認められる特定のシナリオに最適です。しかしながら、オープンエアーの会場/スタジアム、市全域、および公共の屋外環境などのシナリオでは推奨されません。

アドホック不正 AP 検出とレポートを有効にするには、次のコマンドを実行します。

(Cisco Controller) >config rogue adhoc enable

不正なクライアント AAA 検証の有効化

不正なクライアントの AAA 検証を有効にする理由は、WLC が AAA サーバに存在するクライアントを信頼できると継続的にチェックでき、クライアントには [Valid] または [Malicious] がマークされるからです。

(Cisco Controller) >config rogue client aaa enable

不正なクライアント MSE 検証の有効化

Mobility Services Engine（MSE）が使用でき、統合されている場合、MSE はその取得済みクライアントのデータベースの情報を共有して、クライアントが有効か脅威かの検証を WLC ができるようにします。

MSE の使用を有効にして、不正なクライアントが有効かどうかをチェックするには、次のコマンドを実行します。

(Cisco Controller) >config rogue client mse enable

ワイヤレス/RF

すべてのワイヤレス環境で、適切なサイト サーベイを常に実行し、ワイヤレス クライアントに適切な品質のサービスを提供してください。音声またはロケーション導入の要件はデータ サービスよりも厳密です。自動 RF はチャネルおよび電波出力の設定管理に役立つ場合がありますが、誤った RF 設計を訂正できません。

サイト サーベイは、実際のネットワークで使用されるデバイスの電波出力および伝達動作と一致するデバイスで行う必要があります。たとえば、最終的なネットワークで 802.11a/b/g/n および 802.11ac データ レートの最新式デュアル無線を使用する場合に、オムニ アンテナの古い 802.11b/g 無線を使用して、カバレッジ調査をしないでください。

サイト サーベイは、ユーザが設置する予定の AP モデルで実施する必要があります。AP は最終設置で一般的に設定する方向および高さにします。AP のデータ レートは、ユーザ アプリケーション、帯域幅、およびカバレッジ要件で必要とするレートに設定します。2.4 GHz のデータ レート 1 Mbps でカバレッジ エリアを測定しないでください。ネットワーク設計の最優先の目的が、各カバレッジ エリアにおいて 5 GHz のデータ レート 9 Mbps で 30 人の ユーザをサポートすることである場合は、プライマリ ネットワーク デバイスを使用し、5 GHz のデータ レート 9 Mbps のみを有効にしてカバレッジ テストを実行します。次に、AP とクライアント間で実際にトラフィックが流れている際にテスト ネットワーク クライアントに対して、AP で -67 dBm 受信シグナル強度インジケータ（RSSI）を測定します。高品質 RF リンクでは、SN 比（SNR）が良好で、チャネル使用（CU）率が低くなります。RSSI、SNR、および CU 値は WLC のクライアントおよび AP 情報ページに表示されます。

低データ レートの無効化

データ レートの無効化または有効化プロセスは慎重に計画する必要があります。カバレッジが十分な場合、低いデータ レートを下から 1 つずつ無効にしていくことを推奨します。ACK またはビーコンなどの管理フレームは最低必須レート（通常 1 Mbps）で送信されます。このレートでは、ほとんどのエアタイムが最低必須レートで消費されるため、スループット全体が低下します。

サポートするデータ レートの数を増やしすぎないようにしてください。再送のときにクライアントがデータ レートをダウンシフトするのが速くなるためです。一般的にクライアントは最速のデータ レートでの送信を試みます。フレームが通過しない場合、クライアントはフレームが通過するまで、次の最も低いデータ レートで再送します。サポートされているレートの一部を削除することは、フレームを再送する必要があるクライアントが複数のデータ レートを直接ダウンシフトすることを意味し、2 回目の試行でフレームが通過する可能性が高まります。

- ビーコンは最低必須レートで送信され、セル サイズの概略を定義します。
- マルチキャストは、接続しているクライアントに応じて、最低優先度および最高優先度の範囲で送信されます。
- 低いデータ レートが設計上必要ない場合、802.11b データ レート（1、2、5.5、および 11）の無効化を検討し、それ以外を有効にします。
- 802.11b のみ使用できるクライアントのサポートを継続するために、11 Mbps 未満のレートをすべては無効にしない、という意識的な決定も可能です。

次は参考例であり、あらゆる設計に対応した厳格なガイドラインではありません。これらの変更は慎重に行う必要があり、RF カバレッジ設計に大きく依存します。

- たとえば、ホットスポット向けの設計を行う場合は、最も低いデータ レートを有効にします。その目的は速度に対してカバレッジを得ることだからです。
- 逆に、高速ネットワークの設計を行う場合は、すでに RF カバレッジが良好であれば、最も低いデータ レートを無効にします。

低いデータ レート（5 GHz および 2.4 GHz）を無効にするには、次のコマンドを実行します。

(Cisco Controller) >config 802.11a disable network

(Cisco Controller) >config 802.11a 11nSupport enable

(Cisco Controller) >config 802.11a rate disabled 6

(Cisco Controller) >config 802.11a rate disabled 9

(Cisco Controller) >config 802.11a rate disabled 12

(Cisco Controller) >config 802.11a rate disabled 18

(Cisco Controller) >config 802.11a rate mandatory 24

(Cisco Controller) >config 802.11a rate supported 36

(Cisco Controller) >config 802.11a rate supported 48

(Cisco Controller) >config 802.11a rate supported 54

(Cisco Controller) >config 802.11a enable network

(Cisco Controller) >config 802.11b disable network

(Cisco Controller) >config 802.11b 11gSupport enable

(Cisco Controller) >config 802.11b 11nSupport enable

(Cisco Controller) >config 802.11b rate disabled 1

(Cisco Controller) >config 802.11b rate disabled 2

(Cisco Controller) >config 802.11b rate disabled 5.5

(Cisco Controller) >config 802.11b rate disabled 11

(Cisco Controller) >config 802.11b rate disabled 6

(Cisco Controller) >config 802.11b rate disabled 9

(Cisco Controller) >config 802.11b rate supported 12

(Cisco Controller) >config 802.11b rate supported 18

(Cisco Controller) >config 802.11b rate mandatory 24

(Cisco Controller) >config 802.11b rate supported 36

(Cisco Controller) >config 802.11b rate supported 48

(Cisco Controller) >config 802.11b rate supported 54

(Cisco Controller) >config 802.11b enable network

SSID 数を減らす

シスコは、コントローラで設定されるSSID の数を制限することを推奨します。SSID は（各 AP の無線ごとに）同時に 16 個まで設定できますが、それぞれの WLAN または SSID で個別のプローブ応答とビーコンが必要です。SSID がさらに追加されるにつれて、RF 環境は悪化します。また、PDA、WiFi 電話、バーコード スキャナなどの小型ワイヤレス ステーションの一部では、大量の base SSID（BSSID）情報を処理できません。この結果、ロックアップ（動作停止）、リロード、またはアソシエーションの失敗が発生します。また、SSID の数が増えるほどビーコンも増えるため、実際のデータ送信に利用できる RF 時間が減少します。企業の場合は 1 ～ 3 個の SSID を設定し、高密度設計の場合は 1 個の SSID を設定することを推奨します。単一の SSID シナリオでは、ユーザごとの VLAN または設定に AAA オーバーライドを利用できます。

SSID を確認するには、次のコマンドを入力します。

(Cisco Controller) >show wlan summary

```
Number of WLANs.................................8

WLAN ID  WLAN Profile Name / SSID                Status    Interface Name
-------  -----------------------------------  --------  --------------------
1        WLAN-Local / WLAN-Local                Enabled   management
2        WLAN-Lync / WLAN-Lync                  Enabled   Lync
3        WLAN-AVC / WLAN-AVC                    Enabled   AVC
4        WLAN-11ac / WLAN-11ac                  Enabled   11ac
5        WLAN-Visitor / WLAN-Visitor            Enabled   Visitor
6        WLAN-1X / WLAN-1X                      Enabled   1X
7        WLAN-23 / WLAN-23                      Enabled   23
8       WLAN-HS2 / WLAN-HS2                     Enabled   HS2
```

不要な SSID を無効にするには、次のコマンドを実行します。

(Cisco Controller) >config wlan disable 8

(Cisco Controller) >config wlan disable 7

(Cisco Controller) >config wlan disable 6

(Cisco Controller) >config wlan disable 5

...

クライアント ロード バランシングの有効化

高密度実稼働ネットワークでは、コントローラがロード バランシングをオン、ウィンドウ サイズを 5 以上に設定して動作することが確認されています。実際、ロード バランシング動作は大規模グループのユーザが会議場やオープン エリア（会議や授業）に集まっている場合などでのみ有効にします。ロード バランシングはこのようなシナリオでユーザを使用可能な各種 AP へ分散する場合に非常に役立ちます。ローミング問題が発生する場合があるため、音声 WLAN ではこの機能の無効化を推奨します。その他の WLAN では、テストでローミングに問題ないことが確認された場合のみ有効にします。

ロード バランシングを確認するには、次のコマンドを実行します。

(Cisco Controller) >show load-balancing

```
Aggressive Load Balancing.......................per WLAN enabling
Aggressive Load Balancing Window.................5 clients
Aggressive Load Balancing Denial Count...........3
Aggressive Load Balancing Uplink Threshold.......50
```

ロード バランシング ウィンドウ（推奨最小値は 5）を設定するには、次のコマンドを実行します。

(Cisco Controller) >config load-balancing window <0-20>

WLAN でロード バランシングを確認するには、次のコマンドを実行します。

(Cisco Controller) >show wlan <id>

```
WLAN Identifier.................................1
Profile Name....................................employee
Network Name (SSID).............................employee
Status..........................................Enabled
…
```

```
Band Select.....................................Enabled
Load Balancing..................................Disabled
Multicast Buffer................................Disabled
```

WLAN でロード バランシングを許可するには、次のコマンドを実行します。

(Cisco Controller) >config wlan load-balance allow enable <WLAN id>

バンドセレクトの有効化

バンドセレクトによって、デュアルバンド（2.4 GHz および 5 GHz）動作が可能なクライアントの無線を、混雑の少ない 5 GHz AP に移動できます。2.4 GHz 帯は、混雑していることがよくあります。この帯域のクライアントは、Bluetooth デバイス、電子レンジ、およびコードレス電話機からの干渉を受けるだけでなく、他の AP からの同一チャネル干渉も受けます。これは、802.11b/g では、重複しないチャネルが 3 つに制限されるためです。これらの干渉の原因を防止して、ネットワーク全体のパフォーマンスを向上させるには、コントローラで次のようにバンドセレクトを設定できます。

- バンドセレクトは、デフォルトではグローバルに有効または無効になっています。
- バンドセレクトのしくみは、クライアントへのプローブ応答を規制するというものです。5 GHz チャネルへクライアントを誘導するために、2.4 GHz チャネルでのクライアントへのプローブ応答を遅らせます。
- 音声のバンドセレクトを評価する場合は、特にローミングのパフォーマンスに焦点を当ててください。
- AP の 5 GHz シグナルが 2.4 GHz シグナルと同じかより強い場合、大部分の最新クライアントではデフォルトで 5 GHz を優先します。
- 高密度設計では、バンドセレクトを有効にする必要があります。

また、高密度設計では、使用可能な UNII-2 チャネルを調査する必要があります。レーダーによる影響を受けず、クライアントベースで使用可能なチャネルは、RRM DCA リストに使用可能チャネルとして追加する必要があります。

デュアルバンド ローミングは、クライアントによっては低速になる可能性があります。大部分の音声クライアントでローミング動作が低速な場合は、それらのクライアントが 2.4 GHz に留まっている可能性が高くなります。この場合、5 GHz でスキャンの問題が発生しています。一般に、クライアントがローミングすることを決定した場合、現在のチャネルと帯域を最初にスキャンします。クライアントでは一般に、シグナルレベルが大幅に高い（例：20 dB）AP や、大幅に高い SNR を持つ AP を確認するためにスキャンします。そのような接続が使用できない場合、クライアントは現在の AP に留まる可能性があります。この場合、2.4 GHz のチャネル使用率が低く、通話品質が悪くなければ、選択されたバンド（周波数帯）を無効にできます。しかしながら、推奨される設計は、すべてのデータ レートを有効にし、6 Mbps を必須にして、5 GHz でバンドセレクトを有効にすることです。この後、5 GHz RRM の最小送信電力を、RRM によって設定される 2.4 GHz の平均送信電力よりも 6 dBm 高く設定します。

この推奨設定の目的は、クライアントが、より良好な SNR と送信電力のバンド（周波数帯）とチャネルを最初に獲得できるようにすることです。前述のとおり、一般的にクライアントがローミングすることを決定した場合、現在のチャネルとバンド（周波数帯）を最初にスキャンします。このため、クライアントが最初に 5 GHz 帯に参加した場合、5 GHz の送信電力が良好であれば、そのバンド（周波数帯）に留まる可能性が高くなります。5 GHz の SNR レベルは、通常 2.4 GHz よりも高くなります。これは、2.4 GHz には Wi-Fi チャネルが 3 つしかなく、Bluetooth、iBeacon、電子レンジなどのシグナルの干渉の影響を受けやすいためです。

デュアルバンド レポーティングでは、802.11k を有効にすることを推奨します。これにより、すべての 11k 対応クライアントが、経由ローミングのメリットを享受できます。デュアルバンド レポーティングを有効にすると、クライアントでは、クライアントから指示された要求時に、最良の 2.4 および 5 GHz AP のリストを受け取ります。ほとんどの場合、クライアントは同じチャネル、次にクライアントが現在使用している同じ帯域の順序で AP のリストを上から検索します。このロジックにより、スキャン時間が短縮され、バッテリーの電力が節約されます。WLC で 802.11k を有効にしても、802.11k 以外のクライアントに悪影響を与えません。

次のコマンドを入力して、バンドセレクトを確認します。

(Cisco Controller) >show band-select

```
Band Select Probe Response.....................per WLAN enabling
Cycle Count....................................2 cycles
Cycle Threshold................................200 milliseconds
Age Out Suppression............................20 seconds
Age Out Dual Band..............................60 seconds
Client RSSI....................................-80 dBm
```

特定の WLAN でバンドセレクトを有効または無効にするには、次のコマンドを実行します。

(Cisco Controller) >config wlan band-select allow enable <WLAN id>

DCA（動的チャネル割り当て）

ワイヤレス ネットワークがまず初期化される際に、参加するすべての無線でチャネル割り当ては干渉なしに動作する必要があります。DCA を使用すると、チャネル割り当てが最適化されるため、干渉のない動作が可能になります。ワイヤレス ネットワークでは、チャネル割り当て時に、利用可能チャネルごとに各無線から報告された電波メトリックを使用します。これにより、チャネルの帯域幅を最大化し、すべての干渉源（当該ネットワーク（シグナル）、他のネットワーク（外部干渉）、ノイズ（その他すべて））からの RF 干渉を最小化できます。

DCA はデフォルトで有効になっており、社内のネットワークのためにチャネルプランニングのグローバルな解決策として機能します。

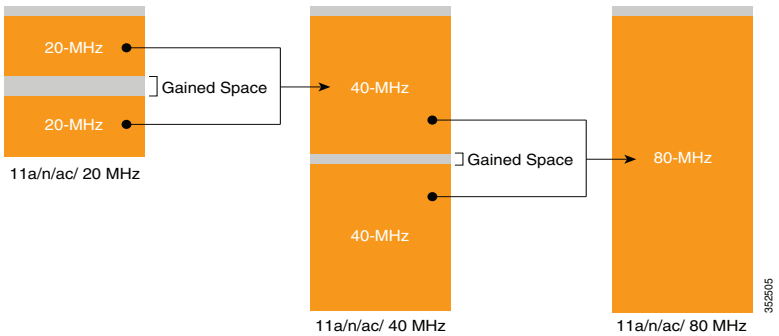
- 可用性および干渉に基づいて、すべての 802.11a または 802.11b/g チャネルが RRM によって自動的に設定されるようにするには、次のコマンドを入力します。

(Cisco Controller) >config 802.11a channel global auto

(Cisco Controller) >config 802.11b channel global auto

チャネル幅

2 つの 20 MHz チャネルを 1 つに束ねることで 802.11n は 40 MHz チャネルで動作可能です。これによりスループットが大幅に向上します。すべての 802.11n デバイスで 40 MHz ボンディング チャネル（クライアント）がサポートされるわけではありません。802.11ac では 20 MHz チャネルを 80 MHz 帯チャネルに束ねて使用できますが、すべてのクライアントで 80 MHz がサポートされている必要があります。重複のない 20 MHz チャネルは使用可能な数の制限が厳しいため、2.4 GHz では実用的ではありません。ただし、5 GHz では 20 MHz チャネルが十分にあれば、スループットおよび速度が大幅に向上します（以下の DFS を参照）。



チャネル幅をすべての対応可能な無線に割り当てる DCA を設定するには、次のコマンドを入力します。

(Cisco Controller) config advanced 802.11a channel dca chan-width-11n <20 | 40 |80>

チャネル幅の概要：

- **20**：無線に 20 MHz チャネルのみを使用した通信を許可します。20 MHz チャネルだけを使用して通信するレガシー 802.11a 無線、20 MHz 802.11n 無線、または 40 MHz 802.11n 無線の場合にこのオプションを選択します。これはデフォルト値です。
- **40**：40 MHz 802.11n 無線に、隣接する 2 つの 20 MHz チャネルを結合して使用した通信を許可します。データのスループット向上のため、無線ではアンカー チャネル（ビーコン用）として選択するプライマリ チャネルおよび拡張チャネルを使用します。各チャネルには、1 つの拡張チャネルがあります（36 と 40 のペア、44 と 48 のペアなど）。たとえば、プライマリ チャネルとして 44 を選択すると、Cisco WLC では拡張チャネルとしてチャネル 48 が使用されます。プライマリ チャネルとして 48 を選択すると、Cisco WLC では拡張チャネルとしてチャネル 44 が使用されます。
- **80**：802.11ac 無線のチャネル幅を 80 MHz に設定します。

20 MHz、40 MHz または 80 MHz モードのアクセス ポイント無線を静的に設定すると、グローバルに設定された DCA チャネル幅の設定（**config advanced 802.11a channel dca chan-width-11n {20 | 40 |80}** コマンドを使用して設定）が無効になります。このアクセス ポイントの無線に対する静的な設定をグローバルに戻すように変更すると、それまでアクセス ポイントで使用されていたチャネル幅がグローバルな DCA 設定で上書きされます。DCA に設定された実行頻度によって、変更は 30 分以内に有効になります。

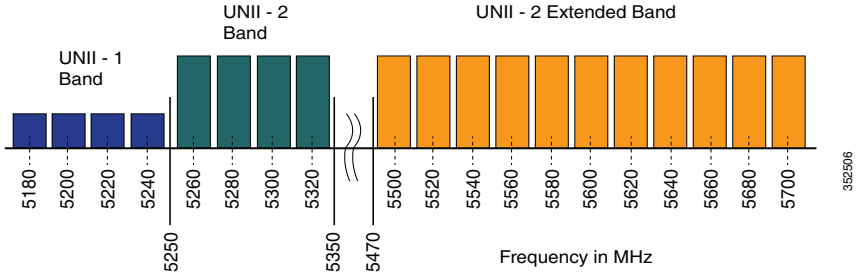
チャネル 116、120、124、および 128 は、米国とカナダの 40 MHz チャネル ボンディングには使用できません。

DFS：動的周波数選択

動的周波数選択は、5 GHz スペクトルでのチャネルの可用性を向上させるために作成されました。規制ドメインに応じて、DFS は 4 ～ 12 の追加チャネルにすることができます。チャネルを多くすることは、容量が増えることを意味しています。

DFS はレーダーシグナルを検出し、同一周波数で運用されている可能性のある気象レーダーと干渉しないことを確認します。DFS 仕様はまた、クライアントと AP を検出されたシグナルから遠ざける、グループ用のモニタとしてマスター AP を指定します。従来、北米では DFS チャネルの使用に関して不安があり、北米では DFS ではない 8 チャネルが使用されています。ETSI の規制ドメイン（ヨーロッパ）では、非 DFS チャネルは 4 個で、長年 DFS チャネルを問題なく使用しています。

5 GHz 帯はより多くのチャネルを提供できますが、5 GHz チャネルは電力が可変的で、屋内/屋外の導入制限があるため、設計全体で注意が必要です。たとえば北米では、U-NII-1 は屋内でのみ使用可能で、最大電力が 50 mW の電力制限があり、U-NII-2 と U-NII-2e の両方が動的周波数選択の対象です。



デフォルトでは、U-NII-2e チャネルは DCA のチャネル リストで無効になっています。

使用されているチャネルを確認するには、次のコマンドを入力します。

(Cisco Controller) show>advanced 802.11a channel

<snip>

802.11a 5 GHz Auto-RF Channel List

Allowed Channel List..36,40,44,48,52,56,60,64,149,153,157,161

Unused Channel List..100,104,108,112,116,120,124,128,132,136,140,165

DCA Outdoor AP option.....Disabled

規制ドメインでより多くのチャネルのために U-NII-2e チャネルを有効にするには、次のコマンドを入力します。

(Cisco Controller) >config advanced 802.11a channel add <channel>

北米およびヨーロッパで利用可能なチャネルは 100 ～ 140（8 追加チャネル）です。120、124、および 128 チャネルは米国では無効であり、ETSI DFS ルールで厳しく罰せられ、サポートされません。

DCA の再起動

チャネルおよびチャネル幅の選択を行った後、または新しいネットワークをインストールした場合、DCA は動的にチャネルを管理し、時間や状況の変化に応じて調整を行います。しかし、これが新しいインストレーションである場合、またはチャネル幅の変更や新しいアクセス ポイントの追加など DCA への大幅な変更を行った場合には、DCA プロセスを再起動できます。これはアグレッシブ検索モード（スタートアップ）を初期化し、最適化開始チャネル プランを提供します。

どの WLC が現在グループ リーダーかを判断するには、次のコマンドを入力します。

(Cisco Controller) >show advanced 802.11a group

(Cisco Controller) >show advanced 802.11b group

識別されたグループ リーダーから DCA を再初期化するには、次のコマンドを入力します。

(Cisco Controller) >config advanced 802.11a channel global restart

(Cisco Controller) >config advanced 802.11b channel global restart

再起動を確認するには、次のコマンドを入力します。

(Cisco Controller) >show advanced 802.11a channel

<snip>

```
Last Run Time.................................0 seconds
DCA Sensitivity Level.....................STARTUP (5 dB)
DCA 802.11n/ac Channel Width...................80 MHz
DCA Minimum Energy Limit.....................-95 dBm
```

成功した場合は、DCA の感度が表示され、起動バナーが表示されます。

注: スタートアップ モードは 100 分間実行され、一般的に 30 ～ 40 分以内で解決に達します。大幅な変更がチャネル幅や AP の数などに行われた場合、これは、クライアントの障害となる可能性があります。

自動送信電力制御（TPC）

Cisco WLC は、ワイヤレス LAN のリアルタイムな状況に基づいて、アクセス ポイントの送信電力を動的に制御します。TPCv1 および TPCv2 の 2 つのバージョンの送信出力制御から選択できます。TPCv1 では、送信電力を低く維持することでキャパシティを増やし、干渉を減らすことができます。TPCv2 では、干渉を最小にするために、送信電力を動的に調整します。TPCv2 は、高密度のネットワークに適しています。このモードでは、ローミングの遅延およびカバレッジ ホールのインシデントが多く発生する可能性があります。

送信電力制御（TPC）アルゴリズムでは、RF 環境での変化に応じてアクセス ポイント（AP）の送信電力を増減させます。ほとんどの場合、TPC では干渉を低減するために AP の送信電力を減らそうとします。しかし、RF カバレッジに急激な変化が生じた場合（たとえば、AP で障害が発生したり、AP が無効になったりした場合）、TPC は周囲の AP の送信電力を増やす可能性もあります。この機能は、主にクライアントと関係があるカバレッジ ホールの検出とは異なります。TPC は AP 間のチャネルの干渉を防止しながら、必要なカバレッジ レベルを達成するために、十分な RF 送信電力を供給します。

注: 最適なパフォーマンスを得るには、無線ごとに最適な送信電力を許可するための [Automatic] 設定を使用します。

a または b 無線のいずれかで自動 TPC を設定するには、次のコマンドを入力します。

(Cisco Controller) >config 802.11a|b txPower global auto

自動カバレッジ ホール検出（CHD）

コントローラは、AP から報告されたクライアントのシグナルの品質情報を基に、AP の送信電力を増やす必要があるかどうかを判断します。カバレッジ ホールの検出（CHD）はコントローラに依存しないため、RF グループ リーダーはこれらの計算に関与しません。コントローラでは、特定の AP に接続しているクライアント数、およびクライアントごとのシグナル対雑音比（SNR）の値がわかります。

クライアントの SNR がコントローラに設定されたしきい値を下回った場合、AP はクライアントを補うために自身の送信電力を増やします。SNR のしきい値は、AP の送信電力とコントローラのカバレッジ プロファイル設定に基づいて設定されます。

CHD を設定する（GUI のみ）には、次の手順を実行します。

1. 次の手順で 802.11 ネットワークを無効にします。
   a. [Wireless] > [802.11a/n/ac] または [802.11b/g/n] > [Network] に移動して、[802.11a（または 802.11b/g）Global Parameters] ページを開きます。
   b. [802.11a（または 802.11b/g）Network Status] チェックボックスをオフにします。
   c. [Apply] をクリックします。
2. [Wireless] > [802.11a/n/ac] または [802.11b/g/n] > [RRM] > [Coverage] に移動して、[802.11a/ac（または 802.11b/g/n）> RRM > Coverage] ページを開きます。
3. [Enable Coverage Hole Detection] をクリックします。
4. [Apply] をクリックします。

アクセス ポイント グループ

コントローラ上に最大 512 の WLAN を作成した後、異なったアクセス ポイントに WLAN を選択的に公開（アクセス ポイント グループを使用して）することで、ワイヤレス ネットワークをより適切に管理できます。一般的な展開では、WLAN 上のすべてのユーザはコントローラ上の 1 つのインターフェイスにマッピングされます。したがって、WLAN に接続しているすべてのユーザは、同じサブネットまたは VLAN に存在します。しかし、複数のインターフェイス間で負荷を分散したり、または AP グループを作成して、個々の部門（たとえばマーケティング部門）などの特定の条件に基づいたユーザのグループに対して負荷を分散したりすることを選択できます。さらに、ネットワーク管理を簡素化するために、これらの AP グループを別個の VLAN で設定できます。AP グループを使用して、物理的な場所に基づいてトラフィックを分離してください。

AP グループを設定するには、次の手順を入力します。

(Cisco Controller) >config wlan apgroup add <group_name>

説明を AP グループに追加するには、次のコマンドを入力します。

(Cisco Controller) >config wlan apgroup description <group_name description>

WLAN を AP グループに割り当てるには、次のコマンドを入力します。

(Cisco Controller) >config wlan apgroup interface-mapping add <group_name wlan_id interface_name>

AP グループに WLAN 無線ポリシーを設定するには、次のコマンドを入力します。

(Cisco Controller) >config wlan apgroup wlan-radio-policy <apgroup_name wlan_id> {802.11a-only | 802.11bg | 802.11g-only | all}

AP を AP グループに割り当てるには、次のコマンドを入力します。

(Cisco Controller) >config ap group-name <group_name Cisco_AP>

RF プロファイル

RF プロファイルを使用すると、共通のカバレッジ ゾーンを共有する AP グループを調整し、そのカバレッジ ゾーン内の AP に対する RRM の動作を選択的に変更できます。たとえば、多くのユーザが集まる、または会合するエリアに、大学が高密度の AP を展開する場合があります。この場合は、同一チャネル干渉を管理しながら、セル密度に対処するために、データ レートと送信電力の両方を操作する必要があります。隣接エリアでは、通常のカバレッジが提供されますが、そのような操作によってカバレッジが失われます。

RF プロファイルと AP グループを使用すると、異なる環境やカバレッジ ゾーンで動作する AP グループに対する RF 設定を最適化できます。RF プロファイルは、802.11 無線用に作成されます。RF プロファイルは、AP グループに属するすべての AP に適用され、そのグループ内のすべての AP に同じプロファイルが設定されます。RF プロファイルによりデータ レートと送信電力値を制御できるため、RF ネットワークの制御性を改善する観点からお勧めします。

RF プロファイルの設定

RF プロファイルの作成

RF プロファイルの説明を指定するには、次のコマンドを入力します。

(Cisco Controller) >config rf-profile description <text profile-name>

この RF プロファイルの AP に適用するデータ レートを設定するには、次のコマンドを入力します。

(Cisco Controller) >config rf-profile data-rates {802.11a | 802.11b} supported <rate profile-name>

最大送信電力割り当ておよび最小送信電力割り当て（この RF プロファイル内の AP が使用できる最大送信電力と最小送信電力）を設定するには次のコマンドを入力します。

(Cisco Controller) >config rf-profile {tx-power-max | tx-power-min} <power-value profile-name>

TPC のバージョン 1 またはバージョン 2 に対するカスタム TPC 送信電力しきい値を設定するには、次のコマンドを入力します。

(Cisco Controller) >config rf-profile {tx-power-control-thresh-v1 | tx-power-control-thresh-v2} <power-threshold profile-name>

カバレッジ データを設定するには、次のコマンドを入力します。

(Cisco Controller) >config rf-profile coverage data <value-in-dBm profile-name>

最小クライアント カバレッジ例外レベルを設定するには、次のコマンドを入力します。

(Cisco Controller) >config rf-profile coverage exception <clients profile-name>

カバレッジ例外レベルの割合を設定するには、次のコマンドを入力します。

(Cisco Controller) >config rf-profile coverage level <percentage-value profile-name>

音声のカバレッジを設定するには、次のコマンドを入力します。

(Cisco Controller) >config rf-profile coverage voice <value-in-dBm profile-name>

AP 無線ごとに許可されるクライアントの最大数を設定するには、次のコマンドを入力します。

(Cisco Controller) >config rf-profile max-clients <num-of-clients profile-name>

クライアントのトラップしきい値を設定するには、次のコマンドを入力します。

(Cisco Controller) >config rf-profile client-trap-threshold <threshold-value profile-name>

マルチキャストを設定するには、次のコマンドを入力します。

(Cisco Controller) >config rf-profile multicast data-rate <rate profile-name>

ロード バランシングを設定するには、次のコマンドを入力します。

(Cisco Controller) >config rf-profile load-balancing {window <num-of-clients> | denial <value} profile-name>

バンドセレクトの設定

バンドセレクト サイクル数を設定するには、次のコマンドを入力します。

(Cisco Controller) >config rf-profile band-select cycle-count <max-num-of-cycles profile-name>

サイクルしきい値を設定するには、次のコマンドを入力します。

(Cisco Controller) >config rf-profile band-select cycle-threshold <time-in-milliseconds profile-name>

バンドセレクトの有効期限を設定するには、次のコマンドを入力します。

(Cisco Controller) >config rf-profile band-select expire {dual-band | suppression} <time-in-seconds profile-name>

プローブ応答を設定するには、次のコマンドを入力します。

(Cisco Controller) >config rf-profile band-select probe-response enable <profile-name>

プローブに応答する条件となる、クライアントの RSSI の最小値を設定するには、次のコマンドを入力します。

(Cisco Controller) >config rf-profile band-select client-rssi <value-in-dBm profile-name>

アクセスポイントグループのために 802.11n 専用モードを設定するには、次のコマンドを入力します。

(Cisco Controller) >config rf-profile 11n-client-only enable <rf-profile-name>

注:802.11n 専用モードでは、アクセス ポイント ブロードキャストによって 802.11n の速度がサポートされます。802.11n クライアントのみが、アクセス ポイントに接続できます

AP グループへの RF プロファイルの適用（CLI）

RF プロファイルを AP グループに適用するには、次のコマンドを入力します。

(Cisco Controller) >config wlan apgroup profile-mapping add <ap-group-name rf-profile-name>

VLAN Select/Pooling

VLAN Select 機能を使用すると、複数の VLAN に対応している単一の WLAN を使用できるようになります。クライアントは、設定されている VLAN の 1 つに割り当てることができます。この機能を使用すれば、インターフェイス グループを使用して 1 つまたは複数のインターフェイスの VLAN に WLAN をマッピングすることができます。この WLAN に接続するワイヤレス クライアントは、インターフェイスで特定されるサブネットのプールから IP アドレスを受信します。有効にすると、VLAN Select 機能により、指定した WLAN のクライアントは、複数のダイナミック インターフェイスから IP アドレスを取得できます。

VLAN を有効にするには、次のコマンドを実行します。

1. インターフェイス グループを作成します。
2. インターフェイス グループにインターフェイスを追加します。
3. インターフェイス グループを WLAN に追加します。

インターフェイス グループを作成するには、次のコマンドを入力します。

(Cisco Controller) >config interface group create <interface_group_name>

(Cisco Controller) >config interface group description <interface_group_name description>

インターフェイス グループにインターフェイスを追加するには、次のコマンドを入力します。

(Cisco Controller) >config interface group interface add <interface_group interface_name>

インターフェイス グループを WLAN に追加するには、次のようにします（CLI）。

(Cisco Controller) >config wlan interface <wlan_id interface_group_name>

RF 管理

自動カバレッジホール検出

説明：自動 CHD を有効にする必要があります。コントローラは、AP から報告されたクライアントのシグナルの品質情報を基に、AP の送信電力を増やす必要があるかどうかを判断します。カバレッジ ホールの検出（CHD）はコントローラに依存しないため、RF グループ リーダーはこれらの計算に関与しません。コントローラは、特定の AP に接続しているクライアント数、およびクライアントごとのシグナル対雑音比（SNR）の値を把握しています。クライアントの SNR がコントローラに設定されたしきい値を下回った場合、AP はクライアントを補うために自身の出力を増やします。SNR のしきい値は、AP の送信電力とコントローラのカバレッジ プロファイル設定に基づいて設定されます。自動 CHD を設定する方法の手順については、『Cisco Wireless Controller Configuration Guide』を参照してください。

[Status]：

準拠：CHD 有効

非準拠：なしまたは 1 つ有効

自動動的チャネル割り当て

説明：RRM が各無線に最適なチャネルを選択できるように自動 DCA を有効にする必要があります。[Fix it Now] をクリックして自動 DCA を有効にします。ワイヤレス ネットワークが初めて初期化される際、参加するすべての無線で、干渉なしで動作するためにチャネルの割り当てが必要になります。チャネルの割り当てを最適化して、干渉のない運用を可能にするのは、DCA の仕事です。ワイヤレス ネットワークでは、このチャネルの割り当て時に、検出された全チャネルについて各無線から報告された電波メトリックを使用します。これは、チャネルの帯域幅を最大化し、すべての干渉源（当該ネットワーク（シグナル）、他のネットワーク（外部干渉）、ノイズ（その他すべて））からの RF 干渉を最小化するための解決策です。DCA はデフォルトで有効になっており、社内のネットワークのためにチャネルプランニングのグローバルな解決策として機能します。

[Status]：

準拠：DCA が 802.11a/b で有効

非準拠：なしまたは 1 つが有効

CLI オプション：次のコマンドを入力して自動 DCA を有効にします。

```
(Cisco Controller) >config 802.11a channel global auto ??(Cisco Controller) >config 802.11b channel
global auto
```

自動送信電力制御

説明：RRM が各無線に最適な送信電力を選択できるように自動 TPC を有効にする必要があります。[Fix it Now] をクリックして自動 TPC を有効にします。Cisco WLC は、ワイヤレス LAN のリアルタイムな状況に基づいて、アクセス ポイントの送信電力を動的に制御します。TPCv1 および TPCv2 の 2 つのバージョンの送信出力制御から選択できます。TPCv1 では、送信電力を低く維持することでキャパシティを増やし、干渉を減らすことができます。TPCv2 では、干渉を最小にするために、送信電力を動的に調整します。TPCv2 は、高密度のネットワークに適しています。このモードでは、ローミングの遅延およびカバレッジ ホールのインシデントが多く発生する可能性があります。送信電力制御（TPC）アルゴリズムでは、RF 環境での変化に応じてアクセス ポイント（AP）の送信電力を増減させます。ほとんどの場合、TPC では干渉を低減するために AP の送信電力を減らそうとします。しかしながら、RF カバレッジに急激な変化が生じた場合（たとえば、AP で障害が発生したり、AP が無効になったりした場合）、TPC が周囲の AP の電力を増やす可能性もあります。この機能は、主にクライアントと関係があるカバレッジ ホールの検出とは異なります。TPC は AP 間のチャネルの干渉を防止しながら、必要なカバレッジ レベルを達成するために、十分な RF 送信電力を供給します。

注：最適なパフォーマンスを得るには、無線ごとに最適な送信電力を許可するための [Automatic] 設定を使用します。

[Status]:

準拠：TPC が 802.11a/b で有効

非準拠：なしまたは 1 つが有効

CLI オプション：次のコマンドを入力して、自動 TPC を有効にします。

```
(Cisco Controller) >config 802.11a txPower global auto ??(Cisco Controller) >config 802.11b txPower
global auto
```

ベスト チャネル幅

説明：DBS はクライアント データ レートが最も高く、無線あたりのチャネル使用率が最も低くなるような、最も広いチャネル幅を選択します。これにより、不正 AP と CleanAir の干渉を回避しながら、5 GHz 帯でデータの再試行回数および CRC エラーを最小限に抑えます。

[Status]:

準拠：両方のバンド（周波数帯）でベストなチャネル幅が選択される

非準拠：両方のバンド（周波数帯）でベストなチャネル幅が選択されない

CLI オプション：次のコマンドを入力して、ベスト チャネル帯域幅を有効にします。

```
(Cisco Controller) >config advanced 802.11a channel dca chan-width best
```

CleanAir 検出

説明：CleanAir を有効にする必要があります。[Fix it Now] をクリックして CleanAir を有効にします。RF 干渉を効果的に検出し軽減するため、可能な限り CleanAir を有効にします。汎用の DECT 電話、電波妨害装置など、セキュリティ アラートを起動する各干渉源に対しては推奨対策があります。

[Status]:

準拠：有効

非準拠：無効

CLI オプション:

ネットワークの CleanAir の設定を確認するには、次のコマンドを入力します。

```
(Cisco Controller) >show 802.11{a|b} cleanair config
```

ネットワークの CleanAir 機能を有効にするには、次のコマンドを入力します。

```
(Cisco Controller) >config 802.11{a|b} cleanair enable network
```

特に電波妨害装置による干渉の検出を有効にするように設定するには、次のコマンドを入力します。

```
(Cisco Controller) >config 802.11{a|b} cleanair device enable jammer
```

Client Band Select

説明：音声やビデオなどの対話的なトラフィックを WLAN で使用するときは、バンドセレクトを使用しないことをお勧めします。[Fix it Now] をクリックしてバンドセレクトを有効にします。バンドセレクトによって、デュアルバンド（2.4 GHz および 5 GHz）動作が可能なクライアントを、混雑の少ない 5 GHz AP に移動できます。2.4 GHz 帯は、混雑していることがあります。2.4 GHz 帯のクライアントは一般に、Bluetooth デバイス、電子レンジ、およびコードレス電話機からの干渉を受けるだけでなく、他の AP からの同一チャネル干渉も発生します。802.11b/g では、重複しないチャネルが 3 つしかないからです。これらの干渉を防止して、ネットワーク全体のパフォーマンスを向上させるには、コントローラで次のようにバンドセレクトを設定してください。

- バンドセレクトは、デフォルトではグローバルで有効または無効になっています。
- バンドセレクトのしくみは、クライアントへのプローブ応答を規制するというものです。5 GHz チャネルへクライアントを誘導するために、2.4 GHz チャネルでのクライアントへのプローブ応答を遅らせます。
- 音声のバンドセレクトを評価する場合は、特にローミングのパフォーマンスに焦点を当ててください。詳細は、以下を参照してください。
- AP の 5 GHz シグナルが 2.4 GHz シグナルと同じまたはより強い場合、最近のほとんどのモデルのクライアントでは、デフォルトで 5 GHz を優先します。
- 高密度設計では、バンドセレクトを有効にする必要があります。

また、高密度設計では、使用可能な UNII-2 チャネルを調査する必要があります。レーダーによる影響を受けず、クライアントで使用可能なチャネルは、RRM DCA リストに使用可能チャネルとして追加する必要があります。デュアルバンド ローミングは、クライアントによっては低速になる可能性があります。大部分の音声クライアントでローミング動作が低速な場合は、それらのクライアントが 2.4 GHz に留まっている可能性が高くなります。この場合、クライアントは 5 GHzのスキャンで問題を抱えています。一般に、クライアントがローミングすることを決定した場合、現在のチャネルと帯域を最初にスキャンします。クライアントでは通常、シグナルレベルが大幅に高い（例：20 dB）AP や、SNR が大幅に高い AP を検出するためにスキャンします。そのような接続が使用できない場合、クライアントは現在の AP に留まる可能性があります。この場合、2.4 GHz の CU が低く、コール品質が悪くない場合、選択したバンド（周波数帯）を無効にすることも許容されます。しかしながら、推奨される設計は、すべてのデータ レートを有効にし、6 Mbps を必須にして、5 GHz でバンドセレクトを有効にすることです。この後、5 GHz RRM の最小送信電力を、RRM によって設定される 2.4 GHz の平均送信電力よりも 6 dBm 高く設定します。この推奨設定の目的は、クライアントが、より良好な SNR と送信電力のバンド（周波数帯）とチャネルを最初に獲得できるようにすることです。前述のとおり、一般的にクライアントがローミングすることを決定した場合、現在のチャネルとバンド（周波数帯）を最初にスキャンします。このため、クライアントが最初に 5 GHz 帯に参加した場合、5 GHz の送信電力が良好であれば、そのバンド（周波数帯）に留まる可能性が高くなります。5 GHz の SNR レベルは、通常 2.4 GHz よりも高くなります。これは、2.4 GHz には Wi-Fi チャネルが 3 つしかなく、Bluetooth、iBeacon、電子レンジなどのシグナルの干渉の影響を受けやすいためです。デュアルバンド レポーティングでは、802.11k を有効にすることを推奨します。これにより、すべての 802.11k 対応クライアントが、アシステッド ローミングのメリットを享受できます。デュアルバンド レポーティングを有効にすると、クライアントは、クライアントが直接要求したベストの 2.4 GHz/5 GHz AP のリストを受け取ります。ここで、クライアントはほとんどの場合、同じチャネル、次にクライアントが現在使用している同じバンド（周波数帯）の順序で AP のリストを上から検索します。このロジックにより、スキャン時間が短縮され、バッテリーの電力が節約されます。Cisco WLC で 802.11k を有効にしても、802.11k 未対応のクライアントには悪影響を与えません。

[Status]:

準拠：すべての WLAN で有効

非準拠：無効

CLI オプション:

次のコマンドを入力して、バンドセレクトを確認します。

```
(Cisco Controller) >show band-select
```

次のコマンドを入力して、WLAN でバンドセレクトを有効にします。

```
(Cisco Controller) >config wlan band-select allow enable wlan-id
```

DCA Cisco AP Load

説明：負荷条件が変動することによる DCA での頻繁な変更を避けるには、このオプションを無効にします

[Status]：

準拠：[Avoid Cisco AP Load] が両方のバンド（周波数帯）で無効

非準拠：[Avoid Cisco AP Load] がどちらかまたは両方のバンド（周波数帯）で有効

CLI オプション：

このコマンドを入力して、DCA Cisco AP の Load を有効にします。

```
(Cisco Controller) >config advanced 802.11{a|b} channel load disable
```

Event Driven RRM

説明：イベント駆動型の RRM を有効にする必要があります。[Fix it Now] をクリックすると、イベント駆動型 RRM が有効になります。

[Status]：

準拠：有効

非準拠：無効

SSID 数が多い

説明：WLAN の数は 4 以下である必要があります。Cisco WLC で設定された SSID の数は制限することをお勧めします。SSID は（各 AP の無線ごとに）同時に 16 個まで設定できますが、それぞれの WLAN または SSID で個別のプローブ応答とビーコンが必要なため、SSID がさらに追加されるにつれて、RF 環境が低下します。さらに、PDA、Wi-Fi 電話機、バーコード スキャナなどのより小型のワイヤレス ステーションの一部では、大量の BSSID 情報を処理できません。この結果、ロックアップ（動作停止）、リロード、またはアソシエーションの失敗が発生します。また、SSID の数が増えるほど必要なビーコンも増えるため、実際のデータ送信に利用できる RF 時間が減少します。たとえば、企業の場合は 1 ～ 3 個の SSID を設定し、高密度設計の場合は 1 個の SSID を設定することを推奨します。単一の SSID シナリオでは、ユーザごとの VLAN 設定に AAA オーバーライドを利用できます。

[Status]：

準拠：4 以下

非準拠：4 超

CLI オプション：

WLAN の数を確認するには、次のコマンドを入力します。

```
(Cisco Controller) >show wlan summary
```

次のコマンドを入力して、不要な WLAN を無効にします。

```
(Cisco Controller) >config wlan disable wlan-id
```

Wi-Fi Interference（不正 AP の干渉）

説明：不正 AP の干渉により ED-RRM を起動します。不正 AP がデューティ サイクルや脅威値と共に干渉として報告されます。

[Status]：

準拠：Wi-Fi Interference Awareness が両方のバンド（周波数帯）で有効で、デューティ サイクルは 80% 以上

非準拠：Wi-Fi Interference Awareness が両方のバンド（周波数帯）で無効で、デューティ サイクルは 80% 未満

CLI オプション：

Wi-Fi Interference（不正APの干渉）を有効にするには、次のコマンドを入力します。

```
(Cisco Controller) >config advanced {802.11a|b} channel cleanair-event enable
(Cisco Controller) >config advanced {802.11a|b} channel cleanair-event rogue-contribution enable
(Cisco Controller) >config advanced {802.11a|b} channel cleanair-event rogue-contribution duty-cycle 80
```

FRA の有効化

説明：フレキシブル ラジオ アサインメント（FRA）により、5 GHz およびモニタなどの他のロールに自動的に XOR 2.4 GHz Radio を割り当てることができます。Cisco Aironet 2800 や 3800 シリーズ AP など、XOR Radio をサポートする AP であれば、FRA を有効にすることをお勧めします。[Fix it Now] をクリックすると FRA が有効になり、[Restore Default] をクリックすると FRA が無効になり、[Ignore] をクリックすると [FRA Enabled] を無視してベスト プラクティス リストに追加されます（必要に応じて、FRA Enabled を無視するリストからベスト プラクティス リストに戻すこともできます）。

[Status]：

準拠：FRA は有効になっています。

非準拠：FRA は無効になっています。

CLI オプション：

次のコマンドを入力して、FRA を有効にします。

```
(Cisco Controller) >config advanced fra enable
```

ローカル クライアント プロファイリングの有効化

WLC は、クライアントが WLAN にアソシエーションした際の情報からクライアント タイプを決定できます。コントローラは情報のコレクタとして機能し、ISE に必要なデータを最適に送信するか、または WLC のダッシュボード上に直接情報が表示されます。

WLAN 上でローカルのプロファイリングを有効にするには、次のコマンドを入力します。

(Cisco Controller) >config wlan profiling local all enable <WLAN id>

Application Visibility and Control（AVC）

Application Visibility and Control（AVC）は、Network-Based Application Recognition（NBAR）エンジンによるシスコのディープ パケット インスペクション（DPI）技術を使用してアプリケーションを分類し、Wi-Fi ネットワークのアプリケーション レベルの可視化と制御を実現します。アプリケーションが認識されると、AVC 機能によってトラフィックをドロップまたはマークできます。

AVC を使用して、コントローラは 1000 以上のアプリケーションを検出できます。AVC により、リアルタイム分析を実施し、ネットワークの輻輳、コストの掛かるネットワーク リンクの使用、およびインフラストラクチャの更新を削減するためのポリシーを作成することができるようになります。

AVC をサポートしているコントローラは、Cisco 2500 シリーズ コントローラ、Cisco 5500 シリーズ コントローラ、セントラル スイッチング モードの Cisco Flex 7500 シリーズ コントローラ、Cisco 8500 シリーズ コントローラ、および Cisco WiSM2 です。

WLAN で（ベースライン アプリケーション使用率に対して）AVC を有効にするには、次のコマンドを入力します。

(Cisco Controller) >config wlan avc 1 visibility enable

WLAN での AVC 統計情報を表示（WLAN あたりのアプリケーション使用率を表示）するには、次のコマンドを入力します。

(Cisco Controller) >show avc statistics wlan <WLAN id>

一般的なユース ケースでは、トラフィックをマーク/ドロップ/レート制限し、次の例のように、最良のユーザ エクスペリエンスのために、Lync ビデオ/音声通話を行うときには Microsoft Lync トラフィックを優先します。

AVC プロファイルを作成するには、次のコマンドを入力します。

(Cisco Controller) >config avc profile MSLync create

AVC プロファイルに 1 つまたは複数のルールを追加する（Lync Audio を DSCP 46 で、ビデオを DSCP 34 でマークする）には、次のコマンドを入力します。

(Cisco Controller) >config avc profile MSLync rule add application ms-lync-audio mark 46

(Cisco Controller) >config avc profile MSLync rule add application ms-lync-video mark 34

WLAN に AVC プロファイルを適用するには、次のコマンドを入力します。

(Cisco Controller) >config wlan avc <WLAN id> profile MSLync

Youtube をドロップするには、次のコマンドを入力します。

(Cisco Controller) >config avc profile DropYoutube rule add application youtube drop

AVC プロファイルのサマリーを表示するには、次のコマンドを入力します。

(Cisco Controller) >show avc profile summary

```
Profile-Name                    Number of Rules
============                    ===============
AVC-Profile-1                          3
AVC-Profile-2                          0
drop-jabber-video                      1
MSLync                                 2
```

AVC プロファイルの詳細を表示するには、次のコマンドを入力します。

(Cisco Controller) >show avc profile detailed MSLync

```
Application-Name   Application-Group-Name          Action  DSCP  DIR   AVG-RATELIMIT   BURST-RATELIMIT
================   ======================          ======  ====  ===   =============   ===============
ms-lync-audio      business-and-productivity-tools Mark    46    Bidirectional
ms-lync-video      business-and-productivity-tools Mark    34    Bidirectional

Associated WLAN IDs       : 1
Associated Remote LAN IDs :
Associated Guest LAN IDs  :
```

ローカル プロファイリング

コントローラは、HTTP、DHCP などのプロトコルに基づいてデバイスのプロファイリングを実行し、クライアントを識別できます。これはネットワークでのより良い可視性を提供し、コントローラが、ユーザごと、またはデバイスごとのエンドポイントを基にした統計を表示できるようにします。ネットワークの可視性の向上に加えて、コントローラはこの情報を使用して、デバイス ベースのポリシーを確立し、ユーザごと、またはデバイスごとのポリシーを適用できます。

ローカル プロファイリングを確認するには、次のコマンドを入力します。

(Cisco Controller) >show wlan <id>

```
WLAN Identifier.............................. 1
Profile Name................................. employee
Network Name (SSID).......................... employee
Status....................................... Disabled
MAC Filtering................................ Disabled
Broadcast SSID............................... Enabled
AAA Policy Override.......................... Disabled
Network Admission Control
Client Profiling Status
    Radius Profiling ........................ Disabled
     DHCP ................................... Disabled
     HTTP ................................... Disabled
    Local Profiling ......................... Disabled
     DHCP ................................... Disabled
     HTTP ................................... Disabled
```

WLAN 上でローカル プロファイリングを有効にするには、次のコマンドを入力します。

(Cisco Controller) >config wlan profiling local all enable <id>

最適なローミングのための 802.11k の有効化

802.11k 標準では、クライアントは、ローミングの先の候補となる既知のネイバー AP の関連情報（ネイバー レポート）を要求できます。802.11k ネイバー リストを使用すると、アクティブおよびパッシブ スキャンを軽減できます。

802.11k が解決の手助けとなる共通の問題は、たいてい特定の AP に接続し、より近い AP で利用できる非常に良いオプションがあるときですら、その特定の AP から離れようとしない、「スティッキ クライアント」への対処です。

WLAN の 802.11k ネイバー リストを有効にするには、次のコマンドを入力します。

(Cisco Controller) >config wlan assisted-roaming neighbor-list enable <WLAN id>

WLAN のデュアルバンド 802.11k ネイバー リストを有効にするには、次のコマンドを入力します。

(Cisco Controller) >config wlan assisted-roaming dual-list enable <WLAN id>

WLAN の Assisted ローミング予測リスト機能を有効にするには、次のコマンドを入力します。

(Cisco Controller) >config wlan assisted-roaming prediction enable <WLAN id>

動的チャネル幅選択（Dynamic Bandwidth Selection）

- DCA は、ネットワークの最適なチャネルを決定するためのコスト メトリックを評価します。
- DCA は次のものを条件付けしながら最も広いチャネル幅を選択します。
  - 最も高いクライアント データ レート
  - Radio ごとの最も低いチャネル利用率
  - 最小データ再試行/CRC エラー

そして同時に、次のことを回避します。

- 不正 AP
- 非 WiFi 干渉源

- 初めて [Best] を有効にするときは、**config 802.11a channel global restart** コマンドを使用して、DCA を完全に再スタートすることを推奨します。
- DCA の再スタートは影響が大きいので、ネットワークのメンテナンス期間中に行う必要があります。
- 次のコマンドで、チャネル幅を最適（best）に設定します。

  (Cisco Controller) >config advanced 802.11a channel dca chan-width best

Wi-Fi Interference Awareness

WiFi 干渉に対処するため、リリース 8.1 から ED-RRM メトリックに不正 AP の重大度が追加されています。不正 AP が無線空間で干渉している場合、Wi-Fi Interference Awareness は次の DCA サイクルまで待機せずに、ただちにチャネルを変更するため、チャネルのパフォーマンスが向上します。

Wi-Fi Interference Awareness を有効にして、デューティ サイクルを 80% に設定するには、次のコマンドを入力します。

(Cisco Controller) >config advanced 802.11a channel cleanair-event rogue-contribution ?

```
disable      Disable cleanair event-driven RRM rogue contribution
duty-cycle   Set event-driven RRM rogue contribution duty cycle
enable      Enable cleanair event-driven RRM rogue contribution
```

(Cisco Controller) >config advanced 802.11a channel cleanair-event rogue-contribution enable

(Cisco Controller) >config advanced 802.11a channel cleanair-event rogue-contribution duty-cycle 80

モビリティ

モビリティのためのベスト プラクティスは次のとおりです。

- モビリティ グループ内のすべてのコントローラは、仮想インターフェイスに同じ IP アドレス（たとえば 192.0.2.x）が必要です。これはローミングのために重要です。モビリティ グループ内のすべてのコントローラが同じ仮想インターフェイスを使用していない場合、コントローラ間ローミングが動作しているように見えても、ハンドオフが完了せず、クライアントの接続はしばらくの間切断されます。

  インターフェイスの概要を確認するには、次のコマンドを入力します。

  (Cisco Controller) >show interface summary

```
Interface Name      Port   Vlan Id   IP Address       Type     Ap Mgr
-----------------   -----  --------  ---------------  -------  ------
ap-manager           LAG   15        192.168.15.66    Static   Yes
management           LAG   15        192.168.15.65    Static   No
service-port         N/A   N/A       10.48.76.65      Static   No
test                 LAG   50        192.168.50.65    Dynamic  No
virtual              N/A   N/A       192.0.2.1        Static   No
```

- 仮想ゲートウェイ アドレスは、ネットワーク インフラストラクチャ内でルーティングされない必要があります。それはワイヤレス クライアントがコントローラに接続するときに到達可能であることだけが目的で、有線経由での接続はできないからです。

- すべてのコントローラの管理インターフェイス間に IP 接続が存在する必要があります。
- ほとんどの状況で、すべてのコントローラは、同じモビリティ グループ名で設定する必要があります。この規則の例外は、通常は DMZ 内におけるゲストアクセス用のコントローラの展開です。
- グループ名は、PMK/L2 高速ローミング識別子として使用されます。高速ローミング設計の場合、同じグループ名を持つ必要があります。
- Webauth/ゲスト用の展開では、同じモビリティ グループ名を持つ必要はありません。
- 一部の WLC にバグが存在し、それ以外には存在しないことによる不整合な動作に直面しないように、すべての WLC を同じソフトウェア コードのバージョンで実行する方が安全です。ソフトウェア リリース 6.0 以降は、すべてのバージョンがモビリティ目的で相互に互換性があるので、WLC のソフトウェア バージョンを合わせることは必須ではありません。
- 不必要に大きいモビリティ グループを作成しないでください。モビリティ グループには、クライアントが物理的にローミングできる領域内の AP を持つすべてのコントローラだけが含まれる必要があります。たとえば、建物内の AP を持つすべてのコントローラです。いくつかの建物が区切られているシナリオがあれば、複数のモビリティ グループに分割する必要があります。これにより、コントローラに、通信することもないであろう、グループ内の有効なクライアント、不正 AP、AP の大規模なリストを保持する必要がないため、メモリと CPU を節約できます。
- また、フロアごとまたはコントローラごとに AP が存在するように（白黒混在の分散ではなく）、モビリティ グループ内のコントローラ間での AP 分散に対応してみてください。これにより、コントローラ間のローミングが減少し、モビリティ グループのアクティビティへの影響はより小さくなります。
- 1 つのモビリティ グループに複数のコントローラがあるシナリオで、コントローラのリロード後、ネットワークで自身の AP についていくつかの不正 AP アラートが表示されるのは正常な動作です。これは、モビリティ グループ メンバー間で、AP、クライアントおよび不正 AP のリストの更新に時間がかかるため発生します。

モビリティ マルチキャスト モードの設定

モビリティのためのマルチキャスト モードの設定により、クライアントがユニキャストで各コントローラに送信するのではなく、モビリティのピア間のマルチキャストで送信するメッセージをアナウンスすることができます。これは送信にかかる時間を節約し、CPU 使用率を低減し、ネットワーク使用率を向上させます。

注: 各コントローラの管理インターフェイスが異なるサブネット上にある場合は、マルチキャスト トラフィックがコントローラ間を通過することを確認してください。

モビリティ マルチキャスト モードを確認するには、次のコマンドを入力します。

(Cisco Controller) >show mobility summary

```
Mobility Protocol Port.....................16666
Default Mobility Domain.....................rfdemo
Multicast Mode .............................Enabled
Mobility Domain ID for 802.11r..............0x6569
Mobility Keepalive Interval.................10
Mobility Keepalive Count....................3
Mobility Group Members Configured...........2
Mobility Control Message DSCP Value.........0

Controllers configured in the Mobility Group
MAC AddressIP Address Group NameMulticast IP    Status
d0:c2:82:dd:66:a0  10.10.10.5   rfdemo     239.0.2.1    Up
```

モビリティ マルチキャスト モードを設定するには、次のコマンドを入力します。

(Cisco Controller) >config mobility multicast-mode enable <local-multicast-address, e.g. 239.0.2.1>

mDNS ゲートウェイ

Bonjour は、Apple のサービス検出プロトコルで、プリンタや他のコンピュータなどのデバイスと、それらのデバイスがローカル ネットワーク上で提供するサービスを、マルチキャスト ドメイン ネーム システム（mDNS）サービス レコードを使用して検出します。Bonjour は、L3 の境界を越えないリンク ローカル プロトコルです。Bonjour ゲートウェイを使用して、Apple デバイスは、レイヤ 3 境界を越えて（異なる VLAN 間で）、エンド ユーザ デバイスに追加の構成なく、Bonjour サービスを検出できます。

グローバル mDNS スヌーピングを有効/無効にするには、次のコマンドを入力します。

(Cisco Controller) > config mdns snooping enable/disable

WLAN の mDNS サポートを有効/無効にするには、次のコマンドを入力します。

(Cisco Controller) >config wlan mdns-profile enable/disable <wlan id/all>

Fast SSID 変更の有効化

Fast SSID 変更が有効になっている場合、コントローラではクライアントが SSID 間でより高速に移動することができます。Fast SSID が有効になっている場合、クライアント エントリがクリアされず、遅延は適用されません。これは Apple IOS デバイスをサポートするために重要です。

Fast SSID 変更を有効にするには、次のコマンドを入力します。

(Cisco Controller) >config network fast-ssid-change enable

CleanAir の有効化

RF 干渉を効果的に検出し軽減するため、可能な限り CleanAir を有効にします。汎用の DECT 電話、電波妨害装置など、セキュリティ アラートを起動する各干渉源に対しては推奨対策があります。

ネットワーク（802.11b）で CleanAir 設定を確認するには、次のコマンドを入力します。

(Cisco Controller) >show 802.11b cleanair config

ネットワーク（802.11a）で CleanAir 設定を確認するには、次のコマンドを入力します。

(Cisco Controller) >show 802.11a cleanair config

```
Clean Air Solution................................Disabled
Air Quality Settings:
Air Quality Reporting.............................Enabled
Air Quality Reporting Period (min)................15
Air Quality Alarms................................Enabled
Air Quality Alarm Threshold.......................35
Unclassified Interference.........................Disabled
Unclassified Severity Threshold...................20
Interference Device Settings:
Interference Device Reporting.....................Enabled
Interference Device Types:
Bluetooth Link....................................Enabled
Microwave Oven....................................Enabled
802.11 FH.........................................Enabled
Bluetooth Discovery...............................Enabled
TDD Transmitter...................................Enabled
```

802.11 ネットワークで CleanAir 機能を有効にするには、次のコマンドを入力します。

(Cisco Controller) >config 802.11b cleanair enable network

(Cisco Controller) >config 802.11a cleanair enable network

電波妨害装置などの干渉検出を有効にするには、次のコマンドを入力します。

(Cisco Controller) >config 802.11b cleanair device enable jammer

802.11 ネットワークで CleanAir が有効かを確認するには、次のコマンドを入力します。

(Cisco Controller) >show 802.11a cleanair config

(Cisco Controller) >show 802.11b cleanair config

```
Clean Air Solution................................Enabled
Air Quality Settings:
Air Quality Reporting.............................Enabled
Air Quality Reporting Period (min)................15
Air Quality Alarms................................Enabled
Air Quality Alarm Threshold.......................35
Unclassified Interference.........................Disabled
Unclassified Severity Threshold...................20
Interference Device Settings:
Interference Device Reporting.....................Enabled
Interference Device Types:
TDD Transmitter...................................Enabled
Jammer............................................Enabled
Continuous Transmitter............................Enabled
DECT-like Phone...................................Enabled
Video Camera......................................Enabled
```

ハイアベイラビリティ（HA）クライアント/AP SSO の有効化

AP ステートフル スイッチオーバー（AP SSO）

Cisco Wireless LAN Controller（WLC）ネットワーク ソフトウェア リリース バージョン 7.3 および 7.4 の HA AP SSO を使用すると、アクセス ポイント（AP）でアクティブ WLC との CAPWAP トンネルを確立でき、AP データベースのミラー コピーをスタンバイ WLC と共有できます。アクティブ WLC が故障した場合、AP は Discovery 状態にならず、スタンバイ WLC がアクティブ WLC としてネットワークを引き継ぎます。アクティブ状態ではただ 1 つの CAPWAP トンネルが AP と WLC 間で維持されます。Cisco Wireless LAN コントローラ ネットワークに AP SSO サポートが追加されたのは、障害状態によって引き起こされるワイヤレス ネットワークの大規模なダウンタイムを削減することを全体的な目標としています。この障害状態は、ボックス フェールオーバーまたはネットワーク フェールオーバーが原因で発生する可能性があります。

サービスに影響を与えずにハイ アベイラビリティをサポートするには、アクティブ コントローラからスタンバイ コントローラへのクライアントおよび AP のシームレスな遷移をサポートすることが必要となります。リリース 7.5 では、クライアント ステートフル スイッチ オーバー（クライアント SSO）をワイヤレス LAN コントローラでサポートしています。クライアント SSO がサポートされるのは、すでに認証および DHCP フェーズが完了し、トラフィックの送信を始めたクライアントです。クライアント SSO を使用することで、WLC にクライアントが接続したとき（またはクライアントのパラメータが変更されたとき）に、クライアント情報がスタンバイ WLC と同期されます。完全に認証されたクライアント（Run 状態のクライアント）は、スタンバイ側に同期されます。これによって、スイッチオーバー時にクライアントの再アソシエーションが回避され、AP およびクライアントのフェールオーバーがシームレスになります。その結果、クライアント サービスのダウンタイムがゼロになり、SSID の停止もなくなります。

注：詳細については、最新の『Cisco Wireless LAN Controller Configuration Guide』を参照してください（http://www.cisco.com/c/en/us/support/wireless/wireless-lan-controller-software/products-installation-and-configuration-guides-list.html）。

HA 設定を始める前に

両方のコントローラの管理インターフェイスが同じサブネット上にあることを確認します。

ローカルのリダンダンシー IP アドレスおよびピアのリダンダンシー マネジメント IP アドレスを設定します。

(Cisco Controller) > config interface address redundancy-management *ip-addr1* peer-redundancy-management *ip-addr2*

コントローラのロールを設定します。

(Cisco Controller) > config redundancy unit {primary | secondary}

SSO の冗長モードを設定します。

(Cisco Controller) > config redundancy mode sso

両方のコントローラはリブートし、次にアクティブおよびスタンバイホット コントローラのロールをネゴシエートします。

スタンバイ コントローラのルート構成を設定します。

(Cisco Controller) > config redundancy peer-route {add *network-ip-addr ip-mask* | delete *network-ip-addr*}

このコマンドは HA ピア コントローラが使用可能であり、正常に動作している場合だけ実行できます。

スタンバイピア コントローラのピア サービス ポートの IP アドレスとネットマスクを設定します。

(Cisco Controller) > config redundancy interface address peer-service-port *ip-address netmask*

このコマンドは HA ピア コントローラが使用可能であり、正常に動作している場合だけ実行できます。

手動スイッチオーバーを開始します。

(Cisco Controller) > config redundancy force-switchover

手動スイッチオーバーが必要な場合のみこのコマンドを実行します。

冗長タイマーを設定します。

(Cisco Controller) > config redundancy timer {keep-alive-timer *time-in-milliseconds* | peer-search-timer *time-in-seconds*}

コントローラ間の通信の暗号化を設定します。

(Cisco Controller) > config redundancy link-encryption {enable | disable}

インフラストラクチャ

次のインフラストラクチャのベスト プラクティスは、WLC の Advanced UI の RF プラクティス ページに追加されます。

アプリケーションの可視化

説明：アプリケーションの可視化を有効にする必要があります。[Fix it Now] をクリックすると、すべての WLAN でアプリケーションの可視化が有効になります。

[Status]：

準拠：1 つ以上の WLAN で有効

非準拠：すべての WLAN で無効

CLI オプション：

次のコマンドを入力して、WLAN で AVC を有効にします。

(Cisco Controller) >config wlan avc wlan-id visibility enable

Aironet IE の無効化

説明：CCX Aironet IE の機能を無効にする必要があります。[Fix it Now] をクリックすると、CCX Aironet IE が無効になります。Aironet IE とは、接続性の向上のためにシスコのデバイスで使用されるシスコ独自の属性です。この属性には、アクセス ポイント（AP）から WLAN のビーコン応答とプローブ応答で送信される、アクセス ポイント名、負荷、接続しているクライアントの台数などの情報が含まれています。Cisco Client Extensions（CCX）クライアントは、この情報を使用してアソシエートに最適な AP を選択します。CCX ソフトウェアは、CCX 対応クライアント デバイスの製造業者およびベンダーに対してライセンスされます。これらのクライアント上にある CCX コードにより、サードパーティ製クライアント デバイスは、シスコ製の AP と無線で通信できるようになり、他のクライアント デバイスでサポートしていないシスコの機能もサポートできるようになります。これらの機能は、セキュリティの強化、パフォーマンスの向上、高速ローミング、および電源管理に関連しています。Aironet IE は CCX ベースのクライアントのためのオプションですが、一部のタイプのワイヤレス クライアントとの互換性の問題の原因となる可能性があります。WGB および Cisco 音声のためには有効にすることを推奨しますが、通常の実稼働ネットワークの場合、検証した結果によっては Aironet IE を無効にした方がよい場合もあります。

[Status]：

準拠：すべての WLAN で CCX Aironet IE が無効です。

非準拠：1 つ以上の WLAN で CCX Aironet IE が有効です。

CLI のオプション：

特定の WLAN に対して Aironet IE のサポートを無効にするには、次のコマンドを入力します。

(Cisco Controller) >config wlan ccx aironetIeSupport disable wlan-id

内部 DHCP の無効化

説明：内部 DHCP は大規模な展開を目的としたものではなく、社内での検証に使用する必要があります。代わりに外部 DHCP サーバを使用することを推奨します。

[Status]：

準拠：内部 DHCP サーバが無効

非準拠：内部 DHCP サーバは使用中

CLI オプション：

次のコマンドを入力して内部 DHCP を有効にします。

(Cisco Controller) >config interface dhcp management primary ip-address

注：IP アドレスは管理 IP アドレスにはできません。

コントローラのハイアベイラビリティ

説明：ハイアベイラビリティが有効になっている必要があります。冗長モードが設定されていない場合は、HA が有効になっていないと見なされます。

[Status]：

準拠：有効

非準拠：無効

ワイヤレス経由での管理（Management over Wireless）アクセス機能の無効化

説明：Cisco WLAN ソリューションのワイヤレス経由での管理（Management over Wireless）アクセス機能では、Cisco WLAN ソリューション オペレータがワイヤレス クライアントを使用してローカル WLC を監視および設定できます。セキュリティ上の理由から、ワイヤレス経由での管理（Management over Wireless）アクセス機能を無効にする必要があります。[Fix it Now] をクリックすると、ワイヤレス経由での管理（Management over Wireless）アクセス機能が無効になります。

[Status]：

準拠：ワイヤレス経由での管理（Management over Wireless）アクセスは無効

非準拠：ワイヤレス経由での管理（Management over Wireless）アクセスは無効

CLI オプション：

次のコマンドを入力して、ワイヤレス経由での管理（Management over Wireless）アクセスを無効にします。

(Cisco Controller) >config network mgmt-via-wireless disable

Fast SSID

説明：Fast SSID を有効にする必要があります。[Fix it Now] をクリックしてFast SSID を有効にします。

[Status]：

準拠：有効

非準拠：無効

CLI オプション：

次のコマンドを入力して、Fast SSID を有効にします。

(Cisco Controller) >config network fast-ssid-change

管理用 HTTPS

説明：セキュアな Web アクセスを有効にする必要があります。Web アクセスは無効である必要があります。[Fix it Now] をクリックすると、HTTPS が有効になり、HTTP が無効になります。

[Status]：

準拠：HTTPS が有効、HTTP が無効

非準拠：HTTPS が有効、HTTP が有効または HTTPS が無効、HTTP が有効

設定する CLI

ユーザによる http://ip-address を使用した WLC GUI へのアクセスを拒否するために Web モードを無効にするには、次のコマンドを入力します。

(Cisco Controller) >config network webmode disable

ユーザによる https://ip-address を使用した WLC GUI へのアクセスを許可するためにセキュアな Web アクセス モードを有効にするには、次のコマンドを入力します。

(Cisco Controller) >config network secureweb enable

ロード バランシング

説明：音声やビデオなどの双方向のトラフィックを WLAN で使用するときは、ロード バランシングを使用しないことをお勧めします。[Fix it Now] をクリックすると、すべての WLAN でのロード バランシングが有効になり、これはその時点でサービスに影響を与える可能性があります。

[Status]：

準拠：1 つ以上の WLAN で有効

非準拠：すべての WLAN で無効

CLI オプション：

次のコマンドを入力して、WLAN 上でロード バランシングを有効にします。

(Cisco Controller) >config wlan load-balance allow enable wlan-id

ロード バランシング ウィンドウ

説明：クライアントのロード バランシングを有効にしたときは、アグレッシブ ロード バランシング アルゴリズムを避けるために、5 以上のウィンドウ サイズを設定することをお勧めします。

[Status]：

準拠：ロード バランシング ウィンドウが 5 以上

非準拠：ロード バランシング ウィンドウが 5 未満

CLI オプション：

次のコマンドを入力して、ロード バランシング ウィンドウを有効にします。

(Cisco Controller) >config wlan disable wlan-id

(Cisco Controller) >config wlan load-balance allow enable wlan-id

(Cisco Controller) >config load-balancing window client-count-more-than-5

(Cisco Controller) >config wlan enable wlan-id

ローカル プロファイリング

説明：ローカル プロファイリングを有効にする必要があります。[Fix it Now] をクリックすると、すべての WLAN でのローカル プロファイリング（DHCP/HTTP）が有効になり、これはその時点でサービスに影響を与える可能性があります。

[Status]：

準拠：1 つ以上の WLAN で有効

非準拠：すべての WLAN で無効

CLI オプション：

すべての WLAN で ローカル プロファイリング（DHCP/HTTP）を有効にするには、次のコマンドを入力します。

(Cisco Controller) >config wlan profiling local all enable

mDNS ゲートウェイ

説明：mDNS スヌーピングを有効にする必要があります。[Fix it Now] をクリックして mDNS スヌーピングを有効にします。

[Status]：

準拠：有効

非準拠：無効

CLI オプション：

次のコマンドを入力して、mDNS スヌーピングを有効にします。

(Cisco Controller) >config mdns snooping enable

マルチキャスト転送

説明：より少ない帯域幅の使用率でパフォーマンスを最大化するにはマルチキャスト フォワーディング モードを使用します。大規模な IPv6 クライアントのネットワークや、ビデオ ストリーミングや mDNS プロキシなしの mDNS などの重いマルチキャスト アプリケーションは、マルチキャスト モードで大いに恩恵を受けるでしょう。

[Status]：

準拠：有効

非準拠：無効

コントローラでマルチキャスト モードを確認するには、次のコマンドを実行します。

(Cisco Controller) >show network summary

マルチキャスト-マルチキャストの動作を設定するには、次のコマンドを入力します。

(Cisco Controller) >config network multicast mode multicast multicast-group-ip-address

(Cisco Controller) >config network multicast global enable

注：マルチキャスト アドレスは、WLC によって、アクセス ポイント（AP）にトラフィックを転送するために使用されます。マルチキャスト アドレスについて、他のプロトコルによってネットワーク上で使用中のアドレスに一致しないことが重要です。たとえば、224.0.0.251 を使用する場合、いくつかのサード パーティ製のアプリケーションが使用する mDNS と競合します。アドレスはプライベート範囲（239.0.0.0 ～ 239.255.255.255、239.0.0.x および 239.128.0.x は含まれない）にすることをお勧めします。マルチキャスト IP アドレスは各 WLC で別の値に設定されることも重要です。自分の AP と通信する WLC は別の WLC の AP に到達して欲しくありません。

AP が管理インターフェイスで使用されているのとは異なるサブネットワークにある場合、ネットワーク インフラストラクチャは管理インターフェイスのサブネットと AP のサブネットワーク間のマルチ キャスト ルーティングを提供する必要があります。

マルチキャスト モビリティ

説明：WLC が個々の WLC の代わりにすべてのモビリティのピアにメッセージをアナウンスすることができ、CPU とネットワークでの利点があります。各々の管理インターフェイスが異なるサブネット上にある場合、マルチキャスト トラフィックが WLC 間で通過することを確認してください。

[Status]：

準拠：有効

非準拠：無効

CLI のオプション：

次のコマンドを入力して、モビリティ マルチキャスト モードを設定します。

(Cisco Controller) >config mobility multicast-mode enable local-multicast-address

マルチキャスト VLAN

説明：使用中のインターフェイス グループで、無線でのマルチキャストを、定義済みマルチキャスト VLAN 上の単一コピーに限定するように、マルチキャスト VLAN を有効化することをお勧めします。

[Status]：

準拠：マルチキャスト VLAN はインターフェイス グループにマッピングされているすべての WLAN に有効

非準拠：マルチキャスト VLAN はインターフェイス グループにマッピングされている 1 つまたは複数の WLAN に有効ではない

CLI のオプション：

次のコマンドを入力して、マルチキャスト VLAN を有効にします。

(Cisco Controller) >config wlan multicast interface wlan-id enable interface-group

NTP

説明：WLC の時刻を同期するのに NTP サーバを使用する必要があります。Network Time Protocol（NTP）はいくつかの機能にとって非常に重要です。ロケーション、SNMPv3、アクセス ポイントの認証、または MFP のいずれかの機能を使用する場合、WLC での NTP 同期の使用は必須です。WLC では認証ありの NTP との同期がサポートされています。

[Status]：

準拠：設定済み

非準拠：未設定

CLI オプション：

NTP サーバを有効にするには、次のコマンドを入力します。

(Cisco Controller) >config time ntp server ntp-server-index ntp-server-ip-address

NTP 認証を有効にするには、次のコマンドを入力します。

(Cisco Controller) >config time ntp auth enable ntp-server-index

(Cisco Controller) >config time ntp key-auth add key-index

タグ付き管理 VLAN

説明：RMI、HA 用の管理インターフェイス、IPv6、および WGB VLAN サポートをタグ付けすることを強くお勧めします。

[Status]：

準拠：管理 VLAN はタグ付き

非準拠：管理 VLAN はタグなし

CLI のオプション：

次のコマンドを入力して、タグ付き管理 VLAN を有効にします。

(Cisco Controller) >config interface vlan management vlan-id

仮想ゲートウェイ IP

説明：仮想インターフェイスの IP アドレスと RCFC5737 に従って割り当てられたインターネット アドレスの重複を避けることをお勧めします。これには、192.0.2.0/24、198.51.100.0/24、および 203.0.113.0/24 ネットワークの IP アドレスが含まれます。

[Status]：

準拠：仮想 IP アドレスは、割り当てられたインターネット アドレスと重複していない

非準拠：仮想 IP アドレスは、割り当てられたインターネット アドレスと重複している

CLI のオプション：

次のコマンドを入力して、仮想ゲートウェイ IP を有効にします。

(Cisco Controller) >config interface address virtual virtual-ip-address

管理インターフェイス上にない WLAN

説明：動的インターフェイスにマッピングされた非管理 WLAN により、管理トラフィックからユーザ トラフィックを分割することをお勧めします。

[Status]：

準拠：ユーザ WLAN は管理インターフェイスにマッピングされていない

非準拠：1 つまたは複数の WLAN が管理インターフェイスにマップされている

CLI のオプション：

次のコマンドを入力して、管理インターフェイスにない WLAN を有効にします。

(Cisco Controller) >config wlan interface wlan-id interface-name

注：このインターフェイスは管理インターフェイスではありません。

FlexConnect のベスト プラクティス

このセクションでは、FlexConnect のベスト プラクティスのいくつかを示します。

- FlexConnect のブランチ サイトでの展開は、リモート オフィスの WLC とは対照的に、セントラル サイトのコントローラによる、資本コストと運用コストの削減の面で、ブランチ設置プランを削減するのに役立ちます。この結果、消費電力と集中型 IT サポートの削減がもたらされます。また、セントラル サイトでの集中管理、WAN の障害に対する耐障害性、セントラル サイトとリモート サイト間の WAN 使用率の削減という利点も提供します。
- 分散型ブランチ オフィスを展開する場合は、最小 WAN 帯域幅、最大 RTT、最小 MTU、フラグメンテーションのガイドラインなど、次のガイドで取得できる特定の構成要件を考慮する必要があります。

  最新の『Flex 7500 Wireless Branch Controller Deployment Guide』（http://www.cisco.com/c/en/us/support/wireless/wireless-lan-controller-software/products-technical-reference-list.html）を参照してください。
- 使用する AP モデルが FlexConnect をサポートしていることを確認します。AP モデル OEAP600 は、FlexConnect モードをサポートしていません。
- UDP ポート 5246 で CAPWAP 制御チャネルのトラフィックが優先されるように、QoS を設定します。

ローカル スイッチング

- WLAN のローカル スイッチングを有効にして、WAN の障害からの復元性を提供し、WAN 経由のデータ量を減らして、WAN 帯域幅の使用率を減らします。
- ローカル スイッチングは、リソースがローカルからブランチ サイトに存在し、データ トラフィックは WAN リンクを介してコントローラに返送される必要がない展開において便利です。
- FlexConnect の AP をスイッチの 802.1Q トランク ポートに接続します。
- VLAN サポートを有効にします。
- AP のネイティブ VLAN と接続するときは、L2 のネイティブ VLAN の設定は AP の設定と一致しなければなりません。
- ローカルにスイッチングされた WLAN 上の対応する各 VLAN は、対応するスイッチ ポートで許可される必要があります。
- このシナリオのスイッチ設定を次に示します。

```
!
interface GigabitEthernet0/1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 52
 switchport trunk allowed vlan 52,154,155
 switchport mode trunk
 spanning-tree portfast trunk
!
```

- スタンドアロン モードまたはローカル スイッチング モードでは、いくつかの機能が利用できません。ローカル スイッチングを使用する場合は、次の制限事項に注意してください。
  - スタンドアロン モードでの MAC/Web 認証
  - IPv6 L3 モビリティ
  - SXP TrustSec
  - Application Visibility and Control（アプリケーションの可視化と制御）
  - Service Discovery Gateway
  - ネイティブ プロファイリングとポリシーの分類

次の FlexConnect 機能マトリックス ガイドのリストを参照してください。

http://www.cisco.com/en/US/products/ps6366/products_tech_note09186a0080b3690b.shtml

Split Tunneling

- リソースのほとんどがセントラル サイトにあり、クライアント データは一元的にスイッチングされる必要があるが、ローカルからリモート オフィスへの特定のデバイスには、WAN の帯域幅の使用率を減らすためにローカル スイッチングが必要なシナリオの場合、Split Tunneling を設定します。
- これに対する典型的なユースケースは、企業の SSID 上のクライアントがローカル ネットワーク上のデバイス（プリンタ、リモート LAN ポート上の有線マシン、またはパーソナル SSID 上のワイヤレス デバイス）と直接通信でき、CAPWAP を介してパケットを送信することで WAN 帯域幅を消費することがないという、OEAP テレワーカー設定です。
- Central DHCP および Split Tunneling は、AP のルーティング機能を使用します。
- Split Tunneling を展開する場合は、次の制限事項に注意してください。
  - OEAP 600 AP では Split Tunneling はサポートされていません。
  - Central DHCP およびローカル分割 WLAN では、スタティック IP のクライアントはサポートされていません。

VLAN Based セントラル スイッチング

- 動的な決定がローカル スイッチまたはセントラル スイッチで行われる必要があり、データ トラフィックは AAA サーバによって返される VLAN に基づき、その VLAN はブランチ サイトに存在するというシナリオでは、VLAN Basedセントラル スイッチングを使用します。
- AAA サーバによって返され、ブランチ サイト上に存在しない VLAN の場合、トラフィックはセントラルでスイッチングされます。

FlexConnect グループ

次に示すような機能を活用する FlexConnect グループを定義します。

- 音声展開のための CCKM/OKC 高速ローミング
- ローカル バックアップ RADIUS サーバ
- ローカル EAP
- AP イメージのスマート アップグレード
- WLAN-VLAN および VLAN-ACL マッピング

CCKM/OKC 高速ローミング

- FlexConnect グループは、FlexConnect AP がコネクテッド モードまたはスタンドアロンモードであり、クライアントに CCKM/OKC 高速ローミングが必要な場合に使用します。
- この機能により、クライアントが AP から別の AP へローミングする際に、完全な RADIUS EAP 認証を実行する必要がなくなります。
- FlexConnect アクセス ポイントでは、アソシエートする可能性のあるすべてのクライアントに対して CCKM/OKC キャッシュ情報を取得する必要があります。これにより、キャッシュ情報をコントローラに返すことなく、すばやく処理できます。

ローカル バックアップ RADIUS サーバ

- WAN の障害、WLC の障害、および RADIUS サーバの障害を視野に入れ、ブランチの復元力を強化するためにローカル バックアップ RADIUS サーバを設定します。
- この機能は、セントラル サイトとの WAN 遅延が大きいリモート オフィスでも使用されます。
- プライマリ バックアップ RADIUS サーバを設定することも、プライマリとセカンダリの両方のバックアップ RADIUS サーバを設定することもできます。スタンドアロン モードの FlexConnect AP は、バックアップ RADIUS サーバに対して完全な 802.1X 認証を実行するように設定できます。
- これらのサーバは、FlexConnect AP がコントローラに接続されていない場合か、または WLAN がローカル認証用に設定されている場合に使用されます。
- RADIUS/ACS がブランチ内部にある場合、クライアントは WAN が停止している間でも、認証とワイヤレス サービスへのアクセスを行います。
- ローカル バックアップ RADIUS サーバを設定するときは、次の制限事項に注意してください。
  - ローカル バックアップ RADIUS サーバをブランチで使用する場合は、オーセンティケータとして機能するすべての AP の IP アドレスを、この RADIUS サーバに追加する必要があります。

ローカル EAP

- 復元力のレベルを上げるために、FlexConnect グループのローカル EAP サーバを有効にします（EAP-FAST、PEAP、EAP-TLS）。
- ローカル EAP 機能は、FlexConnect バックアップ RADIUS サーバ機能と組み合わせて使用できます。FlexConnect グループにバックアップ RADIUS サーバ機能とローカル認証機能の両方を設定した場合、FlexConnect AP はまず、プライマリ バックアップ RADIUS サーバを使用してクライアントの認証を試行します。次に、セカンダリ バックアップ RADIUS サーバによる認証を試行し（プライマリに到達できない場合）、最後に FlexConnect AP 自体のローカルな EAP サーバによる認証を試行します（プライマリとセカンダリの両方に到達できない場合）。
- FlexConnect AP のローカルの EAP を設定するときは、次の制限事項に注意してください。
  - FlexConnect AP では、最大 100 の静的に設定されたユーザを認証できます。グループ内の各 AP は、そのアクセス ポイントにアソシエートされたクライアントのみを認証します。
  - Active Directory（AD）の統合は、この機能ではサポートされていません。

AP イメージのスマート アップグレード

- AP イメージのスマート アップグレード機能を使用して、ブランチ サイトをアップグレードします。この機能は WAN 帯域幅を節約し、サービスのアップグレードによるダウンタイムを短縮し、WAN を介したダウンロードの失敗のリスクを軽減します。効率的な AP イメージ アップグレードにより、個々の FlexConnect AP のダウンタイムが削減されます。
- マスター AP の選択は、FlexConnect グループおよび各グループの AP モデルごとに行われます。
- ネットワークのアップグレードの推奨されるベスト プラクティスは次のとおりです。
  - コントローラ CLI/GUI または Prime Infrastructure を使用して WLC にイメージをダウンロードします。
  - ブート イメージは、予期しない WLC 再起動の場合にすべての AP が並列にダウンロードされるのを避けるために、セカンダリ（そして新たにアップグレードしたものではない）であることを強制されます。
  - コントローラは、各 FlexConnect グループのマスター AP を選択します。マスター AP は手動で選択することもできます。
  - マスター AP はあらかじめセカンダリ ブート イメージに AP のファームウェアをダウンロードします。WAN の帯域枯渇を低減するために、FlexConnect グループごとにこれをスケジュールします。
  - マスター AP のイメージのダウンロードが完了すると、コントローラにメッセージが送信されます。コントローラは、スレーブ AP にマスター AP から AP のファームウェアを事前にダウンロードするように指示します。
  - 新しいイメージをポイントするように、WLC のブート イメージを変更します。
  - コントローラをリブートします。

WLAN-VLAN および VLAN-ACL マッピング

- FlexConnect グループで WLAN-VLAN マッピングを行うと、各 AP でマッピングを設定する必要がなく、容易に設定できます。たとえば、同一の VLAN 上のローカル スイッチングを行うブランチ サイトのすべての AP に対し WLAN-VLAN マッピングを FlexConnect グループ レベルごとに設定できます。
- FlexConnect グループで VLAN-ACL マッピングを行うと、各 FlexConnect AP でマッピングを設定する必要がなく、容易に設定できます。
- WLAN-VLAN マッピングを使用して AP で VLAN を作成する場合、FlexConnect グループではなく AP に VLAN-ACL を作成する必要があります。

FlexConnect グループでの VLAN サポート/ネイティブ VLAN

- FlexConnect グループのレベルで VLAN サポートおよびネイティブ VLAN を設定し、オーバーライド フラグを使用して、1 つの場所ですべての VLAN 設定を統合します。
- この機能により、ブランチ レベルですべての AP の設定を統合することができ、マッピングの一貫性が提供され、設定が容易になります。
- やむを得ない場合を除き、AP ごとの設定は避けられます。

(Cisco Controller) >config flexconnect group <groupName> vlan <enable / disable>

(Cisco Controller) >config flexconnect group <groupName> vlan native <vlan_id>

(Cisco Controller) >config flexconnect group <groupName> vlan override-native-ap <enable / disable>

VLAN 名の AAA オーバーライド

VLAN 名のオーバーライド機能は、中央の 1 つの RADIUS サーバによって複数のブランチを認証する構成で役立ちます。この展開の要件は、認証プロファイルおよびポリシー ルールに基づいてさまざまなブランチ間でクライアントをさまざまな VLAN にマッピングすることです。

この機能を使用する利点は、RADIUS サーバにとっての要件が、ユーザの役割とそのユーザの論理的な分類を認識することに限られる点です。VLAN の設計の詳細は、VLAN 名と VLAN ID のマッピングの形で抽象化することができます。

VLAN 名テンプレートを作成し、マッピング ルールを次のように追加します。

(Cisco Controller) >config flexconnect vlan-name-id create template1

(Cisco Controller) >config flexconnect vlan-name-id template-entry add template1 Marketing 20

(Cisco Controller) >config flexconnect vlan-name-id apply template1

テンプレートは、別のテンプレートからコピーすることによっても作成できます。

(Cisco Controller) >config flexconnect vlan-name-id create template2 copy template1

テンプレートを FlexConnect グループと関連付けます。

(Cisco Controller) >config flexconnect group FlexGroup1 template-vlan-map add template1

屋外のベスト プラクティス

このセクションでは、設計、展開、およびセキュリティに関する、屋外のベスト プラクティスについて説明します。

設計

RF アクティブ サイト サーベイの実行

屋外の環境は、困難な RF 環境です。避けることができない多くの障害物や干渉が存在します。ネットワークを設計する前の、RF アクティブ サイト サーベイは RF 環境を理解する第一歩です。

シスコのレンジおよびキャパシティの計算ツールを使用したカバレッジ範囲の見積

RF アクティブ サイト サーベイを実行すると、ネットワークのデザイン要件を満たすために必要な屋外のアクセス ポイント数を見積もる必要があります。アクセス ポイントのカバレッジ範囲を見積もるのに最適なツールは WNG カバレッジおよびキャパシティの計算ツールです。

http://173.37.206.125/aspnet_client/system_web/2_0_50727/WNG_Coverage_Capacity_Calculator_V2.08/WNG_Coverage_Capacity_Calculator_V2.08.asp

最適な動作モードの選択

屋外のアクセス ポイントは、複数展開モードで動作でき、各展開モードはさまざまなユースケースに合致します。

ローカル モード：屋外展開に最適なオプションです。Cisco Unified Network 機能、RRM の完全なサポートを提供でき、2.4 GHz および 5 GHz 無線をクライアント アクセスのために排他的に使用できます。各アクセス ポイントに専用のイーサネット接続がある場合は、この展開モードを使わなければなりません。

ブリッジ モード：シスコ ワイヤレス レイヤ 2 プロトコルを活用して、アクセス ポイントが長距離をワイヤレスで接続できるようにします。追加のイーサネット接続が利用できない場合、この展開モードを使用する必要があります。

配置

バックホールに対する DFS チャネルの選択の回避

ブリッジ モードで動作しているときに、ワイヤレス バックホールに使用する 5 GHz ワイヤレス チャネルは手動で選択する必要があります。メッシュ ツリーのバックホール チャネルを選択するときに、可能であればレーダーに使用されるチャネル（DFS チャネル）は避けます。これらのチャネルは規制ドメインごとにリスト化されています。

http://www.cisco.com/c/en/us/products/collateral/wireless/aironet-1300-series/product_data_sheet0900aecd80537b6a.html#wp9005314

各ブリッジ モードのアクセス ポイントの BGN および Preferred Parent の設定

ブリッジ モードで動作しているとき、各アクセス ポイントにはブリッジ グループ名と Preferred Parent を割り当てる必要があります。これはメッシュ ネットワークが毎回同じ順序で収束するのに役立ち、ネットワークは初期設計と合致することができます。

ブリッジ グループ名を設定するには、次のコマンドを入力します。

(Cisco Controller) >config` ap bridgegroupname set BGN-name ap-name

確認するには次のコマンドを実行します。

(Cisco Controller) >show ap config general ap-name

Preferred Parent を設定するには、次のコマンドを入力します。

(Cisco Controller) >config mesh parent ap-name parent_MAC

確認するには次のコマンドを実行します。

(Cisco Controller) >show ap config general ap-name

各 BGN での複数の RAP の展開

メッシュ ネットワークを展開するとき、各アクセス ポイントが WLC と通信するのに複数のパスが必要になります。メッシュ ツリーごとに複数のルート アクセス ポイント（RAP）を持つことによって、複数のパスを追加できます。RAP に障害が発生し、オフラインになると、他のメッシュ アクセス ポイントは同じ BGN で別の RAP に参加するので、WLC と通信するパスは引き続き存続します。

バックホール データ レートを自動に設定する

メッシュ ネットワークを展開するときに、各メッシュ ノードは最も高いバックホール データ レートで通信する必要があります。そのためには、「auto」バックホール データ レートを選択して動的レート調整（DRA）を有効にすることをお勧めします。DRA は、すべてのメッシュ リンクで有効にされる必要があります。

「auto」を有効にするには、次のコマンドを入力します。

(Cisco Controller) > config ap bhrate auto ap-name

確認するには次のコマンドを実行します。

(Cisco Controller) > show ap bhrate ap-name

バックホール チャネル幅を 40 MHz に設定する

メッシュ ネットワークを展開するときは、各メッシュ ノードは最も高いバックホール速度で通信する必要があります。40MHz のバックホール チャネルを有効にすることで、より高速なバックホールが可能になります。

AP あたりのチャネル幅を設定するには、次のコマンドを入力します。

(Cisco Controller) >config 802.11a chan_width ap-name 40

バックホールのリンク シグナル対雑音比（LinkSNR）が 25 dBm よりも大きいことを確認

メッシュ ネットワークの最適なパフォーマンスを確保するため、バックホール リンク品質が良いことを確認します。最適なリンク品質は 40 dBm 以上ですが、これは見通しが良くない展開や長距離のブリッジなどでは常に達成可能なわけではありません。シスコは、LinkSNR に少なくとも 25 dBm 以上を推奨しています。

LinkSNR を確認するには、次のコマンドを入力します。

(Cisco Controller) >show mesh neigh summary ap-name

```
AP Name/Radio       Channel       Rate      Link-Snr      Flags      State
-------------       -------      ------     ---------     -----      ------
RAP_e380            136           m15        33           0x0        UPDATED NEIGH PARENT BEACON
```

または:

(Cisco Controller) >show mesh neigh detail ap-name

```
AP MAC : 1C:AA:07:5F:E3:80  AP Name: RAP_e380
backhaul rate m15
FLAGS : 86F UPDATED NEIGH PARENT BEACON
Neighbor reported by slot: 1
worstDv 0, Ant 0, channel 136, biters 0, ppiters 10
Numroutes 1, snr 0, snrUp 40, snrDown 43, linkSnr 39
adjustedEase 8648576, unadjustedEase 8648576
```

セキュリティ

メッシュ MAC 認証用の外部 Radius サーバの使用

MAC 認証用に外部 Radius サーバを設定する必要があります。これにより、すべてのブリッジ モード アクセス ポイントは、1 つの場所で認証でき、ネットワーク管理が簡素化されます。

外部 Radius サーバのセットアップ方法の詳細は、最新のメッシュ展開ガイド（http://www.cisco.com/c/en/us/support/wireless/wireless-lan-controller-software/products-technical-reference-list.html）を参照してください。

コントローラ ベースの wIPS と不正 AP 検出の有効化

コントローラ ベースの wIPS と不正 AP 検出は、WLC でデフォルトで有効になっています。これにより、ネットワーク管理者が望ましくない不正なアクセス ポイントや潜在的なワイヤレス攻撃者がいるかどうかワイヤレス ネットワークを監視することによって、セキュリティが強化されます。

次の設定を行います。

(Cisco Controller) >config mesh ids-state enable

セキュリティ モードとして EAP の有効化

各メッシュのホップは、すべてのワイヤレス トラフィックを暗号化します。無線トラフィックを暗号化するための最も安全な方法は、外部 Radius サーバで EAP オプションを使用することです。

次の設定を行います。

(Cisco Controller) >config mesh security eap

最適化された WiFi 接続用の Adaptive 11r、11k および 11v

iOS 10 以上を実行している iOS 対応デバイスは、AireOS 8.3 以上を実行しているシスコ ネットワークで Adaptive 11r 機能を識別し、WLAN 上の FT アソシエーションを実行します。シスコ ワイヤレス インフラストラクチャは、非 FT WLAN で FT アソシエーションをネゴシエートできるデバイスから、WLAN 上で FT アソシエーションを行うことを許可します。

- config wlan security ft adaptive enable/disable
- Adaptive 11r が有効な場合、AKM を、FT 802.1x または FT PSK ではなく、802.1x または PSK として有効にします。

さらに、AireOS 8.3 が動作している WLC では、SSID 上で 802.11k および 11v 機能がデフォルトで有効になります。これらの機能により、ローミングすべきタイミングとネイバー AP に関する情報がクライアントに通知され、ローミングが必要な時にスキャニングする時間を無駄にすることがなくなるので、クライアントのローミング状況の改善に役立ちます。iOS デバイスはデュアル バンドをサポートするため、802.11k ネイバー リストは、iOS デバイスに対応してデュアル バンドで更新されます。

優先順位の高い業務アプリの FastLane

Apple iOS デバイスは、IETF の推奨に従って QoS マーキングを行います。AireOS 8.3 が動作している WLC では、Fastlane 機能を有効にすることにより、次のような便利な機能を活用することができます。

WLC QoS 設定はグローバルに最適化され、リアルタイム アプリケーションのサポートが向上し、iOS 10 デバイスでは、WMM TSPEC/TCLAS ネゴシエーションを実行することなくアップストリーム音声トラフィックを送信できます。インフラストラクチャがこれらの端末の音声マーキングに対応します。

QoS プロファイルを iOS 10 デバイスに適用して、アップストリームで QoS マーキングが適用されるアプリケーションと、ベスト エフォートまたはバックグラウンドで送信されるアプリケーションを決定することができます。

config qos Fastlane enable/disable wlan <wlan id>

Apple デバイス

次のベスト プラクティスは、WLC の Advanced UI のベスト プラクティス ページに追加された Apple クライアント デバイスとネットワークに適用されます。

WLAN の設定

説明：WLAN が Apple デバイスに推奨される L2 セキュリティ、QoS および詳細設定で設定されているかどうかをユーザが確認できます。アプリケーションの可視化を有効にする必要があります。

[Status]：

準拠：少なくとも 1 つの WLAN が Apple デバイス用のすべての推奨される WLAN 設定に準拠しています。

非準拠：Apple デバイス用のすべての推奨される WLAN 設定に準拠した WLAN はありません。

CLI オプション：

次のコマンドを入力して、複数の機能を設定する必要があります。

Security

高速移行を有効または適応に設定するには、次のコマンドを入力します。

(Cisco Controller) >config wlan security ft {enable | adaptive enable} wlan-id

FT が有効な場合に、FT PSK を有効にするには、次のコマンドを入力します。

(Cisco Controller) >config wlan security wpa wpa2 enable wlan-id

(Cisco Controller) >config wlan security wpa akm ft psk enable wlan-id

FT が有効な場合に、FT 802.1X を有効にするには、次のコマンドを入力します。

(Cisco Controller) >config wlan security wpa wpa2 enable wlan-id

(Cisco Controller) >config wlan security wpa akm ft 802.1x enable wlan-id

Over-the-DS を無効にするには、次のコマンドを入力します。

(Cisco Controller) >config wlan security ft over-the-ds disable wlan-id

QoS

Fastlane を有効にするには、次のコマンドを入力します。

(Cisco Controller) >config qos fastlane enable wlan-id

WLAN QoS をプラチナ（音声）に設定するには、次のコマンドを入力します。

(Cisco Controller) >config wlan qos wlan-id platinum

AVC プロファイルを有効にして、WLAN の AUTOQOS-AVCPROFILE を適用するには、次のコマンドを入力します。

(Cisco Controller) >config wlan avc wlan-id visibility enable

(Cisco Controller) >config wlan avc wlan-id profile AUTOQOS-AVCPROFILE??

WMM ポリシー設定を必須に設定するには、次のコマンドを入力します。

(Cisco Controller) >config wlan wmm require wlan-id

Advanced

802.11k ネイバー リストまたはデュアル バンドを有効にするには、次のコマンドを入力します。

(Cisco Controller) >config wlan assisted-roaming neighbor-list enable wlan-id

802.11v BSS 移行を有効にするには、次のコマンドを入力します。

(Cisco Controller) >config wlan bss-transition enable wlan-id

WLAN 無線ポリシーをすべてまたは 802.11a または 802.11a/g に設定するには、次のコマンドを入力します。

(Cisco Controller) >config wlan radio wlan-id {all | 802.11a-only | 802.11ag}??

mDNS スヌーピングを有効にするには、次のコマンドを入力します。

(Cisco Controller) >config wlan mdns enable wlan-id

5 GHz の有効化

説明：5 GHz 無線を有効にして、より高速でより干渉の少ないネットワークを Apple デバイスに提供します。

[Status]：
準拠：ネットワーク上で 5 GHz 無線が有効です。

非準拠：ネットワーク上で 5 GHz 無線が無効です。

CLI オプション：
次のコマンドを入力して、ネットワーク上での 5 GHz 無線を有効にします。

(Cisco Controller) >config 802.11a enable network

5 GHz EDCA Fastlane

説明：EDCA プロファイルを Fastlane として設定すると、5 GHz ネットワーク上の Apple デバイスのパフォーマンスを向上させることができます。

[Status]：
準拠：EDCA プロファイル名は Fastlane です。

非準拠：EDCA プロファイル名は Fastlane ではありません。

CLI オプション：
このコマンドを入力して、5 GHz ネットワーク上の Fastlane に EDCA プロファイル名を設定します。

(Cisco Controller) >config advanced 802.11a edca-paramter fastlane??

5 GHz MCS レート

説明：Apple クライアント デバイスのパフォーマンスを向上させるには、5 GHz ネットワーク上のすべての MCS レート（0-31）を有効にする必要があります。

[Status]：
準拠：すべての MCS レートが 5 GHz ネットワークで有効です。

非準拠：MCS レートの一部が 5 GHz ネットワークで無効です。

CLI オプション：
このコマンドを入力して、5 GHz ネットワークで MCS レートを有効にします。

(Cisco Controller) >config 802.11a 11acsupport mcs tx {mcs8 | mcs9} ss {1-4} enable

QoS Trust DSCP

説明：QoS マップと Trust DSCP アップストリームを有効にすることで、Apple クライアント デバイスのパフォーマンスを向上させることができます。

[Status]：

準拠：QoS マップが有効で、Trust DSCP アップストリームが QoS マップ アップストリームに選択されています。

非準拠：QoS マップが無効、または UP to DSCP マップが QoS マップ アップストリームに選択されています。

CLI オプション：

次のコマンドを入力して、QoS マップ値を有効にします。

(Cisco Controller) >config qos qosmap enable

(Cisco Controller) >config qos qosmap trust-dscp-upstream enable

QoS プラチナ プロファイル

説明：ユニキャストとマルチキャストの優先順位は、Apple クライアント デバイスのパフォーマンスを改善するために、プラチナ プロファイルのベスト エフォートである必要があります。

[Status]：

準拠：QoS プラチナ プロファイルのユニキャストとマルチキャストの優先順位はベスト エフォートです。

非準拠：QoS プラチナ プロファイルのユニキャストまたはマルチキャストのいずれかの優先順位がベスト エフォートではありません。?

CLI オプション：

プラチナ プロファイルのベスト エフォートを有効にするには、次のコマンドを入力します。

(Cisco Controller) >config qos priority platinum besteffortbesteffort besteffort

mDNS または Bonjour

説明：Apple クライアント デバイスが、プロジェクタ、プリンタなどの、mDNS サービスをサポートする、ローカル デバイスを識別するために、mDNS または Bonjour スヌーピングやポリシーを有効にします。

[Status]：

準拠：mDNS スヌーピングとポリシーが有効です。

非準拠：いずれかの mDNS スヌーピングまたはポリシー、あるいはその両方が無効です。

CLI オプション：

これらのコマンドを入力して mDNS スヌーピングとポリシーを有効にします。

(Cisco Controller) >config mdns snooping enable

(Cisco Controller) >config mdns policy enable

Optimized Roaming の無効化

説明：Apple デバイスが新しい 802.11r、802.11k、または 802.11v ローミングの改善を使用するため、Optimized Roaming を無効にする必要があります。

[Status]：

準拠：Optimized Roaming が無効です。

非準拠：Optimized Roaming が有効です。

CLI オプション：

次のコマンドを入力して、Optimized Roaming を無効にします。

(Cisco Controller) >config advanced 802.11{a | b} optimized-roaming disable