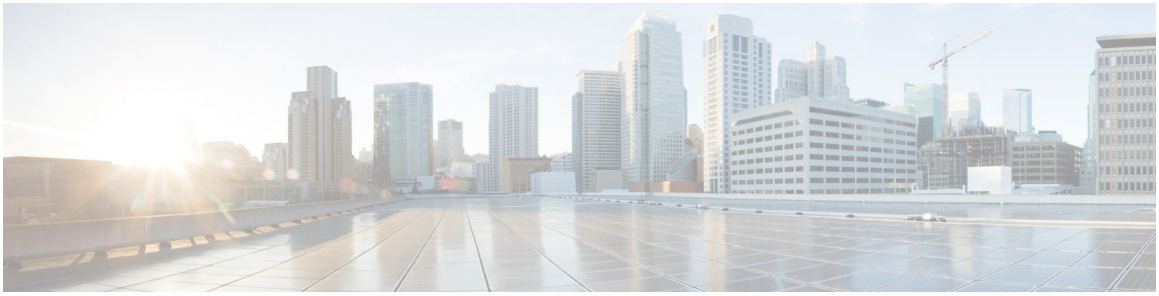


Cisco ワイヤレス LAN コントローラ（WLC）の設定のベスト プラクティス

最終更新日：2014 年 9 月
リリース：Cisco ワイヤレス LAN コントローラ（WLC）の設定のベスト プラクティス、リリース 8.0

はじめに

モビリティの拡大により、ワイヤレス ネットワーク リソースへの期待と利用者の認識は急速に変化してきました。利用者は、ネットワークへのアクセス方法としてワイヤレスを好み、また、ワイヤレス アクセスが唯一の現実的な手段となるケースも少なくありません。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 プラクティスに基づいた設定のヒントを提供します。本ドキュメントは、ワイヤレス ネットワークの多くの実装に当てはまる重要な注意事項について説明することを目的としています。

注 ネットワークにはさまざまな構成があります。そのため、ヒントによっては、実際の環境に該当しない場合もあります。実稼働中のネットワークに何らかの変更を行う場合は、必ず事前に検証してください。

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本的な知識

使用コンポーネント

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いています。

- リリース 8.0 以降のソフトウェアが稼働するシスコ WLC シリーズ。
- Cisco 802.11n および 11ac シリーズ AP。

注 WLC に関するすべての説明は、リリース 8.0 以降のソフトウェアに基づいています。

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

Cisco WLC の設定のベスト プラクティス

ネットワーク設計

以降のセクションでは、ネットワーク設計のベスト プラクティスについて説明します。

AP が接続されるスイッチ ポートでは PortFast を使用する

ローカル モードの AP では、スイッチ ポートに PortFast 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か（switchport host コマンド）、または直接 portfast コマンドで接続します。これにより、AP の参加プロセスが高速化されます。CAPWAP AP は VLAN 間をブリッジしないため、ループが発生する危険性はありません。

インターフェイス ソース（DHCP、SNMP、RADIUS、マルチキャストなど）

CPU が開始するトラフィックのほとんどは、コントローラの管理アドレスから送信されるように設計されています。たとえば、SNMP トラップ、RADIUS 認証要求、マルチキャスト転送などがこれに該当します。

- デフォルトでこのルールの例外となるのは、DHCP 関連のトラフィックです。各 SSID に対して「RADIUS インターフェイス上書き」を有効にすることもできます。この場合、この WLAN の RADIUS トラフィックはダイナミック インターフェイスから送信されます。ただし、これにより、個人所有デバイス持ち込み（BYOD）のフローと認可変更（CoA）との間で設計上の問題が発生します。
- ファイアウォール ポリシーを設定したり、ネットワークトポロジを設計する際には、各 SSID に対する「RADIUS インターフェイス上書き」の有効化を考慮に入れることが大切です。ダイナミック インターフェイスは、コントローラ CPU から到達可能にする必要があるサーバと同じサブ ネットワーク内に設定しないようにすることが重要です。たとえば、RADIUS サーバで非対称ルーティングの問題が生じる可能性があります。
- RADIUS は、RADIUS 上書き機能を使用して、ダイナミック インターフェイスから取得できます。これは、特定のトポロジで必要な場合のみ使用します。

推奨されるスイッチポート モードと VLAN プルーニング

ローカル モードの AP では、スイッチポートを常に「アクセス モード」で設定します。FlexConnect モード（ローカル スイッチングを行う）の AP と WLC に接続されたトランク モードのスイッチポートでは、FlexConnect AP と WLC 上で設定された VLAN のみを許可するように VLAN をプルーニングします。さらに、それらのトランクに対して **switchport nonegotiate** コマンドを実行することにより、スイッチポート上でダイナミック トランキング プロトコル（DTP）を無効にします。これにより、DTP をサポートしない AP/WLC が無駄にフレームを処理することがなくなり、さらに、DTP をサポートしないデバイスとのネゴシエーションにスイッチのリソースを浪費しなくて済むようになります。

ネットワーク接続

ネットワーク接続に関するベスト プラクティスを以下に示します。

ほとんどのコントローラの設定は、すぐに適用されますが、以下の設定を変更した場合は、コントローラをリロードすることを推奨します。

- 管理用アドレス
- SNMP の設定
- HTTPS 暗号化設定
- LAG モード（有効または無効、この場合はリロードが必須）

管理インターフェイスでは TAG タギングを使用する

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ています。これは、HA シナリオでサポートされる唯一のモードであるためです。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との間で送受信されるパケットは、WLC が接続されているトランク ポートのネイティブ VLAN で送信されます。管理インターフェイスを異なる VLAN に設定する場合は、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>

設定した VLAN はスイッチポートで許可され、トランクで（ネイティブ以外の VLAN に）タグ付けされていることを確認してください。

- コントローラに接続されているすべてのトランク ポートで、使用されていない VLAN を除外します。

  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、さらに VLAN 40 と VLAN 50 が 2 つの異なる WLAN 用に使用されている場合、スイッチ側で次の設定コマンドを使用します。

  Switch# switchport trunk allowed vlans 20,40,50

  - インターフェイスのアドレスを 0.0.0.0 のままにしないでください。未設定のサービス ポートなどがこれに該当します。コントローラでの DHCP の処理に影響が生じることがあります。

    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がスイッチ側で同じレイヤ 2 設定である場合を除き、リンク集約（LAG）を使用しないでください。これは、たとえば、あるポートでは一部の VLAN がフィルタされ、他のポートではフィルタされなくなる、といった事態を回避するためです。
- LAG の使用中、トラフィックは同じデータ プレーンで受信する必要があります。コントローラは、ネットワークから受信するトラフィックのロード バランシングについてはスイッチに依存し、1 つの AP に属するトラフィックが、常に同じデータ プレーンに入るものと想定します。5500 シリーズは、1 つのデータ プレーンを備えており、トラフィックは常に同じデータ プレーンに到着します。
- WISM2 と 8500 シリーズは、2 つのデータ プレーンを備えた WLC です。トラフィックは、可能な限り同じデータ プレーンで受信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十分な帯域幅がありますが、 帯域幅が制限されている場合、トラフィックがドロップされる可能性があります。

  EtherChannel のロード 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
  ```

  スイッチ構成を変更するには、次のコマンドを実行します（IOS）。

  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 以降では、PFC3C モード シャーシ用に、負荷分散で VLAN を除外するオプションがあります。この機能を実装するには、**port-channel load-balance src-dst-ip exclude vlan** コマンドを使用します。この機能を使用すると、LAP に属するトラフィックが同じポートで受信されるようになります。
- VSS、スタック スイッチ（3750/2960）または Nexus VPC を使用している場合、LAG は、IP パケットのフラグメントが同じポートに送信される場合に限り動作します。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、物理ポートごとに AP マネージャを作成し、LAG を無効にする必要があります。これにより、冗長性およびスケーラビリティが提供されます。
- 古いソフトウェア バージョンでは許可されていたとしても、可能な限り、AP マネージャ用インターフェイスにバックアップ ポートを作成しないでください。このドキュメントですでに説明したように、複数の AP マネージャ インターフェイスによって冗長性が実現されます。

マルチキャスト転送モードを使用する

帯域幅使用率を下げて最高のパフォーマンスを得るには、マルチキャスト転送モードを使用します。IPV6 クライアントが多いネットワークでは、ビデオ ストリーミングや mDNS プロキシを使用しない Bonjour などの多くの帯域幅を消費するマルチキャスト アプリケーションで、マルチキャスト モードのメリットを享受できます。

コントローラでマルチキャスト モード設定を確認するには、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
```

マルチキャスト-マルチキャスト操作を設定するには、WLC のコマンド ラインで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

- コントローラでは、トラフィックをアクセス ポイント（AP）に転送するためにマルチキャスト アドレスを使用します。マルチキャスト アドレスは、ネットワーク上で他のプロトコルが使用しているアドレスと一致させないようにすることが重要です。たとえば、224.0.0.251 を使用する場合は、一部のサードパーティ アプリケーションで使用されている mDNS が正常に機能しなくなります。シスコでは、マルチキャスト アドレスは、プライベートのアドレス範囲（239.0.0.x および 239.128.0.x を除く 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 アドレスは、WLC ごとに異なる値に設定することも重要です。自身の AP と通信する WLC が別の WLC の AP に到達しないようにするためです。
- AP が管理インターフェイスとは異なるサブネットワークにある場合、管理インターフェイスのサブネットワークと 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、ネットワーク インフラストラクチャがサポートする必要があります。

内部 DHCP を無効にする

コントローラには内部 DHCP サーバを提供する機能が備わっています。この機能は非常に限定的であり、ラボ環境などでの単純なデモンストレーションや概念検証用に使用するものです。この機能は、企業の実稼働ネットワークでは使用しないことを推奨します。

内部 DHCP サーバが使用されているかどうかは、インターフェイスの設定を表示した際に、プライマリ DHCP サーバのアドレスが管理 IP アドレスと同じかどうかで確認できます。以下に例を示します。

(Cisco Controller) >show dhcp summary

```
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）を実稼働環境の DHCP サーバに変更するには、以下のコマンドを実行します。

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

また、既存の内部 DHCP スコープを無効にするか、または削除しておくと安全です。まず、内部 DHCP スコープを確認します。

(Cisco Controller) >show dhcp summary

```
Scope Name                  Enabled          Address Range
Scope1                      Yes              10.10.10.100 -> 10.10.10.150
Either disable the scope:
```

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

または

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

セキュリティ

以降のセクションでは、セキュリティのベスト プラクティスについて説明します。

ローカル EAP を無効にする

ローカル EAP 認証方法を使用すると、ユーザとワイヤレス クライアントをコントローラでローカルに認証できます。内部 DHCP 機能と同様に、ローカル EAP は、ラボ環境での単純なデモンストレーションや概念実証を目的とする簡便な機能です。したがって、ローカル EAP を企業の実稼働環境で使用することは推奨されません。ローカル EAP は、無効にするか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 と 802.1X を併用する WLAN

コントローラと AP は、WiFi Protected Access（WPA）と WPA2 を併用する SSID の WLAN をサポートしていますが、一部のワイヤレス クライアントのドライバでは複雑な SSID 設定を処理できないことがよくあります。WPA2 は、可能な限り Advanced Encryption Standard（AES）とだけ併用することを推奨します。ただし、標準かつ必須の WiFi Alliance 認定プロセスにより、今後のソフトウェア バージョンでは TKIP のサポートが求められます。SSID のセキュリティ ポリシーはシンプルにするようにしてください。たとえば、WPA と Temporal Key Integrity Protocol（TKIP）、WPA2 と Advanced Encryption Standard（AES）を、同じ WLAN または SSID で併用しないようにしてください。シスコでは、TKIP を推奨していないため、TKIP は WEP と併用するか、可能であれば TKIP から PEAP に移行することを推奨します。

WLAN で WPA2 と 802.1X 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 wpa enable <WLAN id>

指定した WPA2/802.1X WLAN 上で、RADIUS 認証サーバを設定します。

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

指定した WPA2/802.1X WLAN 上で、RADIUS アカウンティング サーバを設定します。

(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 オーバーライドを使用する

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け、サブネットワークごとに異なるセキュリティ ポリシーを使用するなど、ID ベースのネットワーク サービスを設計する場合は、1 つまたは 2 つの WLAN で AAA オーバーライド機能を使用します。AAA オーバーライド機能により、ユーザ別の設定を行うことが可能です。たとえば、ユーザを異なる VLAN の特定のダイナミック インターフェイスに移動したり、ユーザ別のアクセス 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>

次のコマンドを実行して、WLAN の設定を確認します。

(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
```

RADIUS のタイムアウト値を短く設定する

802.1x を利用する大規模またはビジーなネットワークでは、RADIUS のタイムアウト値をできるだけ短く設定することを推奨します。タイムアウト値を長く設定すると、フレームの再送が RADIUS 用のキューに長く保持されます。ネットワーク キャパシティとキューの使用率によっては、タイムアウト値が長いと再送の失敗率が高まる可能性があります。また、タイムアウト値が長いと、RADIUS サーバのダウンの検出に通常より時間がかかる場合があります。認証回数が多いネットワークを導入する場合、コントローラのキャパシティを有効利用するため、タイムアウト値は短く設定すべきです。タイムアウト値を短くすると、応答のない RADIUS サーバからの WLC の復帰が早くなります。ただし、RADIUS NAC（ISE）と低速な WAN 上での RADIUS では、タイムアウト値を長めに設定（5 秒）することを推奨します。

次の例では、デフォルトのタイムアウト値は 2 秒です。これは RADIUS のフェールオーバーには十分短い時間ですが、Extensible Authentication Protocol-Transport Layer Security（EAP-TLS）の認証には十分ではありません。RADIUS サーバが外部データベース（Active Directory、NAC、SQL など）と通信する場合、指定したタイムアウト時間内に処理が終わる必要があります。

RADIUS のタイムアウト値を確認するには、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 のタイムアウト値を確認するには、次のコマンドを実行します。

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

EAP アイデンティティ要求タイムアウト

コントローラで、EAP アイデンティティ要求のデフォルト タイムアウト値を増やす必要がある場合があります。たとえば、スマート カードにワンタイム パスワード（OTP）を実装する場合など、アイデンティティの要求にユーザとの対話が必要です。自律 AP のデフォルトのタイムアウト値は 30 秒です。自律ワイヤレス ネットワークから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際はこの点に注意してください。

デフォルトのタイムアウト値を表示するには、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..... 3,600
```

タイムアウト値（秒）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 タイムアウトと最大再試行回数

IP 7920 電話機などの音声クライアントでは、EAPol タイムアウト値をできるだけ小さくすることを推奨します。RF 環境が最適化されていない場合は、最大再試行回数を増やす必要があります。

(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..... 3,600
```

EAPoL タイムアウト値を設定するには、次のコマンドを実行します。

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

EAPoL 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 eapol-key-retries <retries>

EAP 要求タイムアウトと最大再試行回数

クライアントの種類によっては、短時間では動作できないデバイスが一部含まれている場合もありますが、残りのデバイスについては、タイムアウト時間を短くし、再試行回数を増やして、良好ではない RF 環境での回復を早めるほうが適切な場合があります。これは、PEAP/GTC などの内部 EAP 方式で認証するクライアントにも当てはまります。

デフォルトのタイムアウト値を表示するには、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..... 3,600
```

EAP 要求タイムアウト値を設定するには、次のコマンドを実行します。

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

EAP 要求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 タイムスタンプの検証

CCKM の検証を 5 秒に変更し、ピコセルまたはローミングの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+ の管理タイムアウト

再認証が繰り返される場合や、プライマリ サーバがアクティブで到達可能であるにもかかわらずコントローラがバックアップ サーバにフォールバックする場合は、TACACS+ 認証、許可、およびアカウンティング サーバの再送タイムアウト値を長くすることを推奨します。これは、ワンタイム パスワード（OTP）と併用する場合に特に当てはまります。

(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+ 許可再送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 のデフォルト ユーザを変更する

SNMPv3 のデフォルト ユーザを確認します。コントローラには、無効または変更の必要があるデフォルトのユーザ名が設定されています。

SNMPv3 のデフォルト 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 のデフォルト 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 の設定が、コントローラと Wireless Control System（WCS）、Network Control System（NCS）、Prime インフラストラクチャ（PI）の間で一致していることを確認してください。また、セキュリティ ポリシーに合った暗号化とハッシュ キーを使用する必要があります。

Network Time Protocol（NTP）を有効にする

ネットワーク タイム プロトコル（NTP）は一部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、または MFP のいずれかの機能を使用する場合は、コントローラで NTP による同期を行う必要があります。WLC は、認証を使用して NTP による同期をサポートします。

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

確認するには、traplog 内のエントリを確認します。

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 高速移行を有効にする

802.11r は高速なローミングのための IEEE 規格であり、ローミング方法の 1 つです。ターゲット AP（つまり、クライアントが接続しようとしている次の AP）との初期認証ハンドシェイクは、クライアントがターゲット AP にアソシエートする前に実行されます。これを高速移行（FT）と呼びます。デフォルトでは、高速移行は無効です。

注 802.11r に対応していないクライアントは、このWLAN に接続できなくなります。クライアントが 802.11r に対応していることを確認してください（Apple デバイスの場合はバージョン 6 以降、など）。

802.11r すなわち高速移行（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

高度なセキュリティが必要な場合は、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ように設定してください。

WLAN で DHCP Required オプションを指定すると、クライアントが WLAN へのアソシエートを行うたびに、DHCP アドレスの要求と更新が強制され、ネットワークへの各トラフィックの送受信は、その後で許可されるように設定できます。これにより、使用される IP アドレスをセキュリティ面でより厳格に制御できます。ただし、トラフィックが再度の通過を許可されるまでのローミングの合計時間に影響を与える可能性があります。

また、リース時間切れになるまで DHCP 更新を行わないように設定したクライアント実装でも影響が出る可能性があります。これはクライアントの種類によって変わります。たとえば、Cisco 7921 や 7925 の電話機では、このオプションが有効になっていると、ローミングの際に音声に関する問題が発生することがあります。これはコントローラで DHCP の処理が完了するまで音声やシグナリングのトラフィックの通過が許可されないためです。もう 1 つの例として、Android と一部の Linux ディストリビューションを挙げることができます。これらの OS では、DHCP の更新を、ローミング時ではなくリース時間の半分の長さで実行します。これにより、クライアントの期限が切れたときに問題が起きる可能性があります。

一部のサードパーティのプリンタ サーバも、これに該当す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存在する場合は、このオプションを使用しないことを推奨します。これは、厳密な制御によって、DHCP のクライアント側の実装方式に関連する接続性の問題が発生する可能性があるためです。

WLAN 設定で DHCP Required の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
```

不正の管理と検出

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ります。ネットワークの管理者に必要なのは、不明なデバイスのスキャンだけではありません。不正や侵入者の脅威を自動的かつリアルタイムに検出し、無効化、特定、および管理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 テキストまたは他の DoS 攻撃や中間者攻撃により、ワイヤレス 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することが可能になります。これに成功すると、ハッカーは、クリア ツー センド（CTS）フレームを送信できるようになります。CTS フレームは AP を模倣し、特定のワイヤレス LAN クライアント アダプタだけに送信を指示し、他の全アダプタには待機を指示します。その結果、正規のクライアントはワイヤレス LAN リソースにアクセスできなくなります。そのため、無線 LAN のサービス プロバイダーにとっては、サービス提供範囲から不正な AP を排除することは喫緊の課題となります。

一般の企業にとっても、不正な AP を検出し、セキュリティリスクを最小化することは重要な課題です。しかし、OEAP 導入、オープンエアーの会場やスタジアム、市全域、屋外など、不正検出が不要なシナリオもあります。屋外のメッシュ AP を使用して不正を検出したとしても、手間の割にメリットはほとんどありません。さらに、不正の自動封じ込め処理について評価する（または利用をやめる）ことは極めて重要です。自動的に動作するままにしておくと、法的な問題や責任が発生する可能性があるからです。

以降のセクションに挙げたいくつかのベスト プラクティスを利用すれば、不正な AP リストを効率的に管理できるようになります。

不正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 [英語]

悪意のある不正 AP に対する適切なルールを定義する

悪意のある不正 AP のルールを日常的に定義します。即時の対応や低減措置が必要となるメジャーおよびクリティカルな不正 AP 用にアラームを設定し、優先順位を付けます。

クリティカルまたはメジャーな不正 AP アラームとは、「悪意のあるもの」として分類され、ネットワーク上で検出されます。

各不正ルールは、1 つ以上の条件（必須または推奨）で構成されます。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の管理対象 SSID を使用するすべての不正 AP は、「悪意がある」ものと定義されます。管理者は、この脅威を調査し、リスクを軽減する必要があります。
- 最小 RSSI >-70 dBm（推奨）：通常この条件は、不明な不正 AP が施設境界内にあることを示し、ワイヤレス ネットワークに対して潜在的な干渉を与える可能性があります。

  このルールは、自社だけの独立した建物を所有し、境界が安全に保護された企業でのみ導入が推奨されます。

  小売店や、さまざまな入居者が利用する建物など、WiFi 信号が混ざり合う環境では、推奨されません。
- ユーザが設定した SSID またはサブストリング SSID（推奨）は、実稼働 SSID（管理対象 SSID）内でさまざまな文字のバリエーションや組み合わせを使用する SSID を監視します。

ルールの一致条件に対して推奨されるアクションを以下に挙げます。

- 「必須」条件に一致する悪意のある不正 AP については、アクションとして「Contain（封じ込め）」を設定します。
- 各ルールに対して 1 つだけ条件を設定し、関連付けられた条件が直感的にわかるルール名を付け、管理者が簡単に特定およびトラブルシューティングを行えるようにします。
- 「オプション」条件に一致する悪意のある不正 AP については、法律と複雑に関わるため、アクションとして「Contain（封じ込め）」を設定することは推奨されません。代わりに、アクションとして「Alert（アラート）」を設定します。

注 不正 AP の封じ込めには法的な意味合いがあります。しかしながら、実稼働の SSID と同じ SSID を使用する不正 AP は、自動封じ込め処理の例外となる場合もあります。正規のワイヤレス クライアントを引き寄せる不正 AP の潜在的な脅威を低減するうえで、封じ込めを自動で行わないほうがよいケースもありうるからです。

友好的な不正 AP を特定して定期的にリストを更新する

調査後、友好的とわかった不正 AP を「未分類」の不正 AP リストから定期的に（毎週または毎月）削除します。

友好的な不正 AP の例としては、以下のものが挙げられます。

- 組織内の既知の友好的な不正 AP。たとえば、ラボや施設境界内の AP、または、友好的なリストにインポートされている既知の AP MAC など。
- 既知の外部の友好的な不正 AP。たとえば、ベンダーが共有する会場や隣接する小売店など。

分類されていない不正 AP に対する最善の努力

デフォルトでは、定義された分類ルールを満たしていない不正 AP アラームは、重大度「マイナー」で「未分類」として表示されます。このリストが大きくなり、PI で管理しにくくなる可能性があります。たとえば、MiFi デバイスのように、短い期間だけ検出される一時的な不正 AP があります。これらの不正 AP は、有線ネットワーク上で検出されない場合、日常的に監視する必要はありません。代わりに、以下のことを行います。

- 自動スイッチポートトレースなど、自動化された不正 AP 低減メカニズムを実装します。有線ネットワークで見つかった場合は、クリティカル アラームが作動します。
- 月または四半期に一度、未分類の不正 AP に関するレポートを実行し、それらの中から未知の友好的な AP を見つけます。

自動スイッチポートトレース（SPT）を不正 AP 低減スキームとして実装する

不正 AP 低減のために、自動 SPT の実装を推奨します。これは、無線で受信した不正 AP の無線 MAC アドレスを、有線ネットワーク側のイーサネット MAC アドレスに関連付けるためのものです。一致が見つかると、PI に「Found On Network（ネットワーク上で検出）」として報告されます。

- 自動 SPT が開始されると、すべての不正 AP 無線 MAC アドレスが、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 アドレスに対し、フラット レベルで照合されます。
- 重大度が「マイナー」なアラームに対しては、自動 SPT の有効化により低減スキームが発動されるため、安全な管理が可能になります。

AP 上で検出された不正を確認するには、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.................  2,000
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
```

不正設定

AP 上の不正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 上で不正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

RSSI が弱い不正 AP は、検出されたということ以外、ネットワーク管理者にとって価値のある情報を提供しません。RSSI が弱い不正 AP は、RSSI が強い不正 AP よりも、無線ネットワークへの脅威が小さくなります。RSSI が弱い不正 AP が多すぎると、Prime Infrastructure の GUI が乱雑になり、不正 AP の低減が困難になります。これを避けるには、AP が不正 AP を報告するための最小 RSSI 値（**Minimum RSSI for Rogue Classification**）を調整します。

最小 RSSI を -70 dBm として不正 AP 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

不正検出セキュリティレベルを低く（自動封じ込めなし）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

不正ルール

追加の条件セットに対して不正ルールを作成します。たとえば、次のコマンドを実行して「rule1」を作成します。

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

次のコマンドを実行して、ルールを有効にします。

(Cisco Controller) >config rogue rule enable rule1

ルールの要約を確認するには、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
```

1 つの不正ルールに条件を 6 つまで追加できます。これは CLI の例です。不正管理のベスト プラクティス ガイダンスについては、「不正の管理と検出」のセクションを参照してください。

条件ベースのルールを追加することで、ネットワーク上でスプーフィングを行っているユーザを容易に検出できます。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 名に基づく条件を追加します。

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

最小 RSSI（たとえば -70 dBm）に基づく条件を追加します。

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

不正 AP が検出されている期間（秒単位。たとえば 120 秒）に基づく条件を追加します。

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

不正ルールの条件を確認します。

(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 デバイスは、素早く簡単に相互に直接接続して、印刷、同期、コンテンツ共有などを行うことができます。しかし、デバイスがインフラストラクチャと Personal Area Network（PAN）の両方に同時に接続している場合、ワイヤレス ネットワークでセキュリティ上の問題が発生する可能性があります。シスコでは、セキュリティ ホールを防ぐために、Wi-Fi Direct クライアントを禁止することを推奨しています。

Wi-Fi Direct クライアントが WLAN にアソシエートするのを禁止するには、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 スキャン

ローカル モード、FlexConnect モード、モニタ モードの AP の場合、不正をスキャンするチャネルを選択できるオプションが RRM の設定にあります。設定に応じて、AP はすべてのチャネル、カントリー チャネル、または DCA チャネルで不正をスキャンします。以下では、それぞれの利点を簡単に説明します。

- セキュリティを高めるためには、すべてのチャネルを選択します。
- パフォーマンスへの影響を避けたい場合は、最低限のスキャンを行う DCA チャネルを選択します。
- パフォーマンスとセキュリティのバランスをとるには、カントリー チャネル オプションを選択します。

すべてのチャネルに対し、不正検出のための 5 GHz チャネル スキャンを設定するには、次のコマンドを実行します。

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

国番号を指定した 2.4 GHz モニタ チャネル スキャンを設定するには、次のコマンドを実行します。

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

一時的な間隔値を設定して不正をスキャンする

一時的な間隔値を使用して、AP が不正をスキャンする間隔を制御できます。また、AP は、一時的に設定した間隔値で、不正のフィルタリングを行うこともできます。

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レポートが短くなる。
- 一時的不正エントリをコントローラで回避できる。
- 一時的不正への不要なメモリ割り当てを回避できる。

一時的な間隔値を 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

アドホックな不正検出を有効にする

アドホック不正検出は、一般的な不正検出と同様、セキュリティが必要な、企業などの特定シナリオにおいて理想的な方法です。ただし、オープンエアーの会場やスタジアム、市全域、屋外などのシナリオでは価値がありません。

アドホックな不正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

不正クライアントに対して AAA 検証を有効にする

不正クライアントに対して AAA 検証を有効にすると、WLC は、クライアントが AAA サーバ上に存在することを確実かつ継続的にチェックし、正当または悪意あるものとしてマーキングします。

(Cisco Controller) >config rogue client aaa enable

不正クライアントの MSE 検証を有効にする

Mobility Services Engine（MSE）が内蔵されていて、利用可能な場合、収集したクライアント データベース内の情報を共有し、WLC によるクライアントの正否の検証をサポートできます。

不正クライアントが正当かどうかを確認するために、MSE の使用を有効にします（使用できる場合）。

(Cisco Controller) >config rogue client mse enable

ワイヤレスまたは RF

ワイヤレス導入を行う場合、ワイヤレス クライアントに適正品質のサービスを提供できるように、必ず適切なサイト サーベイを実施します。音声やロケーション導入の要件は、データ サービスの要件よりも厳格です。Auto RF はチャネルや出力の設定管理には有効ですが、不適切な RF 設計を修正することはできません。

サイト サーベイを行う際は、実際のネットワークで使用するデバイスと出力や伝搬動作が同じデバイスを使用する必要があります。たとえば、構築するネットワークにおいて、最新のデュアル無線と 802.11a/b/g/n および 802.11ac を使用する場合、古い無指向性アンテナと 802.11b/g の組み合わせでカバレッジを調査すべきではありません。

サイト サーベイは、顧客が設置予定の AP モデルで行う必要があります。AP の向きと高さは、実際の設置状態に合わせる必要があります。AP のデータ レートは、顧客のアプリケーション、帯域幅、およびカバレッジ要件に必要なレートに設定する必要があります。2.4 GHz、1 Mbps のデータ レートでカバレッジ エリアを測定しないようにしてください。ネットワーク設計の主な目的が、カバレッジの各エリアで、30 ユーザ、5 GHz、9 Mbps のデータ レート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 デバイスで 5 GHz、9 Mbps のデータ レートのみを有効にしてカバレッジ テストを実行してください。次に、テスト ネットワーク クライアントに対し、AP で -67 dBm の受信信号強度表示（RSSI）を測定します。その際、AP とクライアントの間でアクティブなデータ トラフィックがある状態を保ちます。RF リンクの品質が高いと、信号対雑音比（SNR）が高くなり、チャネル使用率（CU）パーセンテージが低くなります。RSSI、SNR、CU の値は、WLC のクライアント ページと AP 情報ページにあります。

低データ レートを無効にする

データ レートを無効または有効にするためのプロセスは、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は、低いデータ レートを 1 つずつ無効にしていくことを推奨します。ACK やビーコンなどの管理フレームは、最低の必須レート（一般に 1 Mbps）で送信されるため、全体のスループットが落ちます。最低の必須レートが最も無線通信時間を消費するからです。

クライアントが再送時にレートをより早くダウンシフトできるように、あまり多くのデータ レートをサポートしないようにしてください。一般に、クライアントは、最も高速なデータ レートで送信を試み、フレームが届かない場合は、次に低いデータ レートで再送し、フレームが届くまでこれを繰り返します。サポートされるレートの一部を削除することは、フレームを再送するクライアントが、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届く可能性が高まります。

- ビーコンは最低の必須レートで送信され、セル サイズを大まかに定義します。
- マルチキャストは、アソシエートされているクライアントに応じて、最低から最高までの優先順位の範囲で送信されます。
- 低いデータ レートが不要な場合は、802.11b データ レート（1、2、5.5、および 11）を無効にし、それ以外を有効なままにすることを検討してください。
- 802.11b 専用のクライアントのサポートを停止しないために、11 Mbps よりも低いすべてのレートを意図的に残すことも可能です。

次に示すのは 1 つの例であり、すべての設計に最適なわけではないことに注意してください（厳密なガイドラインとしては使用しないでください）。これらの変更は慎重に行う必要があり、また、RF カバレッジ設計に大きく依存します。

- たとえば、ホットスポット用に設計する場合は、最低のデータ レートを有効にします。これは、速度ではなくカバレッジの達成が目的であるためです。
- 逆に、すでに RF カバレッジが優れており、高速なネットワークのための設計を行っている場合は、最低のデータ レートを無効にします。

低データ レート（5 GHz と 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 の数を減らす

シスコでは、コントローラで設定する Service Set Identifier（SSID）の数を制限することを推奨します。同時に 16 個の SSID を設定できますが（各 AP の無線ごと）、各 WLAN/SSID には個別のプローブ応答とビーコンが必要なため、SSID を追加するたびに RF 環境の低下を招きます。さらに、PDA、WiFi 電話、バーコード スキャナなどの小型ワイヤレス機器の一部で、多くの基本 SSID（BSSID）情報を処理できなくなります。これにより、ロックアップ、リロード、あるいはアソシエーションの失敗が発生します。また、SSID の数が増えると、必要なビーコンも増えるため、実際のデータ転送に使用できる RF 時間が少なくなります。たとえば、企業では 1 ～ 3 個の SSID を使用し、高密度設計用には 1 個の SSID を使用することを推奨します。AAA オーバーライドを利用すれば、単一の SSID シナリオでユーザごとの VLAN または設定を行うことができます。

確認するには、次のコマンドを実行します。

(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

…

クライアントのロードバランシングを有効にする

高密度の実稼働ネットワークでは、ロードバランシングを有効にして、ワイヤレス ネットワークの負荷を最適化できます。たとえば、会議室やオープン エアーの会場に多数の人がいる場合、ロードバランシングにより、使用可能な複数の AP にユーザが分散されます。ただし、音声のような時間の影響を受けやすいアプリケーションでは、ローミングの問題が発生する可能性があります。そのため、WLAN でロードバランシングを有効にする前に、テストを行うことを推奨します。

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
```

WLAN 上でロード バランシングを積極的に有効にするには、次のコマンドを実行します。

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

帯域選択を有効にする

帯域選択によって、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 帯域は、混雑していることがよくあります。この帯域を使用する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だけでなく、他の AP からの同一チャネル干渉も受けます。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。これらの干渉の原因を防ぎ、ネットワーク全体のパフォーマンスを高めるために、コントローラで帯域選択を設定できます。

- 帯域選択は、デフォルトではグローバルに有効化または無効化されます。
- 帯域選択の仕組みは、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。
- 音声の帯域選択を評価する場合は、特にローミングのパフォーマンスに注意してください。詳しい説明については、以下を参照してください。
- AP の 5 GHz 信号が 2.4 GHz 信号と同じかより強い場合、最近のほとんどのモデルのクライアントは、デフォルトで 5 GHz を優先します。
- 高密度設計では、帯域選択を有効にすることを推奨します。

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します。

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な場合があります。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、クライアントが 2.4 GHz にとど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。通常、クライアントは、信号レベルが十分に高い AP をスキャンします（おそらく 20 dB か、SNR が十分に高い AP）。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 にとどまる可能性があります。このケースでは、2.4 GHz の CU が低く、コール品質が悪くない場合、選択した帯域を無効にするほうが良い可能性があります。しかし、設計上推奨されるのは、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 で帯域選択を有効にすることです。そして、5 GHz RRM の最低 Tx 電力レベルを、RRM によって設定される 2.4 GHz の平均電力レベルよりも 6 dBm 高くします。

この推奨設定の目的は、クライアントが、SNR と Tx 電力が優れた帯域とチャネルを最初に獲得できるようにすることです。前述のように、一般には、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。そのため、クライアントが最初に 5 GHz 帯に参加する場合、5 GHz の電力レベルが良好であれば、その帯域にとどまる可能性が高くなります。5 GHz の SNR レベルは一般に 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、電子レンジなどの信号の影響を受けやすいためです。

802.11k を、デュアルバンド レポーティングで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、クライアントは、要求時に最善の 2.4 GHz および 5 GHz AP のリストを受信します。ここで、クライアントは、同じチャネル上の AP リストの先頭を参照し、次に、クライアントが現在使用しているのと同じ帯域上の AP のリストの先頭を参照する可能性が最も高くなります。このロジックにより、スキャン時間が短縮され、バッテリー電力を節約できます。WLC で 802.11k を有効にしても、802.11k 非対応のクライアントに影響はありません。

確認するには、次のコマンドを実行します。

(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 で帯域選択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 ネットワークが最初に初期化されるとき、干渉なしに動作するために、参加するすべての無線がチャネル割り当てを必要とします。チャネル割り当てを最適化し、干渉のない動作を可能にするのは、DCA の仕事です。ワイヤレス ネットワークは、各無線が可能なすべてのチャネルについて報告したエア メトリックを使用してこの作業を行います。これにより、チャネル帯域幅を最大化し、すべてのソース（当該ネットワーク（信号）、他のネットワーク（外部干渉）、ノイズ（その他すべてのもの））による RF 干渉を最小化するための解を導きます。

DCA はデフォルトで有効になっており、ネットワークのチャネル プランに対するグローバルな解を提供します。

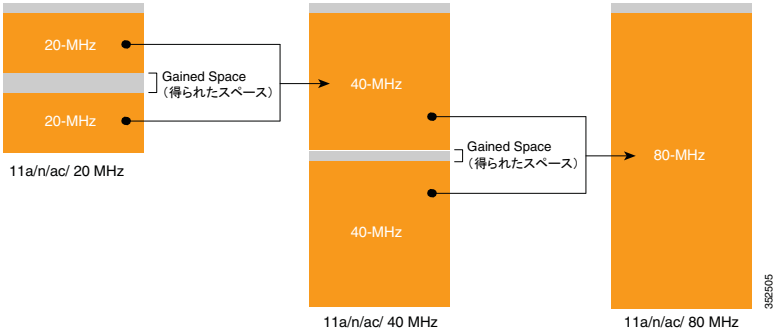
- 可用性と干渉に基づき、RRM がすべての 802.11a または 802.11b/g チャネルを自動的に設定します。

(Cisco Controller) >config 802.11a channel global auto

(Cisco Controller) >config 802.11b channel global auto

チャネル幅

802.11n では 2 本の 20 MHz チャネルをボンディングすることで、40 MHz チャネルとして動作できるため、スループットが大幅に向上します。すべての 802.11n デバイスが 40 MHz のボンディング チャネル（クライアント）をサポートしているわけではありません。802.11ac では、20 MHz チャネルを 80 MHz のワイド チャネルにボンディングして 802.11ac で使用できます。すべてのクライアントは 80 MHz をサポートしている必要があります。これは、2.4 GHz では現実的ではありません。重なっていない使用可能な 20 MHz チャネルの数が非常に限られているからです。しかし、5 GHz では、十分な数の 20 MHz チャネルがあれば、スループットと速度が大幅に向上する可能性があります（以下の DFS を参照）。



DCA で割り当てられたチャネル幅を、対応しているすべての無線に設定するには、次のコマンドを使用します。

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

Channel width overview:

- **20**:無線は 20 MHz チャネルだけを使用して通信できます。20 MHz チャネルだけを使用して運用するレガシーの 802.11a 、20 MHz 802.11n、または 40 MHz 802.11n 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 は、結合された隣接する 2 つの 20 MHz チャネルを使用して通信できます。無線は、ユーザが選択したプライマリ チャネルをアンカー チャネル(ビーコン用)として使用するとともに、より高いデータ スループットのためにその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。

注 20 MHz、40 MHz、または 80 MHz モードのアクセス ポイントの無線を静的に設定すると、config advanced 802.11a channel dca chan-width-11n {20 | 40 |80} コマンドを使用してグローバルに設定された DCA チャネル幅設定が上書きされます。アクセス ポイントの無線の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の設定がグローバルな DCA 設定で上書きされます。変更内容は、DCA が動作するように設定されている頻度に応じて、30 分以内に有効になります。

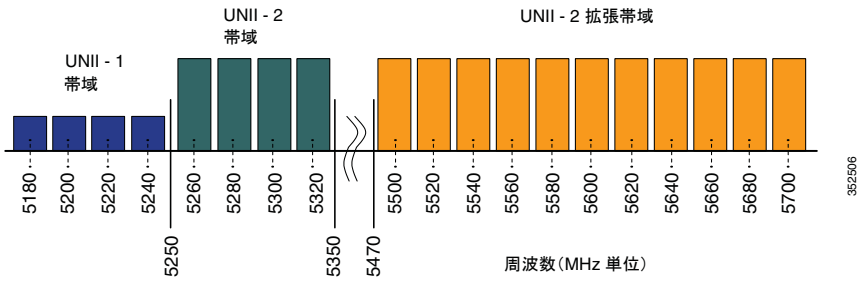
注 米国およびカナダでは、チャネル 116、120、124、および 128 は、40 MHz チャネル ボンディングに使用できません。

DFS:動的周波数選択

チャネルは、すべて一度に作成されているわけではありません。5 GHz スペクトルでより多くのチャネルを利用できるようにするために、動的周波数選択が開発されました。規制ドメインに応じて、4 ～ 12 個の追加チャネルが使用できるようになります。チャネルが増えると、キャパシティが増えることになります。

DFS はレーダー信号を検出し、同じ周波数で動作している気象レーダーとの干渉がないことを確認します。また、DFS では、すべての検出信号から独立してクライアントと AP を制御する、グループの監視役としてマスター(AP)を指定します。北米では、以前から DFS チャネルの使用について懸念があり、代わりに、8 つの非 DFS チャネルがあります。ETSI 規制ドメイン(欧州)では、4 つの非 DFS チャネルがあり、DFS チャネルが何年も問題なく使用されています。

5 GHz 帯はより多くのチャネルを提供しますが、全体的な設計に注意する必要があります。5 GHz チャネルでは、電力および、屋内または屋外での導入にさまざまな規制があるからです。たとえば、北米では U-NII-1 を屋内でしか使用できず、その最大電力は 50 mW に制限されており、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 チャネル リストで無効になっています。使用中のチャネルを確認するには、次のコマンドを使用します。

(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

規制ドメイン内でより多くのチャネルを使用するために、U-NII-2e チャネルを有効にするには、次のコマンドを使用します。

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

北米と欧州で使用できるチャネルは、100 ～ 140（8 個の追加チャネル）です。チャネル 120、124、128 は米国では無効であり、ETSI DFS 規則により重大な罰が科されるため、サポートされていません。

DCA の再起動

チャネルとチャネル幅の選択を終えるか、新しいネットワークですべての AP の設置を完了すると、DCA がチャネルを動的に管理し、時間や状況の変化に伴って調整を行います。ただし、新たな設置の場合や、チャネル幅を変えるか、新しい AP を追加するなど、DCA に大幅な変更を加えた場合は、DCA プロセスを再起動することができます。これにより、積極的な検索モード（スタートアップ）が初期化され、開始チャネル プランが最適化されます。

現在グループ リーダーになっている WLC を特定するには、次のコマンドを実行します。

(Cisco Controller) >show advanced 802.11a group

(Cisco Controller) >show advanced 802.11b group

特定されたグループ リーダーから、DCA を再度初期化します。

(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、次のコマンドを実行します。

(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
```

成功すると、DCA の感度がスタートアップ バナーに表示されます。

注 スタートアップ モードは 100 分間動作し、通常 30 ～ 40 分以内に解を見つけます。大幅な変更を加えた場合（チャネル幅や AP の数）、これがクライアントにとって致命的な影響を及ぼす場合があります（大量のチャネル変更）。スタートアップ中の変更により、求める解に対する条件も変わってしまうため、この手順は最後に実行します。

ローカル クライアント プロファイリングを有効にする

WLC は、クライアントの WLAN へのアソシエート中に受信した情報からクライアントのタイプを判定できます。コントローラは情報の収集者としての機能を果たし、ISE を必要なデータとともに最適な形式で送信するか、WLC のダッシュボードに情報を直接表示します。

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

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

Application Visibility and Control (AVC)

Application Visibility and Control（AVC）は、シスコのディープ パケット インスペクション（DPI）手法と Network-Based Application Recognition（NBAR）エンジンを使用してアプリケーションを分類し、Wi-Fi ネットワークに対するアプリケーションレベルの可視化と制御を可能にします。AVC 機能では、アプリケーションを認識した後、トラフィックをドロップまたはマークすることができます。

AVC を使用すると、コントローラは 1,000 以上のアプリケーションを検出できます。AVC では、リアルタイムな分析を行い、ネットワークの輻輳、コストの高いネットワーク リンクの使用、インフラストラクチャのアップグレードを減らすためのポリシーを作成できます。

AVC がサポートされるコントローラ プラットフォームは、Cisco 2500 シリーズ コントローラ、Cisco 5500 シリーズ コントローラ、中央スイッチング 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 上で AVC の可視化（ベースライン アプリケーション使用率）を有効にするには、次のコマンドを実行します。

(Cisco Controller) >config wlan avc 1 visibility enable

WLAN 上で AVC による統計情報を表示するには、次のコマンドを実行します（WLAN ごとのアプリケーション使用率を表示します）。

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

一般的な使用例は、トラフィックのマーク、ドロップ、レート制限です。この例では、Microsoft Lync でビデオおよび音声コールを行うときのユーザ エクスペリエンスを最大化するために、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、次のコマンドを実行します。

(Cisco Controller) >config avc profile MSLync create

AVC プロファイルに 1 つ以上のルールを追加するには、次のコマンドを実行します（Lync の音声を DSCP 46 でマークし、ビデオを DSCP 34 でマークします）。

(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

AVC プロファイルを WLAN に適用するには、次のコマンドを実行します。

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

AVC プロファイルの要約を表示するには、次のコマンドを実行します。

(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、次のコマンドを実行します。

(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 Bidir
ectional
ms-lync-video             business-and-productivity-tools    Mark      34 Bidir
ectional

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

ローミングを最適化するために 802.11k を有効にする

802.11k 規格を使用すると、クライアントは、サービス セット移行の候補となる既知のネイバー AP 情報を含むネイバー レポートを要求できます。802.11k ネイバー リストを使用することで、アクティブなスキャンとパッシブなスキャンの必要性を制限することができます。

802.11k は、よくある「スティッキー クライアント」の問題の解決に役立ちます。スティッキー クライアントとは、もっと近くの AP によりよい選択肢がある場合でも、ある特定の AP に対してアソシエートを行い続けるクライアントです。

WLAN で 802.11k ネイバー リストを有効にするには、次のコマンドを実行します。

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

WLAN でデュアルバンド 802.11k ネイバー リストを有効にするには、次のコマンドを実行します。

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

WLAN で経由ローミング予測リストの機能を有効にするには、次のコマンドを実行します。

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

モビリティ

モビリティに関するベスト プラクティスについて説明します。

- モビリティ グループに属するすべてのコントローラでは、たとえば 192.0.2.x のように、仮想インターフェイスを同じ IP アドレスに設定する必要があります。これはローミングのために重要です。あるモビリティ グループに属する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と、コントローラ間のローミングは動作するように見えても、引き継ぎの処理が完全に行われず、ある一定の期間、クライアントが接続を失うことになります。

  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
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
```

- 仮想ゲートウェイのアドレスは、ネットワーク インフラストラクチャ内部では**ルーティング不可能**である必要があります。ワイヤレス クライアントがコントローラに接続しているときだけ到達でき、有線接続からは到達できないように意図されています。
- すべてのコントローラの管理用インターフェイス間で IP 接続が確立されている必要があります。
- ほとんどの場合、どのコントローラにも同じモビリティ グループ名を設定する必要があります。ゲストアクセス機能用のコントローラ（通常は非武装地帯（DMZ）上）に配置する場合は、この規則の例外となります。
- グループ名は、PMK/L2 高速ローミング識別情報として使用されます。高速ローミングの設計では、同じグループ名を持つことが必要です。
- WebAuth またはゲスト用に導入する場合は、同じモビリティ グループ名にする必要はありません。
- すべての WLC を同じバージョンのソフトウェア コードで実行すれば、一部の WLC にのみ存在するバグにより動作に不整合が生じる事態を防ぐことができます。ソフトウェア リリース 6.0 以降については、すべてのバージョンはモビリティに関して相互互換性があるため、これは必須ではありません。
- モビリティ グループは不必要に大きくしないでください。1 つのモビリティ 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エリアの AP を管理するコントローラだけをすべて含めるようにします。たとえば、1 つの建物内の AP を管理するすべてのコントローラがこれに該当します。複数の建物に分かれているシナリオでは、これらを複数のモビリティ グループに分割する必要があります。このようにすると、グループ内で相互に通信しない有効なクライアント、AP、および不正な AP で構成される大容量のリストをコントローラで保持する必要がなくなるため、メモリと CPU を節約できます。
- また、モビリティ グループ内の複数のコントローラに AP が分散するようにします。たとえば、フロアごとやコントローラごとに分散させ、ソルト アンド ペッパー配置（複数のアクセス ポイントが交互に異なるコントローラで終端される配置）を避けます。これにより、コントローラ間のローミングが減り、モビリティ グループのアクティビティへの影響が少なくなります。
- 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は、あるコントローラのリロード後に、ネットワーク内の AP について不正 AP 警告が発生するのは問題ではありません。これは、モビリティ グループのメンバ間で、AP、クライアント、不正メンバのリストのアップデートに時間がかかるためです。

モビリティ マルチキャスト モードの設定

モビリティ マルチキャスト モードを設定することで、クライアントは、各コントローラにユニキャストを送信する代わりに、モビリティ ピアにマルチキャストでメッセージを送信することができます。これは、時間、CPU 使用率、ネットワーク使用率の点でメリットがあります。

注 コントローラが異なるサブネットを管理している場合、トラフィックがコントローラ間を通過していることを確認します。

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

(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、次のコマンドを実行します。

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

Fast SSID Change を有効にする

コントローラで Fast SSID Change を有効にすると、クライアントは SSID 間をより速く移動できます。Fast SSID が有効になっていると、クライアント エントリはクリアされず、遅延が適用されません。これは、Apple IOS デバイスをサポートする上で非常に重要です。

Fast SSID Change を有効にするには、次のコマンドを実行します。

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

CleanAir を有効にする

RF の干渉を効果的に検出して低減するには、できるだけ CleanAir を有効にします。汎用の DECT 電話、妨害装置など、セキュリティ アラートを発行するさまざまな干渉源に対して推奨事項があります。

ネットワーク（802.11b）に対する CleanAir 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 802.11b cleanair config

ネットワーク（802.11a）に対する CleanAir 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 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、次のコマンドを実行します。

(Cisco Controller) >config 802.11b cleanair enable network

(Cisco Controller) >config 802.11a cleanair enable network

特に妨害装置に対する干渉検出を有効にするには、たとえば次のコマンドを実行します。

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

802.11 ネットワークで CleanAir が有効になっていることを確認するには、次のコマンドを実行します。

(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
```

高可用性クライアント（AP SSO）を有効にする

AP ステートフル スイッチオーバー（AP SSO）

高可用性（HA）機能 APSSO を、Cisco ワイヤレス LAN コントローラ（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 で設定すると、アクセス ポイント（AP）は、アクティブ WLC と CAPWAP トンネルを確立し、スタンバイ WLC と AP データベースのミラー コピーを共有できます。アクティブな 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。AP とアクティブ状態の WLC の間で一度に維持される CAPWAP トンネルは 1 つだけです。AP SSO サポートは、ボックス フェールオーバーまたはネットワーク フェールオーバーによって障害状態が発生し、ワイヤレス ネットワークが長時間ダウンすることを防ぐために、Cisco ワイヤレス LAN コントローラ ネットワークに追加されました。

サービスに悪影響を及ぼさずに高可用性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 コントローラに、クライアントと AP をシームレスに移行する必要があります。リリース 7.5 は、ワイヤレス LAN コントローラのクライアント ステートフル スイッチオーバー(Client SSO)をサポートしています。Client SSO は、すでに認証と DHCP フェーズを完了し、トラフィックの送受信を開始したクライアントに対してサポートされます。Client SSO を使用すると、クライアントが WLC にアソシエートしたとき、または、クライアント パラメータが変化したときに、クライアントの情報がスタンバイ 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 WLC に同期されます。このような仕組みにより、スイッチオーバー時にクライアントの再アソシエートを避けることができ、クライアントだけでなく AP にとってもフェールオーバーがシームレスに行われ、クライアントのサービス ダウンタイムと SSID の停止時間がなくなります。

注 詳細については、『Cisco Wireless LAN Controller 設定ガイド』[英語] を参照してください。

HA の設定を開始する前に

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にあることを確認します。

ローカル冗長 IP アドレスとピア冗長管理 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がリブートし、アクティブ コントローラとスタンバイホット 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設定を行います。

(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 コントローラが利用可能かつ動作可能な場合にのみ実行できます。

スタンバイ 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 コントローラが利用可能かつ動作可能な場合にのみ実行できます。

手動スイッチオーバーを開始します。

(Cisco Controller) > config redundancy force-switchover

このコマンドは、手動スイッチオーバーが必要な場合にのみ実行します。

冗長性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}

FlexConnect のベスト プラクティス

ここでは、FlexConnect のベスト プラクティスをいくつか示します。

- ブランチ サイトに FlexConnect を導入すると、各リモート オフィスに WLC を設置する代わりに、中央サイトにコントローラを設置することができ、これにより、ブランチの設備投資コストと運用コストを削減できます。さらに、電力消費量が削減され、IT サポートの一元化も可能になります。また、管理を中央サイトに一元化し、WAN 障害に対する耐性を高め、中央サイトとリモート サイト間の WAN 使用率を削減できるメリットもあります。
- 分散したブランチ オフィスへの導入では、最小 WAN 帯域幅、最大 RTT、最小 MTU、およびフラグメンテーションのガイドラインに関して、アーキテクチャ要件を考慮する必要があります。詳細については、次のガイドを参照してください。

  http://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/7-5/Flex_7500_DG.html#wp43317 [英語]
- 使用する AP モデルで FlexConnect がサポートされていることを確認してください。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 上で、CAPWAP 制御チャネル トラフィックを優先するように QoS を設定します。

ローカル スイッチング

- WLAN でローカル スイッチングを有効にすると、WAN 障害に対する復元力が高まり、WAN 上で送受信されるデータの量が減るため、高価な WAN 帯域幅の使用率が低くなります。
- ローカル スイッチングは、リソースがブランチ サイトに存在し、データトラフィックを WAN リンクを介してコントローラに送信する必要がない場合に有効です。
- FlexConnect AP を、スイッチの 802.1Q トランク ポートに接続します。
- VLAN のサポートを有効にします。
- AP のネイティブ VLAN に接続する際、L2 のネイティブ VLAN 設定は、AP の設定に一致させる必要があります。
- ローカルにスイッチングされる WLAN の各対応 VLAN は、対応するスイッチ ポート上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
!
```

- 一部の機能は、スタンドアロン モードやローカル スイッチング モードでは使用できません。ローカル スイッチングを使用する際は、次の制限事項に注意してください。
  - スタンドアロン モードの MAC または Web 認証
  - IPv6 L3 モビリティ
  - SXP TrustSec
  - アプリケーションの可視性と制御
  - サービス検出ゲートウェイ
  - ネイティブ プロファイリングとポリシー分類

完全なリストについては、『FlexConnect Feature Matrix』を参照してください。
http://www.cisco.com/en/US/products/ps6366/products_tech_note09186a0080b3690b.shtml [英語]

スプリット トンネリング

- ほとんどのリソースが中央サイトにあり、クライアント データを中央でスイッチングする必要があるものの、WAN 帯域幅の使用率を下げるために、リモート オフィスの一部のローカル デバイスでスイッチングをローカルに行うシナリオでは、スプリット トンネリング機能を設定します。
- この機能の一般的な使用例は、OEAP テレワーカーのセットアップです。企業用 SSID 上のクライアントはローカル 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、または個人用 SSID 上の無線デバイス)と直接通信でき、CAPWAP 上でパケットを送信することにより、WAN 帯域幅を消費しません。
- 中央の DHCP 機能とスプリット トンネリング機能は、AP のルーティング機能を使用します。
- スプリット トンネリングを導入するときには次の制限事項に注意してください。
  - スプリット トンネリングは OEAP 600 AP ではサポートされていません。
  - 静的な IP クライアントは、中央の DHCP およびローカルに分離された WLAN ではサポートされていません。

VLAN ベースの中央スイッチング

- AAA サーバから返された VLAN と、ブランチ サイトにある VLAN に基づき、データ トラフィックをローカルにスイッチングするか中央でスイッチングするかを動的に決める必要があるシナリオでは、VLAN ベースの中央スイッチングを使用します。
- AAA サーバから返され、ブランチ サイトに存在しない VLAN については、トラフィックは中央でスイッチングされます。

FlexConnect グループ

次のような機能を利用するには、FlexConnect グループを定義します。

- 音声導入のための 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
- スマート AP イメージ 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 が接続モードまたはスタンドアロン モードの場合に、クライアントで CCKM/OKC 高速ローミングが必要なシナリオで使用します。
- この機能により、クライアントをある 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 AP では、アソシエートを行う可能性のあるすべてのクライアントについて CCKM/OKC キャッシュ情報を取得する必要があります。それにより、CCKM キャッシュ情報をコントローラに送り返さずに、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、RADIUS サーバの障害に対するブランチの復元力を高めるには、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、中央サイトへの WAN 遅延が大きいリモート オフィスでも使用します。
- 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可能です。スタンドアロン モードの FlexConnect AP は、バックアップ RADIUS サーバに対する完全な 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か、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 の停止中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 サーバを設定する際には、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、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 RADIUS サーバに追加する必要があります。

ローカル EAP

- 復元力を高めるために、FlexConnect グループ上でローカル 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 サーバ機能とともに使用できます。FlexConnect グループがバックアップ RADIUS サーバとローカル認証の両方で設定されている場合、FlexConnect AP は、必ず最初にプライマリ 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みます。その後、セカンダリ バックアップ RADIUS サーバを試行し（プライマリに接続できない場合）、最後に FlexConnect AP 上のローカル EAP サーバ自身の認証を試行します（プライマリとセカンダリの両方に接続できない場合）。
- FlexConnect AP 上でローカル EAP を設定する際には、次の制限事項に注意してください。
  - 最大 100 人の静的に設定されたユーザを FlexConnect AP で認証できます。グループ内の各 AP は、自身にアソシエートされたクライアントのみ認証します。
  - Active Directory（AD）統合は、この機能ではサポートされません。

スマート AP イメージ アップグレード

- スマート AP イメージ 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 の帯域幅を節約し、アップグレードに伴うサービス ダウンタイムを削減するとともに、WAN 上でのダウンロード失敗のリスクを軽減します。効率的な AP イメージのアップグレードにより、各 FlexConnect AP のダウンタイムが短縮されます。
- マスター AP の選択は、FlexConnect グループと各グループの AP モデルごとに実行されます。
- ネットワークのアップグレードに対して推奨されるベスト プラクティスは次のとおりです。
  - コントローラの CLI または GUI か、Prime Infrastructure を使用して、イメージを WLC にダウンロードします。
  - ブート イメージを強制的にセカンダリにし（新たにアップグレードするイメージではありません）、予期せぬ理由で WLC が再起動された際、にすべての AP で並列ダウンロードが実行されるのを避けます。

- コントローラは、各 FlexConnect グループのマスター AP を選出します。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、セカンダリ ブート イメージに AP ファームウェアを事前ダウンロードします。これを FlexConnect グループごとにスケジュールし、WAN が枯渇しないように制限します。
- マスター AP は、イメージのダウンロードを完了すると、コントローラにメッセージを送信します。コントローラは、スレーブ AP に対し、マスター AP から AP のファームウェアを事前ダウンロードするように指示します。
- WLC のブート イメージを、新しいイメージに変更します。
- 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 マッピングを使用すると、設定が容易になり、各 AP でマッピングを設定する必要がなくなります。たとえば、同じ VLAN 上でローカル 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 マッピングを使用すると、設定が容易になり、各 FlexConnect AP でマッピングを設定する必要がなくなります。
- WLAN-VLAN マッピングを使用して VLAN を AP 上で作成する場合は、VLAN-ACL も FlexConnect グループではなく AP で作成する必要があります。

屋外でのベスト プラクティス

ここでは、屋外での設計、導入、セキュリティのベスト 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 サーベイの実施

屋外環境は、非常に課題の多い RF 環境です。避けることのできない多くの障害物や干渉があります。ネットワーク設計の前に、RF 環境を理解するための最初のステップとして、RF アクティブ サイト サーベイを行う必要があります。

Cisco Range and Capacity Calculator を使用してカバレッジ エリアを見積もる

RF アクティブ サイト サーベイを実行すると、RF 環境についての理解が得られます。次に、ネットワークの設計要件を満たすために必要となる屋外アクセス ポイントの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 エリアを見積もるための最良のツールは、WNG Coverage and Capacity Calculator です。

http://www.cisco.com/c/en/us/support/wireless/aironet-1530-series/products-implementation-design-guides-list.html [英語]

最適な動作モードの選択

屋外アクセス ポイントは、複数の導入モードで動作できます。それぞれの導入モードは、異なる使用例に対応しています。

ローカル モード:屋外の導入に最適なオプションです。Cisco ユニファイド ネットワークの機能である無線リソース管理(RRM)を完全にサポートし、2.4 GHz と 5 GHz の無線をクライアント アクセス専用に使用できます。この導入モードは、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に使用します。

ブリッジ モード:シスコ ワイヤレス レイヤ 2 プロトコルを利用し、長距離でのアクセス ポイントの無線接続が可能になります。この導入モードは、追加のイーサネット接続が使用できない場合に使用します。

導入

バックホール用に DFS チャネルを選択することは避ける

ブリッジ モードで動作している場合、ワイヤレス バックホールに使用される 5 GHz のワイヤレス チャネルを手動で選択する必要があります。メッシュ ツリー用のバックホール チャネルを選択する場合は、レーダーに使用される可能性があるチャネル(DFS チャネル)はできるだけ避けます。これらのチャネルの規制ドメインごとのリストについては、以下を参照してください。

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

ブリッジ モード アクセス ポイントごとに BGN と優先される親を設定する

ブリッジ モードで動作する各アクセス ポイントには、ブリッジ グループ名と優先される親を割り当てる必要があります。これにより、メッシュ ネットワークが毎回同じ順序で統合され、ネットワークが設計どおりに動作するようになります。

ブリッジ グループ名を設定するには、次のコマンドを実行します。

(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

優先される親を設定するには、次のコマンドを実行します。

(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 に複数の RAP を導入する

メッシュ ネットワークを導入する際は、各アクセス ポイントから WLC に戻る複数のパスが必要です。複数のパスを追加するには、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)を持たせます。ある RAP が障害になってオフラインになった場合、他のメッシュ アクセス ポイントが同じ BGN の別の RAP に参加し、WLC へのパスも残ります。

バックホール データ レートを auto に設定する

メッシュ ネットワークを導入する場合、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、バックホール データ レートとして「auto」を選択し、Dynamic Rate Adjustment（DRA）を有効にすることを推奨します。DRA は、すべてのメッシュ リンクで有効にする必要があります。

「auto」を有効にするには、次のコマンドを実行します。

(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 ネットワークを導入するとき、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。40 MHz のバックホール チャネルを有効にすることで、バックホール速度が高くなります。

AP ごとにチャネル幅を設定するには、次のコマンドを実行します。

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

バックホール Link Signal to Noise Ratio（LinkSNR）を 25 dBm よりも大きくする

メッシュ ネットワーク上での最適なパフォーマンスを確保するには、バックホール リンク品質が良好であることを確認します。最適なリンク品質は 40 dBm 以上で得られますが、見通し外通信の導入や長距離ブリッジでは、これを常に達成できるとは限りません。LinkSNR は、25 dBm 以上にすることを推奨します。

LinkSNR を確認するには、次のコマンドを実行します。

(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、次のコマンドを実行します。

(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 認証に外部 RADIUS サーバを使用する

MAC 認証用に外部 RADIUS サーバを設定することを推奨します。これにより、すべてのブリッジ モード アクセス ポイントを 1 か所で認証でき、ネットワークの管理がシンプルになります。

外部 RADIUS サーバの設定方法については、メッシュ導入ガイドを参照してください。
http://www.cisco.com/c/en/us/td/docs/wireless/technology/mesh/7-6/design/guide/mesh76/mesh76_chapter_0101.html#ID5198 [英語]

コントローラ ベースの wIPS と不正検出を有効にする

コントローラ ベースの wIPS と不正検出は、WLC でデフォルトで有効になっています。これにより、ワイヤレス ネットワークの望ましくない不正アクセス ポイントや潜在的なワイヤレス攻撃を監視し、セキュリティを強化することができます。

設定するには次のコマンドを実行します。

(Cisco Controller) >config mesh ids-state enable

EAP をセキュリティ モードとして有効にする

各メッシュ 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 サーバとともに EAP オプションを使用することです。

設定するには次のコマンドを実行します。

(Cisco Controller) >config mesh security eap