Cisco Catalyst 3850 スイッチ

サービス ガイド

2013 年 4 月

内容

概要

Cisco® Catalyst® 3850 スイッチは、ユニファイド アクセス データ プレーン（UADP）の特定用途向け集積回路（ASIC）上に構築されます。これは最先端の ASIC で、すべてのサービスがチップに完全に統合されるため、追加モジュールを必要としません。ASIC はプログラム可能で、将来の要件をサポートできる柔軟性があります。また、有線およびワイヤレス ネットワーク上において、柔軟性と可視性のあるサービスを提供します。

ネットワークのアクセス レイヤは、ネットワークにトラフィックを送信するだけのネットワークから、多様なサービスを提供するネットワークへと進化を遂げました。有線およびワイヤレス ネットワークのコンバージェンスにより、アクセス レイヤに適用されているサービスがより高度になります。サービスリッチおよびサービスアウェアなネットワーキング プラットフォームにより、総所有コスト（TCO）の削減だけでなく、サービス提供にかかる時間の短縮も実現されます。

このマニュアルでは、Cisco Catalyst 3850 の概要および、Cisco Catalyst 3850 のサービスを導入するための手順について説明します。内容は次のとおりです。

- セキュリティ
- Quality of service
- Flexible NetFlow
- マルチキャスト
- モビリティ

Cisco Catalyst 3850 セキュリティ ポリシー

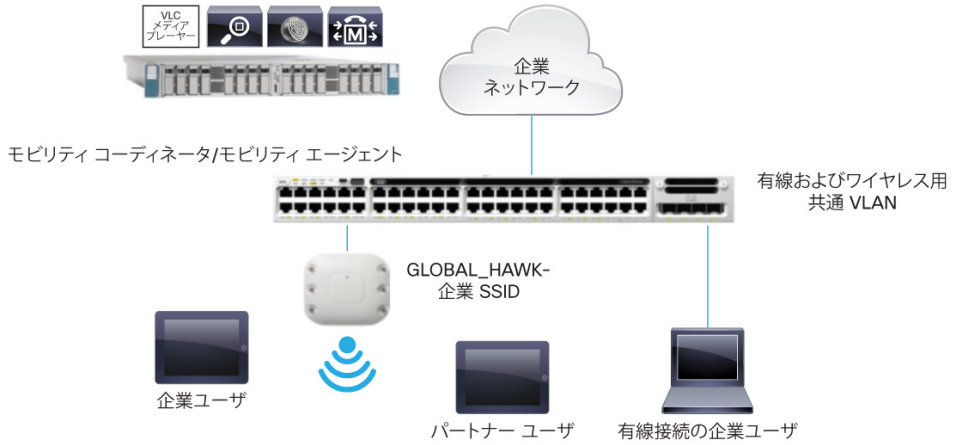
今日のネットワーク環境では、有線およびワイヤレス ネットワークのセキュリティ ポリシーの管理が課題となっています。これは、有線およびワイヤレス ユーザがネットワーク上の異なるポイントで識別され、異なるポリシーに従うことが主な原因です。

Cisco Catalyst 3850 では、有線およびワイヤレス ネットワークが 1 つのアクセス スイッチに集められるため、アーキテクチャが大きく変わっています。Cisco Catalyst 3850 上でワイヤレス ユーザが終端されるため、有線ユーザと同様、アクセス レイヤでネットワークに接続するユーザに関する詳細情報を入手できます。またこの変更では、ポリシー ポイントがアクセス層に移動されます。したがってポリシー ポイントが有線エンドポイントに一致します。

統合アクセスにおける 802.1X の設定

図 1 のトポロジ図では、有線の企業ユーザとアクセス ポイントが Cisco Catalyst 3850 に接続されています。2 つのワイヤレス クライアントが、Cisco Catalyst 3850 上でサービス セット ID（SSID）に接続されています。ワイヤレス ユーザのうちの 1 つが企業ユーザであり、他のユーザはパートナーです。企業ユーザとパートナー ユーザにはさまざまなセキュリティ ポリシーがあり、それらはキャンパス サービス ブロック内の Cisco Identity Services Engine（ISE）サーバで定義されています。キャンパス サービス ブロックには、他にもコール マネージャやビデオ ストリーミング サーバ、Cisco Prime™ Infrastructure サーバなどのサーバがあります。

図 1　統合アクセスを使用した 802.1X



認証、許可およびアカウンティング（AAA）グループと RADIUS サーバは、Cisco Catalyst 3850 で設定されます。認証と許可は ISE サーバにリダイレクトされます。ワイヤレス クライアントは dot1x を使用して認証するように設定されます。

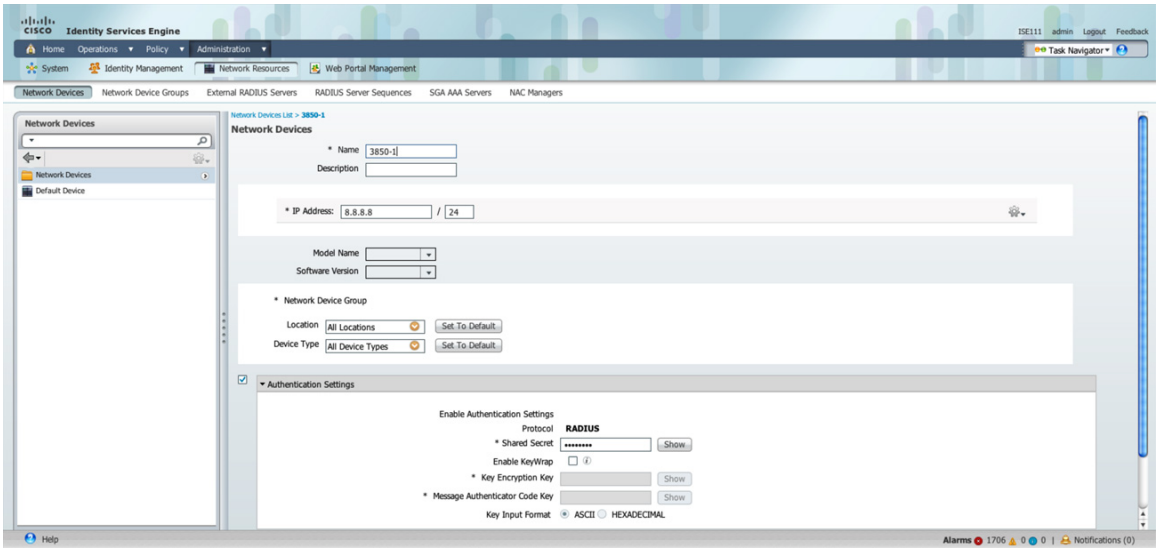
```
aaa new-model
aaa authentication dot1x CLIENT_AUTH group radius
aaa authorization network CLIENT_AUTH group radius
!
```

ISE サーバは RADIUS サーバ、スイッチはネットワーク デバイスの 1 つとして ISE サーバ上で定義されます。RADIUS サーバは、スイッチ上に定義する必要があります。

```
radius server ise
 address ipv4 9.9.9.9 auth-port 1812 acct-port 1813
 timeout 60
 retransmit 3
 key cisco123
!
```

Cisco Catalyst 3850 を定義するには、ISE 画面で、[Administration] → [Network Resources] → [Network Devices] の順に移動します（図 2 参照）。

図 2　ISE のデバイス定義



dot1x は、有線およびワイヤレス クライアントに対してスイッチでグローバルで有効にする必要があります。

```
dot1x system-auth-control
!
```

有線ユーザの 802.1X 設定

有線ユーザの 802.1X は、ポートごとに設定されます。ポート設定は次のとおりです。

```
interface GigabitEthernet1/0/13
 switchport access vlan 12
 switchport mode access
 access-session port-control auto
 access-session host-mode single-host
 dot1x pae authenticator
 service-policy type control subscriber DOT1X
```

また、Cisco Catalyst 3850 には、現在の Cisco IOS ® ソフトウェア プラットフォームにある Auth Manager に代わる製品であるセッションアウェア ネットワーキング（SaNet）が導入されています。

SaNet を導入する目的は、セッションや認証方式に適用される機能の間に依存関係を持たせないためです。したがって、適切な AAA の対話により、何らかの認証方式によって機能の承認データを取得し、セッションで実行する必要があります。これは、ルーティング プロトコルやファイアウォール ルール、QoS などで使用される Modular Policy Framework（MPF）に類似したポリシー モデルを使用することで達成されます。詳細については、http://www.cisco.com/en/US/docs/ios-xml/ios/san/configuration/xe-3se/3850/san-overview.html で SaNet のマニュアルを参照してください。次のポリシーは SaNet の例です。

```
class-map type control subscriber match-all DOT1X_NO_RESP
 match method dot1x
!
policy-map type control subscriber DOT1X
 event session-started match-all
  1 class always do-until-failure
   2 authenticate using dot1x retries 3 retry-time 60
 event authentication-success match-all
 event authentication-failure match-all
  5 class DOT1X_NO_RESP do-until-failure
   1 authentication-restart 60
!
```

ワイヤレス ユーザの 802.1X 設定

ワイヤレス クライアントの場合、802.1x は WLAN コンフィギュレーション モードで設定されます。AAA 認証方式は、有線クライアントに似ています。

```
wlan Predator 1 Predator
security dot1x authentication-list CLIENT_AUTH
```

ユーザが資格情報を入力すると、ISE サーバでユーザを認証し、承認します。許可が成功すると、ISE ユーザ グループまたはデバイス タイプに基づいてポリシーを提供する特定の VLAN が割り当てられます。また、QoS、ダウンロード可能アクセス コントロール リスト(dACL)などのポリシーがあります。

クライアント セッションは承認後、Cisco Catalyst 3850 でセッションが終了するまで保持されます。クライアントの状態は、ワイヤレス コントロール マネージャ(WCM)プロセスによって制御されます。

dot1X を使用して認証するエンド ステーション(有線またはワイヤレス)を「クライアント」といい、このクライアント特有の dACL、QoS などのすべてのポリシーは、既存の 3K スイッチのポートとは異なり、ハードウェア内のクライアント エンティティにインストールされます。これは、有線およびワイヤレス クライアントの間で整合性を達成する方法の一例です。

スイッチに接続された有線およびワイヤレス デバイス全体を確認するには、次のコマンドを使用できます。

```
Switch#sh access-session

Interface  MAC Address    Method  Domain  Status Fg Session ID
Gi1/0/13   0024.7eda.6440 dot1x   DATA    Auth      0A0101010000109927B3B90C
Ca1        b065.bdbf.77a3 dot1x   DATA    Auth      0a01010150f57a300000002e
Ca1        b065.bdb0.a1ad dot1x   DATA    Auth      0a01010150f57ac20000002f

Session count = 3

Key to Session Events Status Flags:

  A - Applying Policy (multi-line status for details)
  D - Awaiting Deletion
  F - Final Removal in progress
  I - Awaiting IIF ID allocation
  P - Pushed Session (non-transient state)
```

```
  R - Removing User Profile (multi-line status for details)
  U - Applying User Profile (multi-line status for details)
  X - Unknown Blocker
```

次の出力は、ワイヤレス クライアントのセッションの詳細なビューを示します。

```
Switch#sh access-session mac b065.bdb0.a1ad details
            Interface:  Capwap0
               IIF-ID:  0xE49A0000000008
          MAC Address:  b065.bdb0.a1ad
         IPv6 Address:  Unknown
         IPv4 Address:  12.0.0.2
            User-Name:  user1
               Status:  Authorized
               Domain:  DATA
       Oper host mode:  multi-auth
     Oper control dir:  both
      Session timeout:  N/A
    <snip….snip>

 Server Policies (priority 100)
              ACS ACL:  xACSACLx-IP-user1-46a243eb
Method status list:
       Method           State  dot1x            Authc Success
```

次は、有線ポートの設定です。

```
Switch#sh run int gig1/0/13
Building configuration...

Current configuration : 317 bytes
!
interface GigabitEthernet1/0/13
 description dot1X Wired Port in Vlan 30
 switchport access vlan 30
 switchport mode access
 load-interval 30
 access-session host-mode single-host
 access-session port-control auto
 dot1x pae authenticator
 spanning-tree portfast
 service-policy type control subscriber 802.1x
end
```

次は、有線クライアント セッションの詳細な出力です。

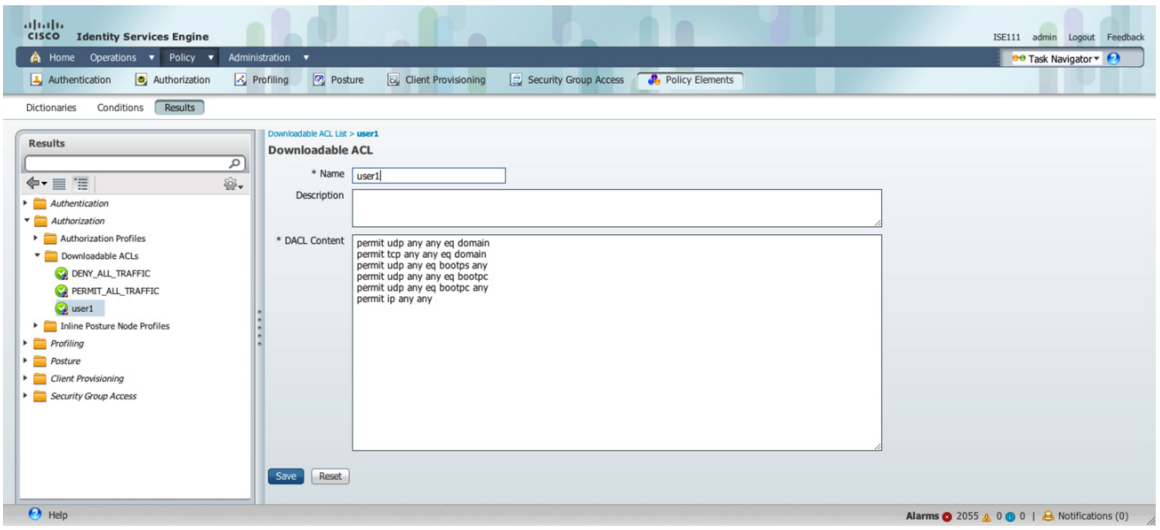
```
Switch#sh access-session mac 0024.7eda.6440 details
            Interface:  GigabitEthernet1/0/13
               IIF-ID:  0x1092DC000000107
          MAC Address:  0024.7eda.6440
         IPv6 Address:  Unknown
         IPv4 Address:  10.3.0.113
            User-Name:  corp1
               Status:  Authorized
               Domain:  DATA
       Oper host mode:  single-host
     Oper control dir:  both
      Session timeout:  N/A
    Common Session ID:  0A010101000011334A316CE0
      Acct Session ID:  Unknown
               Handle:  0x8B00039F
      Current Policy:  802.1x

Server Policies:
              ACS ACL:  xACSACLx-IP-Corp-506f07b4

Method status list:
       Method           State
       dot1x            Authc Success
```

注: この出力では、ACL はクライアントのエンティティにインストールされますが、ポートにはインストールされません。

ダウンロード可能アクセス コントロール リスト

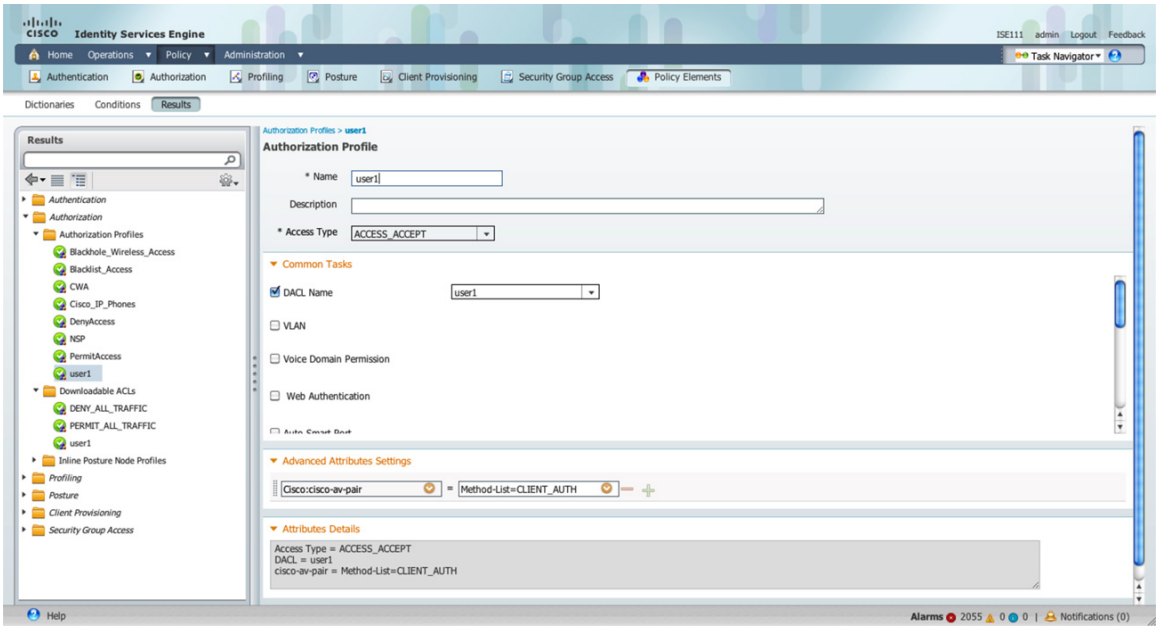
図 3 のスクリーン ショットは、ISE 上の dACL の定義を示します。

図 3 [Downloadable ACL] 画面



ISE の ACL を定義したら、図 4 に示すように、許可プロファイルに関連付けることができます。

図 4　許可プロファイル



注:　名前付き認証 **method-list** が AAA 用に存在している場合、図 4 で、[Method-List] が [CLIENT_AUTH] となっているように、属性を ISE から設定する必要があります。

ACL のダウンロードに成功した後で、クライアントは承認されます。以下は、ACL の出力です。

```
Switch#sh access-lists
Extended IP access list xACSACLx-IP-user1-46a243eb (per-user)
     1 permit udp any any eq domain
     2 permit tcp any any eq domain
     3 permit udp any eq bootps any
     4 permit udp any any eq bootpc
     5 permit udp any eq bootpc any
     6 permit ip any any
```

アクセス コントロール リストの配置に関する考慮事項

Cisco Catalyst 3850 および統合アクセスを使用すると、ACL は、有線ポート/クライアントでアプリケーションに適用されているのと同じように、ワイヤレス クライアントに適用することができます。Cisco Catalyst 3850 では、3K-X スイッチよりも ACL の方に多くの三値連想メモリ（TCAM）が割り当てられています。ここでは、スケーラビリティの値の一部について説明します。

表 1 に、アクセス コントロール エントリの（ACE）のスケーラビリティをまとめます。

表 1　スケール番号

ACL リソース	Cisco Catalyst 3850
IPv4 ACE	3000 エントリ
IPv6 ACE	1500 エントリ
L4OP/ACL	8 L4OP

ACE の合計容量は ACE のすべてのタイプを構成する集約数です。ただし、1 種類の ACE は最大 1500 まで拡張できます。たとえば、ポート ACL（PACL）の**アクセス コントロール エントリ**の総数が 1500 を超えることはできません。ただし、PACL およびルータ ACL（RACL）の**アクセス コントロール エントリ**の合計数は 3000 まで拡張できます。

Cisco Catalyst 3850 の QoS

Cisco Catalyst 3850 の主要な利点の 1 つは、アクセス レイヤでワイヤレス パケットを見られることです。この可視性は強力な機能で、ネットワーク管理者はこれを使用して有線トラフィックの豊富なインテリジェント サービスを適用し、ワイヤレス トラフィックにもこれらのサービスを拡張することをできます。QoS は、有線ネットワーク上でのアプリケーションの場合と同様、ワイヤレス トラフィックにも適用される機能の 1 つです。

重要な QoS 機能は、Cisco Catalyst 3850 上の有線にもワイヤレスにも導入されました。その一部をここで簡単に説明します。詳しくは後述します。

- モジュラ QoS CLI（MQC）
- アクセス ポイント、無線、基本サービス セット ID（BSSID）、およびクライアントで階層型サポートを提供する、無線ユーザの帯域幅管理用の Approximate Fair-Drop（AFD）アルゴリズム。
- 有線ポート 1 つあたり 8 キュー、およびワイヤレス ポート 1 つあたり 4 キュー
- ワイヤレス クライアントのハードウェアにおける双方向ポリシー サポート
- 有線ポートにおける 2 階層型 QoS
- SSID ごとの帯域幅管理、すなわち SSID で差別化された帯域幅管理

有線およびワイヤレス メディアと送信方法に固有の違いのため、有線およびワイヤレス QoS では違いがあります。

Cisco Catalyst 3850 の有線 QoS については後で説明します。その次に、ワイヤレス QoS について次項で説明します。

有線の QoS

Cisco Catalyst 3850 の信頼動作

Cisco Catalyst 3850 の信頼動作は、Cisco Catalyst 3K シリーズ スイッチのものから変更されています。デフォルトでは、Cisco Catalyst 3850 は有線ポート上のマーキングを信頼します。有線ポートについては、IP 電話やテレプレゼンス ユニット、カメラ、ノート型コンピュータなどのエンドポイントからの IP パケットの Differentiated Services Code Point（DSCP）マーキングは信頼および保持されます。

保持されるマーキングを表 2 にまとめます。

表 2　信頼動作

着信パケット	発信パケット	信頼動作
L3	L3	DSCP/precedence の保持
L2	L2	N/A
タグ付き	タグ付き	DSCP およびサービス クラス（CoS）の保持
L3	タグ付き	DSCP の保持、すなわち CoS が 0 に設定される

MQC の導入により、「trust cos/dscp」の CLI は、Cisco Catalyst 3850 で廃止されました。ただし、インターフェイス レベルの「trust device」は引き続きサポートされます。インターフェイスのデフォルト モードは **trusted** で、信頼できないデバイスが検出された場合のみ **untrusted** に変更されます。untrusted モードでは、DSCP/precedence/CoS は 0 にリセットされます。

有線とは異なり、ワイヤレスは Cisco Catalyst 3850 では信頼できないものと見なされます。ワイヤレス ターゲットのデフォルトの信頼設定値は **untrust** です。つまり、パケットは SSID ベースのポリシーがない場合、0 にマーク ダウンされます。

Cisco Catalyst 3850 のスタートアップ コンフィギュレーションの CLI は常に次のとおりです。

```
qos wireless-default-untrust
```

この CLI は、デフォルト設定の一部（自動的に作成される）であり、現在のリリースでは変更できません。これはワイヤレスが常に信頼できないことを意味します。

有線と同様に信頼動作がワイヤレスで必要になる場合、テーブル マップを定義する必要があります。デフォルト コピー オプションは、テーブル マップのマーキングを保護するために使用できます。

ダウンストリーム トラフィック上のマーキングはワイヤレス ターゲットで維持されません。したがって、マーキングを保持するためには、ダウンストリーム方向にテーブル マップが必要です。

マーキングを保持するテーブル マップの例を次に示します。

```
table-map dscp2dscp
 default copy
!
```

入力の Quality of Service の設定

入力分類

QoS 分類ポリシーを作成する場合、ネットワーク管理者は、ネットワークのアクセス レイヤに存在するアプリケーションを考慮する必要があります（入力方向）。アクセス エッジに存在するアプリケーションを分類して、適切なマーキングまたはポリシングでマーキングする必要があります。

MQC は、QoS 設定のスケーラビリティと柔軟性を提供し、さまざまなシスコ スイッチとルータ間で整合性のある設定を提供します。次の設定例では、各アプリケーションの拡張アクセス リストを作成し、クラス マップ コンフィギュレーション モードで適用します。

```
ip access-list extended BULK-DATA
 remark FTP
 permit tcp any any eq ftp
 permit tcp any any eq ftp-data
..
..
..
ip access-list extended DEFAULT
 remark EXPLICIT CLASS-DEFAULT
 permit ip any any
ip access-list extended MULTIMEDIA-CONFERENCING
 remark RTP
 permit udp any any range 16384 32767
ip access-list extended SCAVENGER
 remark KAZAA
 permit tcp any any eq 1214
 permit udp any any eq 1214
ip access-list extended SIGNALING
 remark SCCP
 permit tcp any any range 2000 2002
 remark SIP
 permit tcp any any range 5060 5061
```

```
 permit udp any any range 5060 5061
ip access-list extended TRANSACTIONAL-DATA
 remark HTTPS
 permit tcp any any eq 443
```

```
remark ORACLE-SQL*NET

permit tcp any any eq 1521
 permit udp any any eq 1521
```

次に、各アプリケーション サービス用のクラス マップを作成し、match 文を適用する設定を示します。

```
class-map match-any BULK-DATA
  match access-group name BULK-DATA
class-map match-any VVLAN-SIGNALING
  match ip dscp cs3
class-map match-any MULTIMEDIA-CONFERENCING
  match access-group name MULTIMEDIA-CONFERENCING
class-map match-any DEFAULT
  match access-group name DEFAULT
class-map match-any SCAVENGER
  match access-group name SCAVENGER
class-map match-any SIGNALING
  match access-group name SIGNALING
class-map match-any VVLAN-VOIP
  match ip dscp ef
class-map match-any TRANSACTIONAL-DATA
  match access-group name TRANSACTIONAL-DATA
```

入力マーキングおよびポリシング

各クラスが入力方向にアクセス レイヤで使用されるかもしれない帯域幅を制限することが重要です。適切なポリシングを達成するためには、アクセス レイヤ スイッチでの入力トラフィックの正確な DSCP マーキングは重要です。すべての信頼済みアプリケーション クラスに対して明示的なマーキング コマンドを使用することを推奨します。

入力マーキングには 2 通りの方法があります。これらは、「table-map」、「set」コマンドです。ただし、マーキングについては、使用可能なオプションは table-map のみです。

table-map を使用すると、DSCP や CoS などの同じまたは異なるマーキング間で使用できる値のマップを作成できます。マッピング可能な値は 10 進数の 0 ～ 99 です。table-map にも、明示的に設定されたマッピングのない値のデフォルトの動作モードがあります。このモードが ignore に設定されている場合、明示的なマッピングが設定されていなければ、マーキングに変更はありません。また、特定の値をコピーするか、または設定するように設定できます。

次に、table-map の設定例を示します。

```
table-map cos2cos
     default copy

policy-map cos-trust-policy
   class class-default
```

```
          set cos cos table cos2cos
```

次の設定例では、アクセス レイヤ スイッチの入力ポートに複数のクラスのポリシーを設定する方法を示します。

```
policy-map Phone+PC-Policy
 class VVLAN-VOIP
  police 128000 8000 conform-action transmit exceed-action drop
  set dscp ef
 class VVLAN-SIGNALING
  police 32000 8000 conform-action transmit exceed-action drop
  set dscp cs3
 class MULTIMEDIA-CONFERENCING
  police 5000000 8000 conform-action transmit exceed-action drop
  set dscp af41
 class SIGNALING
  police 32000 8000 conform-action transmit exceed-action drop
  set dscp cs3
 class TRANSACTIONAL-DATA
  police 10000000 8000 conform-action transmit exceed-action set-dscp-
 transmit dscp table markdown
  set dscp af21
 class BULK-DATA
  police 10000000 8000 conform-action transmit exceed-action set-dscp-
 transmit dscp table markdown
  set dscp af11
 class SCAVENGER
  police 10000000 8000 conform-action transmit exceed-action drop
  set dscp cs1
 class DEFAULT
  police 10000000 8000 conform-action transmit exceed-action set-dscp-
 transmit dscp table markdown
```

入力ポリシーの適用

他の Cisco Catalyst プラットフォームと同様に、Cisco Catalyst 3850 スイッチは、サービス ポリシーを適用する 2 種類のシンプルな方法を提供します。展開モデルに応じて、次のいずれかの方法を使用することができます。

- **ポート ベースの QoS**：物理ポート単位ポリシーを適用すると、ネットワークを入力する前に、パススルー QoS ポリシーにトラフィックを強制します。
- **VLAN ベースの QoS**：VLAN ベースのサービス ポリシーを適用すると、ポリシー マップを論理レイヤ 3 インターフェイスまたはスイッチ仮想インターフェイス（SVI）に付加する必要があります。

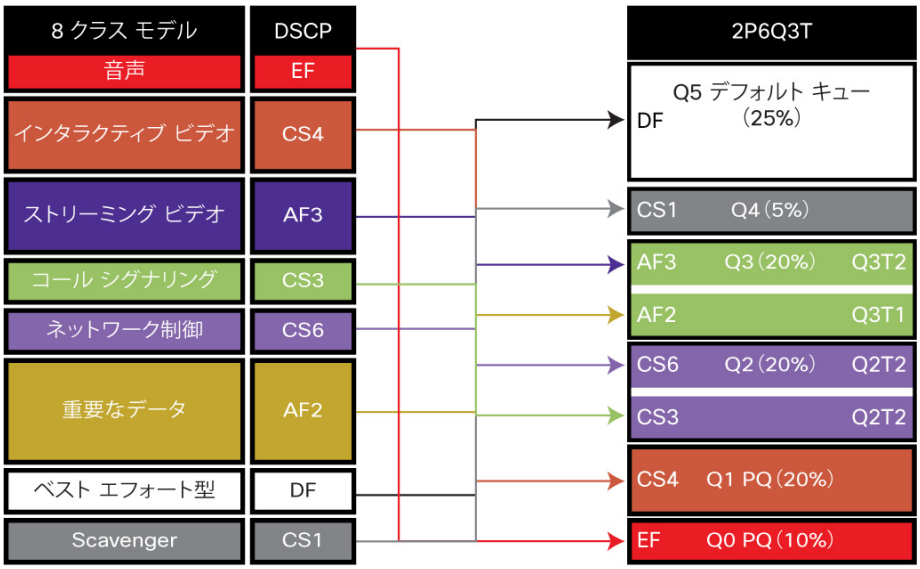
次の設定例は、アクセス レイヤ スイッチのポート ベースの QoS を配置する方法を示します。

```
interface fastethernet0/4
 description CONNECTED TO PHONE+PC
  service-policy input Phone+PC-Policy
```

出力の QoS

Cisco Catalyst 3850 には、有線ポート 1 つにつき 8 つのキューがあります。スイッチは 2P6Q3T モードで動作するように設定できます。Voice over IP（VoIP）Expedited Forwarding（EF）およびブロードキャスト ビデオの Class Selector 5（CS5）はプライオリティ キューに割り当てることができます。図 5 は 2P6Q3T モードについて説明します。

図 5　2P6Q3T モード




```
class-map VOICEQ
match dscp ef

class-map match-any VIDEOQ
match dscp cs4

class-map NETWORK-MGMT
match dscp cs6

class-map CALL-SIG
match dscp cs3

class-map CRITICAL-DATA
match dscp af21 af22 af23

class-map VIDEO-STREAM
match dscp af31 af32 af33

class-map Scavenger-Q
match dscp cs1
```

DSCP を使用してトラフィックを識別すると、ポリシー ベースを分類に適用できます。

```
policy-map 2P6Q3T
 class VOICEQ
  priority level 1
 class VIDEOQ
  priority level 2
class NETWORK-MGMT
 bandwidth remaining percent 10
 class CALL-SIG
```

```
    bandwidth remaining percent 10
  class CRITICAL-DATA
    bandwidth remaining percent 10
  class VIDEO-STREAM
    bandwidth remaining percent 10
  class SCAVENGER
    bandwidth remaining percent 1
  class class-default
    bandwidth remaining percent 25
```

出力ポリシーは、入力ポリシーと同様、ポートまたは L3 インターフェイスに適用できます。

ワイヤレス QoS

ワイヤレス ターゲット

ワイヤレス QoS には、アップストリームとダウンストリームという 2 つの用語があります。アップストリームとは、アクセス ポイントから入り、有線ネットワークから出ることを意味します。ダウンストリームとは、有線ネットワークから入り、アクセス ポイントへ出ることを意味します。次の表では、ターゲット インターフェイスの各タイプ、すなわちアクセス ポイント、無線、SSID、およびクライアントの QoS マーキング/ポリシングおよびキューイング機能を要約します。

ワイヤレス ターゲットでは、QoS ポリシーは複数レベルに適用できます。これらのターゲットはそれぞれ、次の項で説明します。

インターフェイス	アップストリーム（入力）		ダウンストリーム（出力）	
	マーキング/ポリシング	キューイング	マーキング/ポリシング	キューイング
ポート	No	No	No	Yes
無線	*No*	*No*	*No*	*Yes*
SSID	Yes	No	Yes	Yes
クライアント	Yes	No	Yes	AFD レート制限

ワイヤレス：入力の QoS

ワイヤレス クライアントの入力マーキングおよびポリシング

入力方向では、トラフィックはクライアント レベルでマークされ、ポリシングできます。次に、クライアントから送信されたアプリケーションのさまざまなクラスに対して差別化されたマーキングおよびポリシングの例を示します。

```
policy-map PER-CLIENT
 class VOICE
   set dscp ef
    police 128k 8000 exceed-action drop
 class SIGNALING
  set dscp cs3
    police 32k 8000 exceed-action drop
```

```
 class MULTIMEDIA-CONFERENCING
   set dscp af41
    police 5m 8000 exceed-action drop
 class TRANSACTIONAL
   set dscp af21
 class CLASS-DEFAULT
   set dscp default
```

クライアント ポリシーは SSID インターフェイス（以下を参照）に直接適用できます。または、ポリシー サーバ（ISE）からプッシュできます。

```
wlan open 1 Employees
service-policy client input PER-CLIENT
```

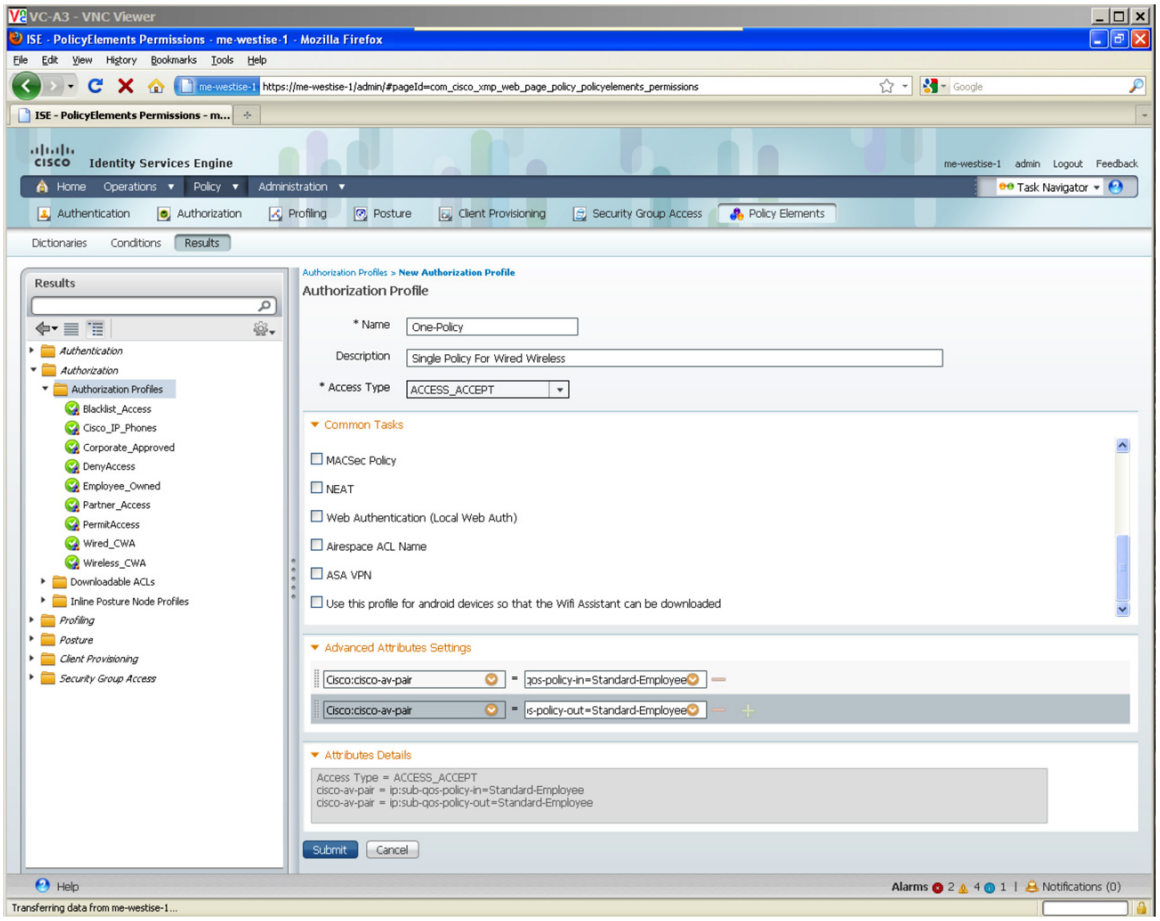
適用されたポリシーが次の CLI で参照できます。

```
Switch# sh policy-map interface wireless client
Client 000A.CC10.0001
  Service-policy input: Standard-Employee
    Class-map: Voice (match-all)
      Match: access-group name Voice
      police:
          cir 128000 bps, bc 4000 bytes
        conformed 0 bytes; actions:
          transmit
…
      QoS Set
        dscp ef
…
    Class-map: TRANSACTIONAL-DATA (match-all)
      Match: access-group name TRANSACTIONAL-DATA
      QoS Set
        dscp af21
    Class-map: class-default (match-any)
      Match: any
      QoS Set
        dscp default
```

前の設定では、SSID 上で結合されたワイヤレス クライアントごとにポリサーが強制されます。この場合は、Cisco Catalyst 3850 はクライアントごとに機能するマイクロフロー ポリサーを使用します。

ポリシー名が ISE サーバからダウンロードされた場合、図 6 に示すように、ip:sub-qos-policy-in=Standard-Employee の AV ペアでサーバを設定する必要があります。

図 6　認証プロファイル



開かれた有線ポートの場合も、同じポリシーが適用されます。ポリシーは、クライアントではなくポートに接続する必要があります。現在、QoS ポリシーを有線「クライアント」に接続することはできません。

注:　有線ポートの適用については、有線セクションで説明済みです。

WLAN/SSID の入力ポリシー

ポリシーの適用は CLI の観点から WLAN レベルで行われますが、ポリシーは実際には、システムの <access point, radio> ペアのそれぞれにあるすべての SSID のインスタンスに適用されます。これは内部的に BSSID と呼ばれます。SSID は、このドキュメントで BSSID と同義的に使用されます。SSID レベルでポリシングおよびマーキングできます。ただし、SSID レベルでは、マーキングは table-map を使用した場合のみ実行可能です。次の例では、コピーのデフォルト アクションを含む table-map のみが定義されます。これにより、IP パケットの入力 DSCP が保持されます。

```
table-map dscp2dscp
   default copy

Policy-map TRUST
Table Map dscp2dscp
   default copy
```

QoS ポリシーは、WLAN 設定下で適用されます。SSID ポリシーは次の例のように適用されます。その結果、有線と同様に、ワイヤレスからの入力トラフィック用の「trusted」動作が発生します。

```
wlan open 1 Employees
service-policy input TRUST
```

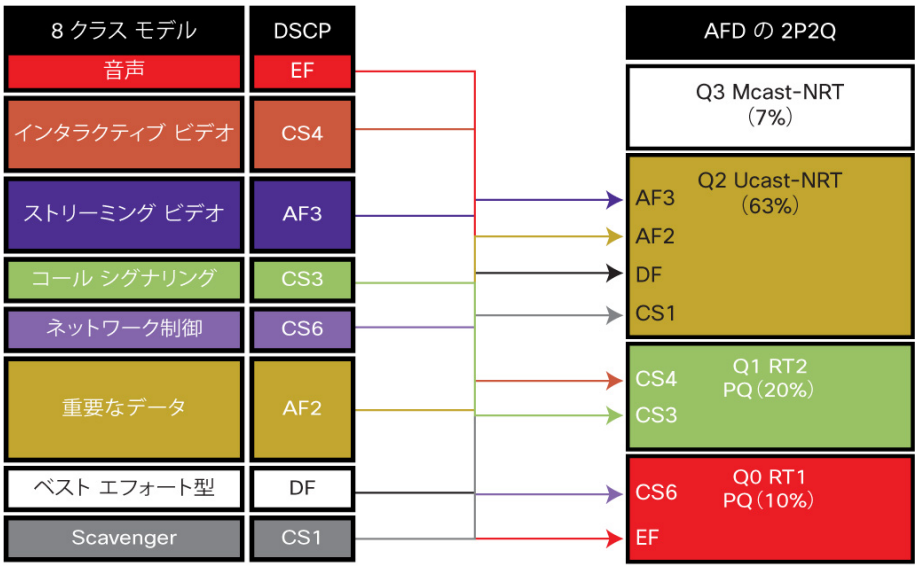
ワイヤレス：出力の QoS

これは Cisco Catalyst 3850 で使用できる QoS 機能について説明します。出力（ダウンストリーム）では、アクセス ポイント、無線、SSID、およびクライアントごとに QoS 機能が存在します。

アクセス ポイントとポートに関するポリシー

このマニュアルでは、アクセス ポイントに接続されたポートは、ワイヤレス ポートと呼びます。アクセス ポイントの 4 つのキューに合わせて、ワイヤレス ポートに 4 つのキューがあります。キュー構造は 2P2Q3T、すなわち 2 つのプライオリティ キューと 2 つの SRR キューがあり、それぞれに 3 つのしきい値があります。2P2Q3T 構造で推奨されるキューイング設定を図 7 に示します。

図 7　キューイングのアプリケーション トラフィックの 2P2Q3T キュー方式



ポートがワイヤレス ポートとして設定されると、リアル タイム 1（RT1）、RT2、ユニキャスト非リアル タイム（NRT）、およびマルチキャスト非クライアント NRT、という 4 つのキューがポート レベルで作成されます。

マルチキャスト非クライアントは、マルチキャストまたはブロードキャストの宛先 IP アドレスを持つトラフィックに分類されます。

次は 4 つのキューのデフォルトの動作です。

Q0（RT1）：制御トラフィック

Q1（RT2）：なし

Q2（NRT）: マルチキャスト NRT および制御トラフィック以外のすべて

Q3（マルチキャスト NRT）: マルチキャストおよび非クライアント トラフィック

デフォルトの QoS ポリシーは、ダウンストリーム（出力）方向のワイヤレス ポートに適用されます。ポート レベルでは、アップストリーム（入力）方向のポリシーはサポートされていません。ポートに関するポリシーはアクセス ポイントに出力される CAPWAP カプセル化パケットに適用されます。

デフォルトのワイヤレス ポート ポリシーには、ポート シェーパーと子ポリシーが含まれます。親ポリシーは、ユーザが変更することはできません。また、WCM によって制御されます。この親ポリシーには、ポート シェーパーがあります。ポート シェーパーはアクセス ポイントの無線レートの合計です。ワイヤレス ポートの子ポリシーは、ユーザが設定可能です。

次は、デフォルトの子ポリシーの設定について説明します。

```
policy-map port_child_policy
 class non-client-nrt-class
    bandwidth remaining ratio 10
```

次は、全体的なワイヤレス ポート ポリシーを示します。

```
Switch#sh policy-map in gig1/0/3
 GigabitEthernet1/0/3

  Service-policy output: defportangn

    Class-map: class-default (match-any)
      Match: any
      Queueing

      (total drops) 0
      (bytes output) 17633136
      shape (average) cir 600000000, bc 2400000, be 2400000
      target shape rate 600000000

      Service-policy : port_child_policy

        Class-map: non-client-nrt-class (match-any)
          Match: non-client-nrt
          Queueing

          (total drops) 0
          (bytes output) 17633136
          bandwidth remaining ratio 10

        Class-map: class-default (match-any)
          Match: any

          (total drops) 0
          (bytes output) 0
```

「port_child_policy」は、SSID レベルで異なるアプリケーションのトラフィックをキューイングするようにユーザが変更できます。このトラフィックはポート レベルで適切なキューにキューイングされます。次は、「port_child_policy」の設定例です。

```
Switch#sh run policy-map port_child_policy
Building configuration...
Current configuration : 227 bytes
!
 class non-client-nrt-class
    bandwidth remaining ratio 10
 class voice
    priority level 1
    police 20000
 class video
    priority level 2
    police 20000
 class class-default
    bandwidth remaining ratio 25
```

「class voice」および「class video」ポリシング内の「police 20000」ステートメントは、ポートやアクセス ポイント レベルの各クラスのマルチキャスト トラフィックを集約します。「voice」および「video」クラス マップを使用して分類されるユニキャスト トラフィックはポリシングされません。

無線に関するポリシー

無線レベルのポリシーは、ユーザが設定することはできません。これは無線に送信されるすべてのトラフィックを制限するレート リミッタです。現在は、アクセス ポイントごとに 2 つの無線のみがサポートされているため、アクセス ポイントごとに 2 個のレート リミッタのみがサポートされます。Cisco Catalyst 3850 は、無線の最大レートを検出するようにアクセス ポイントをポーリングします。シェーパーは、無線のオーバーサブスクリプションを制限するために配置されます。最大レートの検出に基づいて、レート リミッタは 2.4G および 5G バンドに対してそれぞれ 200 または 400 Mbps に制限できます。

次に無線レベルのポリシーを示します。

```
Switch#sh policy-map interface wireless radio

Radio dot11b iifid: 0x104F10000000011.0xC9CA4000000004

  Service-policy output: def-11gn

    Class-map: class-default (match-any)
      Match: any
      shape (average) cir 200000000, bc 800000, be 800000
      target shape rate 200000000

Radio dot11a iifid: 0x104F10000000011.0xCF8F4000000005

  Service-policy output: def-11an

    Class-map: class-default (match-any)
```

```
        Match: any
        shape (average) cir 400000000, bc 1600000, be 1600000
        target shape rate 400000000
```

上記のポリシーはシェーピングを示していますが、レートの緩衝や排除は行いません。基本的に、これは無線レベルのレート リミッタです。

Service Set ID に関するポリシー

SSID レベルまたは BSSID レベルのポリシーは、アップストリームとダウンストリームの両方向でユーザが設定可能です。SSID レベルのポリシーは、WLAN コンフィギュレーション モードで適用されます。

ダウンストリーム方向では、推奨されるポリシーは、親クラスのデフォルト内のテーブル マップ ベースのマーキングによる階層型キューイング ポリシーです。SSID のテーブル マップが未設定の場合、パケットはすべて 0 に再マーキングされます。パケットはポート レベルで NRT キューから送信されます。これは、テーブル マップがない場合に、WLAN が信頼できないものと見なされるためです。

音声/ビデオ トラフィックが順位付けされる必要がある場合、ポート/アクセス ポイントと SSID の両方の子ポリシーマップは、クラス マップと適切な動作で設定する必要があります。音声/ビデオを区別するための子ポリシーがいずれかのターゲット（ポート/アクセス ポイントや SSID）に存在しない場合、ワイヤレス ネットワーク上で音声およびビデオ トラフィックの優先順位をつけられません。

次に、企業およびゲストの 2 つの SSID の例を示します。音声/ビデオ トラフィックは企業で順位付けされますが、ゲスト トラフィックはデフォルトとして分類され、適切にキューイング処理されます。

```
Policy-map enterprise-ssid-child
     Class  voice
          Priority level 1
         Police  20000
Class video
        Priority level 2
        Police  20000
Policy-map enterprise-ssid
Class class-default
        bandwidth remaining percent 70
    set wlan-user-priority dscp dscp2up1
        set dscp dscp dscp2dscp1
        service-policy enterprise-ssid-child

Policy-map guest-ssid
Class class-default
     Shape average percent 20
```

企業 SSID のクラス マップの音声とビデオでは、ポリサーは BSSID のレベルでユニキャスト トラフィックを強制的に集約します。クラス デフォルトは、輻輳がない場合に追加の未使用帯域幅を利用できる企業 SSID への最小帯域幅割り当てを提供するように設定されます。

ただし、ゲストの SSID のクラスのデフォルトは、帯域の利用率や輻輳に関係なく、使用可能な帯域幅の 20% にシェーピングされます。

クライアント

クライアント ポリシーは、アップストリームとダウンストリームの両方向で適用できます。クライアント ポリシーはユーザが設定でき、WLAN のコンフィギュレーション モードで適用できます。WLAN コンフィギュレーション モードで適用

すると、すべてのクライアントは、SSID の同じポリシーを受け取りますが、ポリシー適用はマイクロフロー ポリシングを使用して、ユーザ単位で行われます。

クライアント レベルのポリシーは、AAA サーバから適用されます。ポリシーはスイッチに対してローカルで定義され、ポリシーの名前はクライアント認証時に AAA サーバからダウンロードされます。ダウンロード可能なポリシーを使用して、差別化されたポリシーをクライアントまたはクライアント グループに対して適用です。

クライアント ポリシーがクライアントに関連付けられた後、クライアント ポリシーはクライアントの MAC アドレスを使用して検索できます。

次は、出力(ダウンストリーム)方向に適用されるクライアントのポリシー マップの出力です。

```
Switch#sh policy-map interface wireless client mac b065.bdbf.77a3

Client B065.BDBF.77A3 iifid:
0x1047D4000000011.0xD7E4C000000076.0xDD94000000028D.0xFCEBC000000373

  Service-policy output: egress-client

    Class-map: class-default (match-any)
      Match: any
      police:
          cir 500000 bps, bc 15625 bytes
        conformed 404432 bytes; actions:
          transmit
        exceeded 0 bytes; actions:
          drop
        conformed 0000 bps, exceed 0000 bps
```

Flexible NetFlow

Flexible NetFlow(FnF)は、データの収集と測定を行う Cisco IOS ソフトウェアの重要な部分であり、これによってネットワーク内のすべてのルータまたはスイッチをテレメトリや監視デバイスのソースとして使用できるようになります。FnF によって、非常にきめ細かく正確なトラフィック測定およびハイレベルに集約されたトラフィックの収集が可能になります。FnF は、リアルタイムのネットワーク モニタリング、セキュリティ インシデントの検出、およびネットワーク トラフィックのフローの分類機能を提供します。

Cisco Catalyst 3850 NetFlow アーキテクチャ(有線およびワイヤレス)

NetFlow Cisco Catalyst 3850 の概要

Cisco Catalyst 3850 は、ライン レートでスイッチの全ポートの入力と出力両方の FnF をサポートします。スイッチの未処理のスケーラビリティは、最大 24,000 のキャッシュフローですが、UADP ASIC ごとの入力は 8,000、出力は 16,000 です。Cisco Catalyst 3850 は、IPv4、IPv6、レイヤ 2 フローおよびサンプル NetFlow の NetFlow バージョン 9 をサポートします。TCP フラグは、フロー情報の一部としてエクスポートされます。Cisco Catalyst 3850 スイッチが相互にスタックされている場合、個々のスタック メンバがコレクタに自身のフローをエクスポートします。Cisco Catalyst 3850 は、フロー モニタごとに 8 個の異なるコレクタを同時に使用して、最大 16 個のフロー モニタをサポートします。マイクロフロー ポリシングはワイヤレス クライアントでのみサポートされます。

Cisco Catalyst 3850 の FnF 機能は、IP ベース バージョン以前のバージョンで有効です。Cisco Catalyst 3850 の 48 ポート スイッチには、スイッチごとに 2 つの UADP ASIC があり、Cisco Catalyst 3850 の 24 ポート スイッチには 1 つの UADP ASIC があります。

Cisco Catalyst 3850 スイッチに対する NetFlow の設定

FnF 構成には、フロー レコード、フロー エクスポータ、およびフロー モニタという 3 つのコンポーネントがあります。

フロー レコード

NetFlow フロー レコードは、プライマリ フィールドと非プライマリ フィールドで構成されます。プライマリ フィールドは、フローを分類し、特定するために使用されるパケット ヘッダーのフィールドです。追加情報をフロー レコードに追加できます。この情報は、非プライマリ フィールドに含まれます。次に示す match コマンドはプライマリ フィールドを定義するために使用されますが、collect コマンドは非プライマリ フィールドを定義するために使用されます。

フロー レコードの設定（入力）

```
flow record v4
 match ipv4 tos
 match ipv4 protocol
 match ipv4 source address
 match ipv4 destination address
 match transport source-port
 match transport destination-port
 match interface input
 collect interface output
 collect transport tcp flags
 collect counter bytes long
 collect counter packets long
 collect timestamp absolute first
 collect timestamp absolute last
 collect counter bytes layer2 long
```

注: 「match interface output」は入力フロー モニタに設定できません。出力インターフェイスの情報を取得するためには、入力フロー レコードの「collect interface output」コマンドを使用します。

同様に、「match interface input」は出力フロー レコードでサポートされないため、次に示す「collect interface input」を使用します。

フロー レコードの設定（出力）

```
flow record v4out
 match ipv4 protocol
 match ipv4 tos
 match ipv4 source address
 match ipv4 destination address
 match transport source-port
 match transport destination-port
 match interface output
 collect interface input
 collect transport tcp flags
 collect counter bytes long
 collect counter packets long
 collect timestamp absolute first
 collect timestamp absolute last
 collect counter bytes layer2 long
```

エクスポータ/コレクタ情報

NetFlow データにアクセスするには 2 種類の主な方法があります。ひとつは CLI で show コマンドを使用する方法、もうひとつはスイッチによって定期的に送信されるエクスポート済み NetFlow 情報を受信するアプリケーションを使用する方法です。

```
flow exporter Collector
destination 10.1.1.28
dscp 48
transport udp 2055
template data timeout 30
option exporter-stats timeout 30
```

flow exporter コマンドは、エクスポータ/コレクタの宛先 IP アドレスを指定します。DSCP は、エクスポータおよび Collector に送信されるデータグラムの DSCP 値を指定します。次のコマンドは、エクスポータ/コレクタ アプリケーションがスイッチからの NetFlow エクスポート パケットをリスンする L4 ポートを指定します。テンプレート コマンドは、指定された秒数後にスイッチが Netflow テンプレートをエクスポータ/コレクタへ送信できるようにします。Cisco Catalyst 3850 は、フロー モニタごとに 8 個のエクスポータ/コレクタを同時にサポートします。

フロー モニタ

フロー モニタはインターフェイスに適用される FnF コンポーネントです。フロー モニタは、レコード、キャッシュ パラメータおよびエクスポータ/コレクタで構成されます。フロー モニタのキャッシュは、フロー モニタが最初のインターフェイスに設定されると自動的に作成されます。

フロー モニタは、次の情報のためのコンテナです。

- フロー レコード
- フロー キャッシュ パラメータ
- エクスポータ/コレクタ情報

```
flow monitor v4
    exporter Collector
    exporter Collector 1
    cache timeout active 60
    cache timeout inactive 20
record v4
```

サポートされるポート タイプへのフロー モニタの接続

有線ポート

```
interface GigabitEthernet1/0/1
    description Interface for WIRED CLIENT in CONVERGED VLAN
    switchport access vlan 10
    switchport mode access
    ip flow monitor v4 input
    ip flow monitor v4out output
    load-interval 30
  no shutdown
!
```

ワイヤレス WLAN ポート

```
wlan SSID 1 SSID
 client vlan 12
 ip flow monitor v4 input
 ip flow monitor v4out output
no shutdown
!
```

VLAN インターフェイス

```
Vlan configuration 500
 ip flow monitor v4 input
 ip flow monitor v4out output
!
```

エクスポータの簡易ネットワーク管理プロトコルの設定

```
snmp-server community public RO
snmp-server community private RO
```

簡易ネットワーク管理プロトコル（SNMP）を設定することで、外部コレクタがスイッチ上の NetFlow 関連の設定を読み取ってフローを収集できるようになります。

Flexible NetFlow 出力

Flexible NetFlow フロー モニタのステータスと統計情報を表示するには、特権 EXEC モードで「Show Flow monitor」コマンドを使用します。

```
Switch# show flow monitor
Flow Monitor v4:
  Description:       User defined
  Flow Record:       v4
  Flow Exporter:     Collector
  Cache:
    Type:              normal (Platform cache)
    Status:            allocated
    Size:              Unknown
    Inactive Timeout:  15 secs
    Active Timeout:    60 secs
    Update Timeout:    1800 secs
```

インターフェイスの Flexible NetFlow 設定ステータスを表示するには、特権 EXEC モードで「Show Flow Interface」コマンドを使用します。

```
Switch# show flow interface
Interface GigabitEthernet2/0/26
  FNF:  monitor:      v4
        direction:        Input
        traffic(ip):      on
  FNF:  monitor:          v4out
```

```
        direction:        Output
        traffic(ip):      on
```

フロー モニタのキャッシュから集約フロー統計情報を表示するには、「Show flow monitor cache format table」コマンドを使用します。

```
Switch# Show flow monitor v4 cache format table
Cache type:                               Normal (Platform cache)
  Cache size:                              Unknown
  Current entries:                               2

  Flows added:                                26492
  Flows aged:                                 26490
    - Active timeout      ( 1800 secs)          4
    - Inactive timeout    (   15 secs)      26486
IPV4-SRC-ADDR DST-ADDR SRC-PORT DST-PORT INTF-INPUT intf-output bytes-long
pkts-long time-abs-first time-abs-last
===============  ===============  =============  =============
====================
10.1.22.102 10.1.1.22  52226  5060  Gi1/0/4 LIIN0  1038  3    19:52:12.755
19:52:12.755
10.1.22.101 10.1.1.22  51524  5060  Gi1/0/3 LIIN0  1038  3    19:52:10.755
19:52:10.755
```

フロー モニタのキャッシュから上位 N 宛先の集約フロー統計情報を表示するには、次のコマンドを使用します。

```
Switch# show flow monitor v4 cache aggregate ipv4 destination add sort
counter bytes long top 4
Processed 4 flow
Aggregated to 4 flow
Showing the top 4 flow

IPV4 DST ADDR         flows            bytes long             pkts long
===============  ==========  ====================  ====================
10.1.1.22                1                  1038                     3
10.1.1.92                2                  1038                     3
10.1.1.82                4                  1038                     3
10.1.1.52                9                  1038                     3
```

フロー モニタのキャッシュから上位 N 送信元アドレスの集約フロー統計情報を表示するには、次のコマンドを使用します。

```
Switch# sh flow monitor v4 cache aggregate ipv4 source address sort highest
ipv4 source address top 2
Processed 2 flows
Aggregated to 2 flows
Showing the top 2 flows


IPV4 SRC ADDR         flows            bytes long             pkts long
```

```
===============  ==========  ====================  ====================
10.1.22.102              1                  1038                     3
10.1.22.101              1                  1038                     3
```

IPv6 Flexible NetFlow フロー モニタのステータスと統計情報を表示するには、特権 EXEC モードで「Show Flow monitor」コマンドを使用します。

```
Switch# show flow moni v6_m1 cache format table
  Cache type:                               Normal (Platform cache)
  Cache size:                               Unknown
  Current entries:                               12

  Flows added:                                   30
  Flows aged:                                    18
    - Inactive timeout     (    15 secs)         18


IPV6 SRC ADDR  IPV6 DST ADDR   TRNS    SRC PORT  TRNS DST PROT  bytes long
pkts long
============================================  ==================
2322::2   FF02::1:FF00:1   0   34560   58    72           1
2322::2   2201::2          1024 1026   17    9166290      43649
2322::2   2201::2          1024 1027   17    9166290      43649
2322::2   2201::2          1024 1024   17    9166500      43650
```

フロー モニタのキャッシュから上位 N IPv6 宛先アドレスの集約フロー統計情報を表示するには、次のコマンドを使用します。

```
Switch# show flow monitor v6_m1 cache aggregate ipv6 destination address
sort counter bytes long top 2
Processed 10 flows
Aggregated to 2 flows
Showing the top 2 flows

IPV6 DESTINATION ADDRESS:  2322::2
counter flows:             5
counter bytes long:        3278889600
counter packets long:      15613760

IPV6 DESTINATION ADDRESS:  2201::2
counter flows:             5
counter bytes long:        3221137920
counter packets long:      15338752
```

フロー モニタのキャッシュから上位 N 送信元アドレスの集約フロー統計情報を表示するには、次のコマンドを使用します。

```
Switch# show flow monitor v6_m1 cache aggregate ipv6 source address sort
highest ipv6 source address top 2
Showing the top 2 flows
```

```
IPV6 SOURCE ADDRESS:    2322::2
counter flows:          5
counter bytes long:     3919704180
counter packets long:   18665258

IPV6 SOURCE ADDRESS:    2201::2
counter flows:          5
counter bytes long:     3913954800
counter packets long:   18637880
```

マルチキャストの概要（従来のマルチキャストおよび統合マルチキャスト）

特に動画やモビリティ、クラウド テクノロジーの登場により、帯域幅の効率的かつインテリジェントな使用が最優先事項となります。また、1 対多、または多対多通信ベースのアプリケーションに関連するデータの急増を考えても、このことは非常に重要です。マルチキャストは、必要なタイミングや場所で単一のストリームを複製する固有の機能により、このような帯域を多く必要とするアプリケーションの要件の達成を支援します。

今日のネットワークでは、有線クライアントのレプリケーションは、ネットワーク スイッチで実行されます。ワイヤレスでマルチキャストが動作する方法は 2 通りあります。クライアントの関係しているアクセス ポイントにコントローラがレプリケートする方法と、すべてのアクセス ポイントが参加しているマルチキャスト グループ アドレスにコントローラが 1 つのパケットをレプリケートし、マルチキャスト対応ネットワーク インフラストラクチャへのレプリケーションをオフロードする方法です。したがって、マルチキャスト ストリームの複製が 1 組あり、片方は有線用、もう片方はワイヤレス用となります。

Cisco Catalyst 3850 および有線/ワイヤレス コンバージェンスでは、ネットワークには 1 個のみのマルチキャストストリームがあります。Cisco Catalyst 3850 は、有線およびワイヤレス クライアントにこのストリームを複製します。これによって同一のソースから送信されるストリームの数が減少し、帯域幅の節約、全体的なパフォーマンスの向上に役立ちます。

有線マルチキャスト設定は既存の Cisco Catalyst 3K シリーズ スイッチと同じです。有線ネットワークの IP マルチキャストの設定については、『IP Multicast Configuration Guide』を参照してください。

IP マルチキャスト ルーティングの設定の制限

次は、IP マルチキャスト ルーティングの設定の制約事項です。

- IP マルチキャスト ルーティングは、LAN ベース フィーチャ セットが稼働しているスイッチではサポートされません。
- マルチキャスト Flexlink はスイッチでサポートされていません。
- レイヤ 3 IPv6 マルチキャスト ルーティングはスイッチでサポートされていません。

Cisco Catalyst 3850 のワイヤレス IP マルチキャストの設定

ワイヤレス マルチキャストが Cisco Catalyst 3850 で動作するモードは 2 種類あります。基本モードでは、スイッチはアクセス ポイントに対象のクライアントが存在するポートだけに個々のパケットを複製します。このモードでは、パケットの複製は対象のアクセスポイントを宛先とするパケットに CAPWAP カプセル化が追加される前に実行されます。これにより、各アクセス ポイントへの各パケットが再循環のブロックを通過するため、スイッチの再循環が向上します。ただし、複製されたパケットはクライアントが該当のアクセスポイントのみに送信されるため、スイッチの帯域幅が効率的に使用されるようになります。

マルチキャスト マルチキャスト モードでは、スイッチとそれに接続されているすべてのアクセス ポイントは、ネットワーク内の他の場所に使用されていない 1 つの一意のマルチキャスト グループに加入します。キャンパス ネットワークからの入力の送信元ストリームは一度複製され、このマルチキャスト グループ（スイッチとすべてのアクセス

ポイントの間に形成される）の宛先アドレスで CAPWAP 内にカプセル化されます。このモードでは、複製はグループに対して 1 度だけ行われます。すなわち、CAPWAP カプセル化の再循環も 1 度だけです。このパケットは、接続されているすべてのアクセス ポイントに送信されます。このモードでは、UADP ASIC によって切り替えられるパケット数は、スイッチ帯域幅のコストに最適化されています。スイッチは常に、管理インターフェイスの IP アドレスをソースとして使用し、これらの CAPWAP カプセル化マルチキャスト パケットを送信します。アクセス ポイントは外部 CAPWAP ヘッダーのカプセル化を解除し、すべての BSSID および無線上において、最も低いデータ レートで元のマルチキャスト パケットをブロードキャストとして送信します。

ビデオストリーム モードは、上記の機能をさらに拡張したものです。最も低いデータ レートでブロードキャストとしてマルチキャストを送信する代わりに、アクセス ポイントは最大限のデータ レートで、対象のクライアントだけにユニキャストおよび送信元としてのマルチキャスト パケットを変換します。この機能はアクセス ポイント レベルで実行されるので、現在の Cisco Unified Wireless Network で動作する場合とまったく同じ方法で動作します。

次のコマンドによって、Cisco Catalyst 3850 スイッチのワイヤレス マルチキャストを有効化します。

```
Switch#conf t
Switch(config)#ip multicast-routing
Switch(config)#wireless multicast
Switch(config)#wireless broadcast
Switch(config)#Wireless multicast non-ip
Switch(config)#interface interface-id
Switch(config-if)# ip pim {dense-mode | Sparse-Mode | Sparse-dense-mode}
Switch(config)#vlan configuration <id>
Switch(config-vlan)#ipv6 nd suppress
Switch(config-vlan)#ipv6 snooping
Switch(config-vlan)#end
Switch#copy running-config startup-config
```

有効な IP マルチキャスト ルーティングに関係なく、IP マルチキャスト トラフィックを受信するためには、ワイヤレス クライアントのクライアント VLAN で Internet Group Management Protocol（IGMP）のスヌーピングをイネーブルにする必要があります。

Cisco Catalyst 3850 スイッチでマルチキャスト ルーティングをイネーブルにするには、「ip multicast-routing」コマンドを使用します。（マルチキャストに該当するか否かにかかわらず）すべてのクライアントにワイヤレスでマルチキャストを送信するには、「wireless-multicast」コマンドを使用します。「wireless-multicast」コマンドはスイッチのワイヤレス データ プレーンのパケットのブロードキャストをイネーブルにします。

ワイヤレスでマルチキャスト フラッディングをイネーブルにするには、「wireless multicast non-ip」コマンドを使用します。

マルチキャスト モードの設定

ワイヤレス マルチキャスト パケットは、ユニキャストまたはマルチキャスト トンネル内の CAPWAP でカプセル化されたパケットとして、アクセス ポイントに送信する必要があります。マルチキャスト モードをイネーブルにすると、WCM は Cisco IOS ソフトウェア内にマルチキャスト CAPWAP トンネルを作成し、マルチキャスト トンネルを指すマルチキャスト モードにアクセス ポイント トンネルを変換します。

アクセス ポイントがマルチキャスト モードの場合、このアクセス ポイントの後ろのクライアントへのマルチキャスト/ブロードキャスト パケットは、外部のマルチキャスト トンネルでこのアクセス ポイントに送信されます。

マルチキャスト モードのすべてのアクセス ポイントは、マルチキャスト トンネルを監視する必要があります。マルチキャスト グループはマルチキャスト トンネルの作成中に指定します。次に、マルチキャスト モードの設定を示します。

```
Switch# conf t
Switch(config)# ap capwap multicast <Multicast IP Address>
```

次に、ワイヤレス マルチキャストの基本設定を示します。

- IGMP スヌーピングおよびクエリアの設定:

```
Switch(config)#ip igmp snooping
Switch(config)#ip igmp snooping querier
```

- ワイヤレス マルチキャストとアクセス ポイント CAPWAP モードの設定:

```
Switch(config)#wireless multicast
Switch(config)#ap capwap multicast 234.5.6.7
```

- マルチキャスト ルーティングの設定(3850 のみ):

```
Switch(config)#ip multicast-routing
Switch(config)#interface vlan 100
Switch(config)# ip pim sparse-dense-mode
```

マルチキャストの show コマンド

また、リソースの使用状況を学習し、ネットワーク問題を解決するための情報を表示することもできます。さらに、ノードの到達可能性に関する情報を表示し、そのパケットが経由するネットワーク内のパスを検出することもできます。

次の表に示す特権 EXEC コマンドのいずれかを使用すると、さまざまなルーティング統計情報を表示できます。

スイッチとアクセス ポイントのマルチキャスト モードのワイヤレス マルチキャスト ステータス、および各 VLAN のブロードキャストおよび非 IP マルチキャスト ステータスを表示するには、特権 EXEC モードで、「show wireless multicast」コマンドを使用します。

```
Switch#show wireless multicast
show wireless multicast

Multicast                                 : Enabled
AP Capwap Multicast                       : Unicast
Wireless Broadcast                        : Disabled
Wireless Multicast non-ip-mcast           : Disabled

Vlan        Non-ip-mcast     Broadcast        MGID
------------------------------------------------------
1           Enabled          Enabled          Disabled
410         Enabled          Enabled          Disabled
411         Enabled          Enabled          Enabled
412         Disabled         Disabled         Enabled
413         Disabled         Disabled         Enabled
414         Enabled          Enabled          Disabled
```

すべての（S、G、V）リストおよび対応する MGID 値を表示するには、特権 EXEC モードで「show wireless multicast group summary」コマンドを使用します。

```
Switch#show wireless multicast group summary
IPv4 groups
-------------
MGID        Source             Group              Vlan
-------------------------------------------------------------
4160        0.0.0.0            239.255.67.250     412
4162        0.0.0.0            239.255.255.250    412
4163        0.0.0.0            224.0.1.60         412

Switch#show ip igmp snooping wireless mgid
Total number of L2-MGIDs    = 3

Total number of MCAST MGIDs = 3

 Wireless multicast is Enabled in the system
 Vlan     bcast    nonip-mcast    mcast     mgid     Stdby Flags
 1      Disabled   Disabled    Enabled     Disabled   0:0:1:0
 410    Disabled   Disabled    Enabled     Disabled   0:0:1:0
 411    Disabled   Disabled    Enabled     Enabled    0:0:1:0
 412    Disabled   Disabled    Enabled     Enabled    0:0:1:0
 413    Disabled   Disabled    Enabled     Enabled    0:0:1:0

Index  MGID                  (S, G, V)
-----------------------------------------------------------
160 4163   (0.0.0.0, 224.0.1.60, 412)
409 4162   (0.0.0.0, 239.255.255.250, 412)
409 4160   (0.0.0.0, 239.255.67.250, 412)
```

クライアントの SVG へのマッピングを含む、スイッチ上の VLAN による IP IGMP スヌーピング追跡を表示するには、特権 EXEC モードで、「show ip igmp snooping igmpv2-tracking」コマンドを使用します。

```
Switch#show ip igmp snooping igmpv2-tracking
Client to SGV mappings
----------------------
Client: 10.33.170.4 Port: Ca1
  Group: 239.255.255.250 Vlan: 412 Source: 0.0.0.0 blacklisted: no

Client: 10.33.170.33 Port: Ca7
  Group: 239.255.255.250 Vlan: 412 Source: 0.0.0.0 blacklisted: no

Client: 10.33.170.75 Port: Ca1
  Group: 239.255.255.250 Vlan: 412 Source: 0.0.0.0 blacklisted: no
  Group: 239.255.67.250 Vlan: 412 Source: 0.0.0.0 blacklisted: no

SGV to Client mappings
```

```
----------------------
Group: 224.0.1.60 Source: 0.0.0.0 Vlan: 412
  Client: 10.33.170.101 Port: Ca10 Blacklisted: no

Group: 239.255.67.250 Source: 0.0.0.0 Vlan: 412
  Client: 10.33.170.75 Port: Ca1 Blacklisted: no

Group: 239.255.255.250 Source: 0.0.0.0 Vlan: 412
  Client: 10.33.170.75 Port: Ca1 Blacklisted: no
  Client: 10.155.156.71 Port: Ca1 Blacklisted: no
```

クライアント アソシエーションを持つ特定のマルチキャスト グループの詳細情報を表示するには、特権 EXEC モードで、「show wireless multicast group vlan」コマンドを使用します。

```
Switch#show wireless multicast group 239.255.255.250 vlan 412
 Source : 0.0.0.0
 Group  : 239.255.255.250
 Vlan   : 412
 MGID   : 4162

 Number of Active Clients : 4
  Client List
 -------------
Client MAC         Client IP         Status
-----------------------------------------------------------------
2477.0336.e574     10.33.170.4       MC_ONLY
2477.035e.d848     10.33.170.109     MC_ONLY
6033.4b24.fa89     10.33.170.33      MC_ONLY
7cd1.c391.c674     10.33.170.75      MC_ONLY
```

スイッチの IP IGMP スヌーピング グループを表示するには、特権 EXEC モードで「show ip igmp snooping groups」コマンドを使用します。

```
Switch#show ip igmp snooping groups
Vlan      Group                   Type        Version     Port List
------------------------------------------------------------------------------
412       224.0.1.60              igmp        v2          Ca10
412       239.255.67.250          igmp        v3          Ca1
412       239.255.255.250         igmp        v2,v3       Ca1, Ca7
```

スイッチに直接接続され、IGMP を通じて学習されたマルチキャスト グループを表示するには、特権 EXEC モードで「show ip igmp groups」コマンドを使用します。

```
Switch#show ip igmp groups
IGMP Connected Group Membership
Group Address    Interface   Uptime    Expires   Last Reporter
239.255.255.255  Vlan413     4d18h     00:02:42  10.32.104.1
239.255.255.255  Vlan412     4d18h     00:01:39  10.33.170.1
239.255.255.250  Vlan412     01:27:18  00:02:45  10.33.170.75
```

ICMP エコー要求でマルチキャスト グループへの到達可能性を表示するには、特権 EXEC モードで「ping」コマンドを使用します。

```
Switch#ping 239.255.255.255
Type escape sequence to abort.
Sending 1, 100-byte ICMP Echos to 239.255.255.255, timeout is 2 seconds:

Reply to request 0 from 10.32.104.1, 20 ms
Reply to request 0 from 10.33.170.1, 20 ms
Reply to request 0 from 10.32.104.1, 20 ms
```

インターフェイスのマルチキャスト関連情報を表示するには、特権 EXEC モードで「show ip igmp interface vlan」コマンドを使用します。

```
Switch#show ip igmp interface vlan412
Vlan412 is up, line protocol is up
  Internet address is 10.33.170.1/24
  IGMP is enabled on interface
  Current IGMP host version is 3
  Current IGMP router version is 3
  IGMP query interval is 60 seconds
  IGMP configured query interval is 60 seconds
  IGMP querier timeout is 120 seconds
  IGMP configured querier timeout is 120 seconds
  IGMP max query response time is 10 seconds
  Last member query count is 2
  Last member query response interval is 1000 ms
  Inbound IGMP access group is not set
  IGMP activity: 43 joins, 38 leaves
  Multicast routing is enabled on interface
  Multicast TTL threshold is 0
  Multicast designated router (DR) is 10.33.170.1 (this system)
  IGMP querying router is 10.33.170.1 (this system)
  Multicast groups joined by this system (number of users):
      224.2.127.254(1)  239.255.255.255(1)
```

スイッチのすべてのマルチキャスト グループの IP IGMP メンバーシップのステータスを表示するには、特権 EXEC モードで「show ip igmp membership all」コマンドを使用します。

```
Switch#show ip igmp membership all
Flags: A  - aggregate, T - tracked
       L  - Local, S - static, V - virtual, R - Reported through v3
       I - v3lite, U - Urd, M - SSM (S,G) channel
       1,2,3 - The version of IGMP, the group is in
Channel/Group-Flags:
       / - Filtering entry (Exclude mode (S,G), Include mode (G))
Reporter:
       <mac-or-ip-address> - last reporter if group is not explicitly
tracked
```

```
        <n>/<m>      - <n> reporter in include mode, <m> reporter in exclude

 Channel/Group         Reporter        Uptime   Exp.  Flags  Interface
 *,239.255.255.255     10.32.104.1     4d18h    02:05 3LA    Vl413
 *,239.255.255.255     10.33.170.1     4d18h    02:59 3LA    Vl412
 *,239.255.255.250     10.33.170.33    01:32:53 02:59 2A     Vl412
```

特定のマルチキャスト グループの統計情報を表示するには、特権 EXEC モードで「show ip igmp membership」を使用します。

```
Switch#show ip igmp membership 239.255.255.255
Flags: A  - aggregate, T - tracked
       L  - Local, S - static, V - virtual, R - Reported through v3
       I - v3lite, U - Urd, M - SSM (S,G) channel
       1,2,3 - The version of IGMP, the group is in
Channel/Group-Flags:
       / - Filtering entry (Exclude mode (S,G), Include mode (G))
Reporter:
       <mac-or-ip-address> - last reporter if group is not explicitly
       tracked
       <n>/<m>      - <n> reporter in include mode, <m> reporter in exclude

 Channel/Group         Reporter        Uptime   Exp.  Flags  Interface
 *,239.255.255.255     10.32.104.1     4d18h    00:39 3LA    Vl413
 *,239.255.255.255     10.33.170.1     4d18h    01:34 3LA    Vl412
```

Cisco Catalyst 3850 との統合アクセス

Cisco Catalyst 3850 はスケーラブルで耐障害性に優れた、将来対応型の有線およびワイヤレス サービスを提供します。スタックあたり最大 50 台の Cisco アクセス ポイントと 2000 台のクライアントに対応した統合ワイヤレス LAN コントローラとして機能します。Cisco Catalyst 3850 は、シスコ アクセス ポイントが最大 250 台、クライアントが最大 16,000 台まで拡張できる配置の基盤を形成できます。既存の Cisco Unified Wireless Network に統合アクセス展開モードが構築されます。250 台のアクセス ポイントと 16,000 台のクライアントを超えて展開するには、Cisco Catalyst 3850 と Cisco 5760 ワイヤレス LAN コントローラを併用すれば、アクセス ポイントを 72,000 台まで、クライアントを 864,000 台まで拡張できます。

統合アクセス展開は、ワイヤレス LAN コントローラ（WLC）からアクセス ネットワークの Cisco Catalyst 3850 スイッチに機能のいくつかを分散することによって実現されます。アクセス スイッチは、CAPWAP でカプセル化されたワイヤレス トラフィックをローカルで終了させ、ワイヤレス トラフィックをイーサネットフレームに変換します。これにはスイッチの有線およびワイヤレス トラフィックを統合する追加のメリットがあり、ワイヤレス トラフィック上で豊富な機能を持つインテリジェントな有線サービスを適用することができます。

ここでは、Cisco Catalyst 3850 スイッチとの統合アクセス展開について詳しく説明します。

詳細について説明する前に、各アクセス スイッチに分散される機能を理解することが重要です。

統合アクセスを実現する分散された機能

WLC のワイヤレス サービスをイネーブルにするソフトウェアの機能には、2 つ重要なものがあります。

モビリティ エージェント

このソフトウェア機能は、アクセス ポイントからの CAPWAP トンネル終端を管理し、ローカルで実行され、アンカー WLC から移動するクライアント ステーション（エンドポイント）のデータベースを構築します。また、モビリティ エージェントは、802.1x オーセンティケータ、プロキシ IGMP、およびプロキシ ARP 機能をローカルで実行されるクライアントに対して提供します。

モビリティ コントローラ

この機能はモビリティ エージェントのソフトウェア機能を補完し、ある WLC から別の WLC へのクライアント ステーションに対するモビリティ（ローミング）を管理して、DMZ のゲストのアンカー コントローラをによって CAPWAP トンネルを構築することで、ゲスト アクセス機能を提供します。モビリティ コントローラはアクセス ポイントのライセンスも管理します。また、アクセス ポイントの外側にある RF スペクトルを管理する方法を提供します。これは無線リソース管理（RRM）と呼ばれ、不正の検出、動的なチャネル割り当て、アクセス ポイントの送信電力、カバレッジ ホールの検出、CleanAir® などが含まれます。さらに、モビリティ コントローラもすべてのモビリティ エージェントにわたるクライアント ステーションのデータベースを構築します。モビリティ コントローラは、すべてのモビリティ エージェントのすべてのクライアントの Pairwise Master Key（PMK）のキャッシュ作成を行います。これは、サブドメインおよびモビリティ グループ内のクライアントの高速ローミングを可能にします。

前述の重要な機能により、モビリティ コントローラは統合アクセス展開の必須要素です。モビリティ コントローラ ソフトウェア機能は Cisco Catalyst 3850 スイッチ スタックのアクティブ メンバ内で実行されるため、アクティブ フェールオーバーの場合にはスタック内のスタンバイ メンバに対してフェールオーバーされる場合があります。モビリティ コントローラ機能をホストするスイッチ スタックは、ローカルで接続されたすべての Cisco アクセス ポイントに対するアクティブ メンバのモビリティ エージェント機能を実行できます。

モビリティ コントローラの責任領域は、コントローラが制御するモビリティのサブドメインにあります。サブドメインのすべてのモビリティ エージェントは、モビリティ コントローラへの CAPWAP モビリティ トンネルを形成し、モビリティ コントローラにローカルのクライアントおよびローミングしたクライアントの状態をレポートします。モビリティ コントローラは、すべてのモビリティ エージェントにわたるクライアント ステーションのデータベースを構築します。

アクセス内の Cisco Catalyst 3850 スイッチにこれらの機能を分散させることで、統合アクセスは、スケーラブルで耐障害性に優れた機能豊富なワイヤレス サービスを、有線のサービスと機能とともに提供します。

モビリティ オラクル

これは、モビリティ ドメイン内のモビリティ コントローラ（モビリティのサブドメイン）をまたぐクライアント ステーションの可視性を担当するソフトウェア機能です。モビリティ オラクルは、モビリティ エージェント - モビリティ コントローラ - モビリティ オラクルの階層の任意のエンティティです。統合アクセス展開のためにモビリティ オラクルを設定することの利点は、特に複数のモビリティ コントローラ環境で、最初のクライアント参加とクライアント ローミングに対して発生するコントロール イベントを測定して減らすことにあります。この機能は、Cisco Catalyst 3850 ではホストできません。ソフトウェアをアップグレードした Cisco 5508 WLC、WiSM2、または Cisco 5760 WLC でのみホストできます。通常、モビリティ オラクルは、モビリティ コントローラ機能を実行しているコントローラ アプライアンスでホストされます。

ロールの論理的な階層型グループ

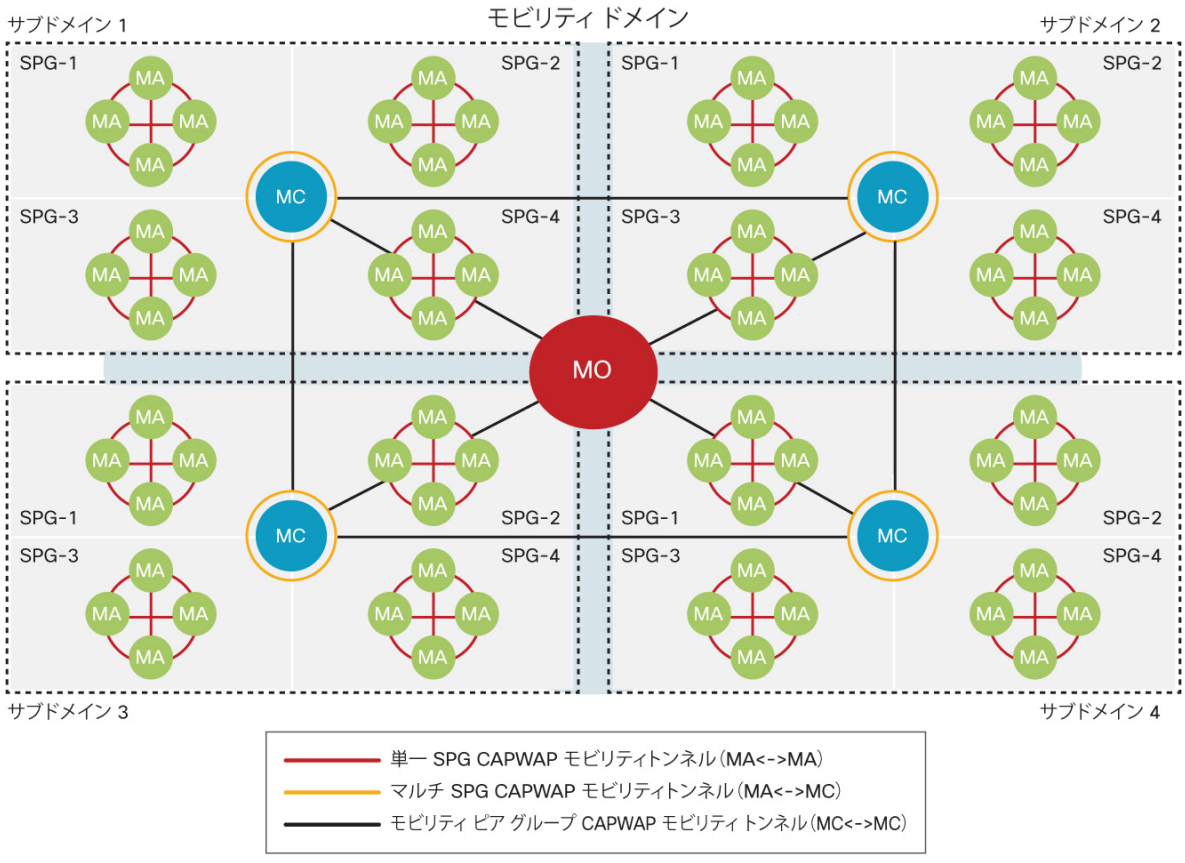
モビリティ グループ

現在の Cisco Unified Wireless Network では、モビリティ グループは、モビリティ グループのモビリティ コントローラ内のクライアントの高速ローミングを有効にするモビリティ コントローラの論理グループと定義されます。

スイッチ ピア グループ（SPG）

統合アクセス展開では、1 つのモビリティ コントローラ（またはモビリティ サブドメイン）内のモビリティ エージェントの論理グループとして、スイッチ ピア グループ（SPG）を定義します。SPG を設定する主な利点は、SPG を構成するスイッチへのローミング トラフィックを制限することです。モビリティ コントローラ上の 1 つの SPG にモバイル エージェントが設定されている場合、ソフトウェアは自動的に、モビリティ エージェント スイッチの間にフル メッシュ CAPWAP トンネルを形成します。これらの CAPWAP トンネルは、マルチレイヤ ネットワーク設計（モビリティ エージェントが VLAN 上で L2 に隣接している場合）、またはルーテッド アクセス設計（モビリティ エージェントのスイッチが L3 に隣接している場合）内に形成できます。（図 8 を参照）。

図 8　統合アクセスの階層的なロール

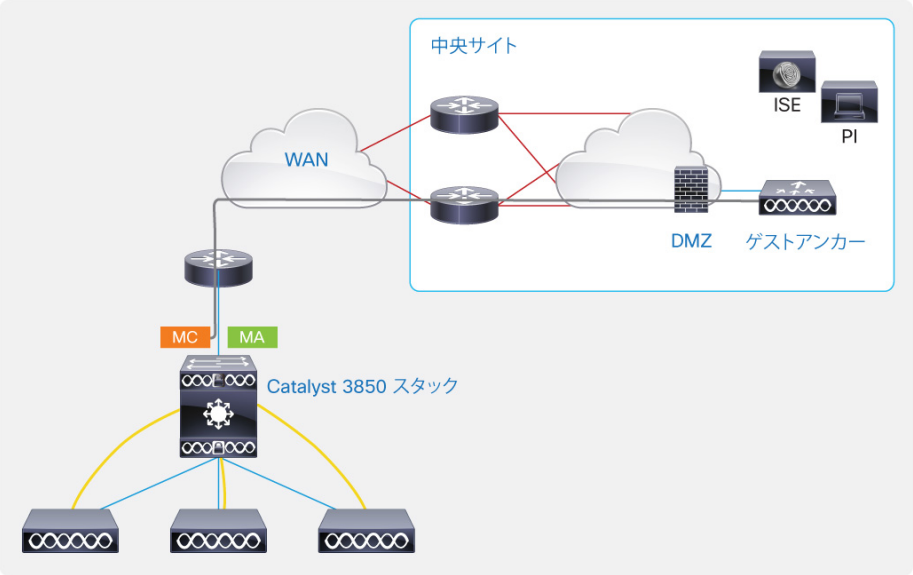


SPG は、ユーザが頻繁にローミングするモバイル エージェント スイッチのグループとして設計されています。SPC 上でのローミングではモビリティ コントローラを通過するトラフィックが必要ですが、SPG 内のローミングがその SPG でローカルで行われ、モビリティ コントローラを含める必要はないことが重要です。

Cisco Catalyst 3850 による統合アクセス ネットワークの設計

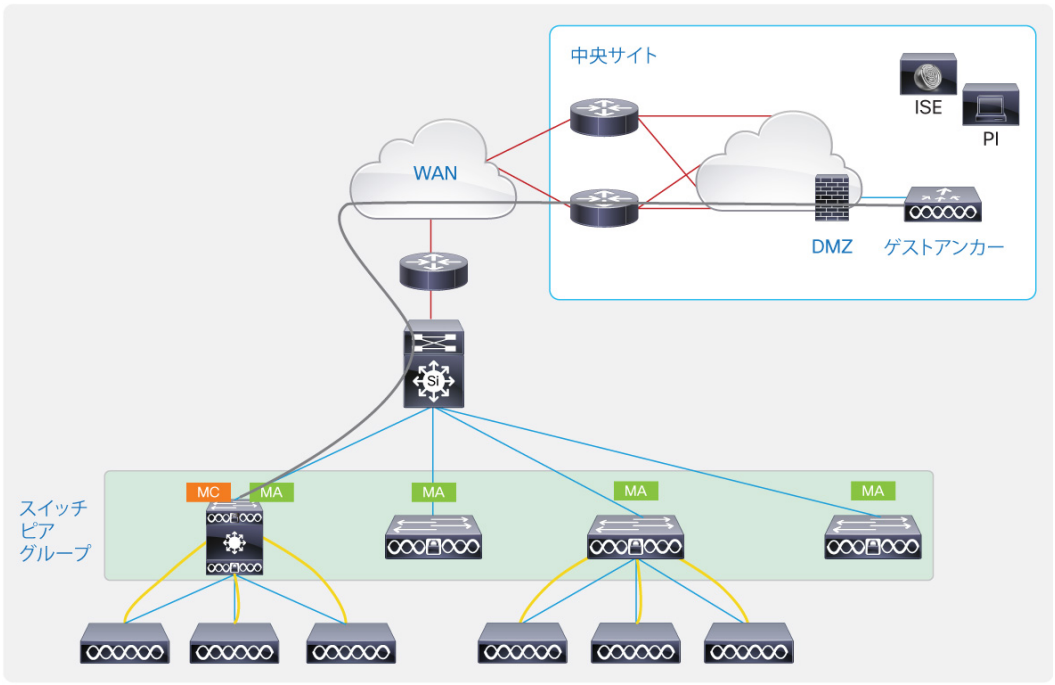
図 9 に示すように、ワイヤレスの実装がモビリティ コントローラおよび、小規模ブランチ タイプの実装に適したモビリティ エージェントとして機能する 1 台の Cisco Catalyst 3850 スイッチで構成されている場合、50 台のシスコ アクセス ポイントと 2000 台のクライアントがサポートされます。

図 9　小規模ブランチの有線/ワイヤレス向けの単一の Cisco Catalyst 3850 スタック



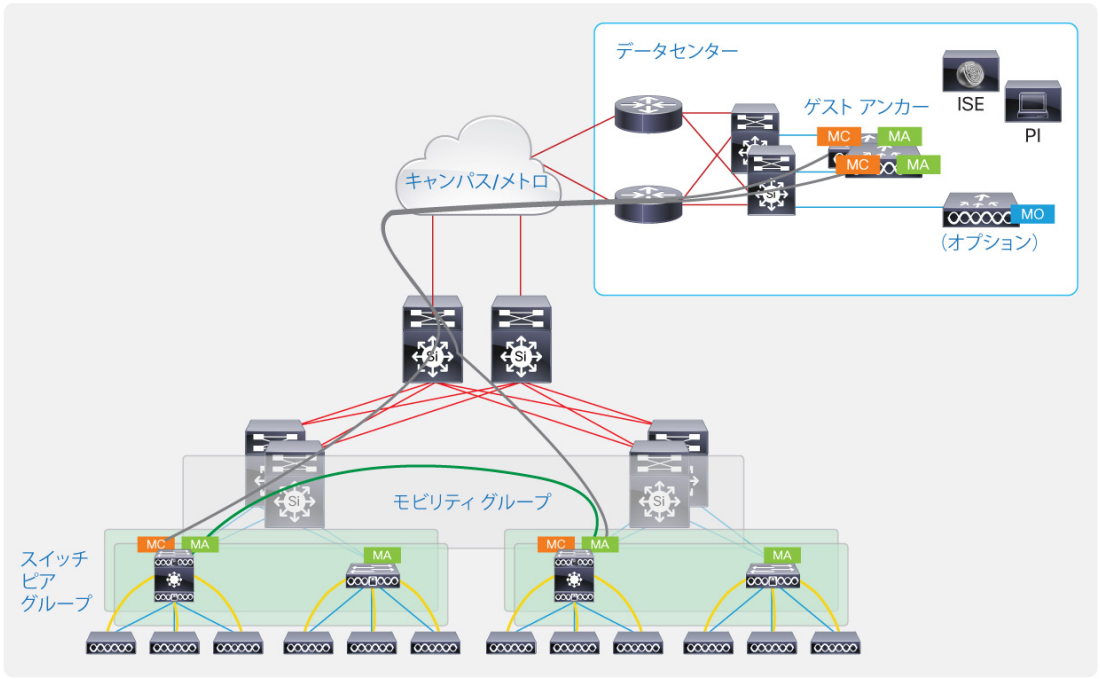
ワイヤレスの実装が、モビリティ コントローラとして動作する Cisco Catalyst 3850 スイッチ 1 台および、モビリティ エージェントとして動作するその他数台のスイッチで構成されている場合、16 台のモビリティ エージェントを、1 台のモビリティ コントローラのもとで 1 つの SPG にグループ化することができます。アクセス ポイントとクライアントの規模は、図 10 に示すように 50 台のシスコ アクセス ポイントと 2000 台のクライアントのままになります。Cisco 5508、5760 コントローラ機器、または WiSM2 サービス モジュールのみが、DMZ のゲスト アクセス コントローラ機能をサポートします。ゲスト アクセス コントローラ機能は Cisco Catalyst 3850 ではサポートされていません。

図 10　中規模から大規模ブランチの有線/ワイヤレスのための単一のモビリティ コントローラと Cisco Catalyst 3850 スイッチ



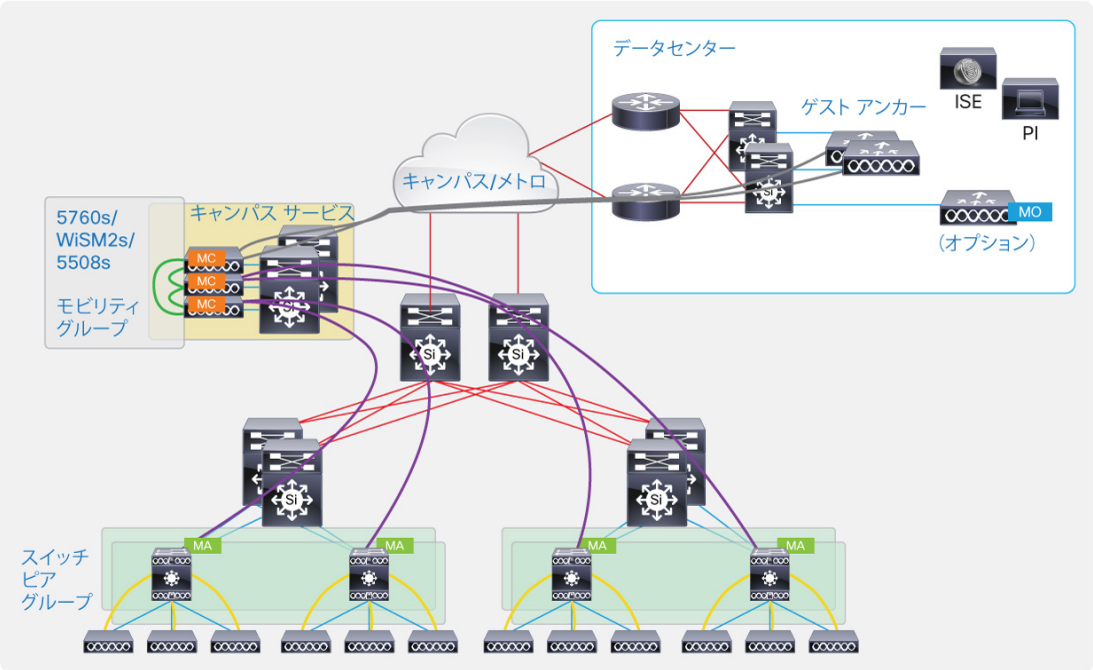
最大 250 台のシスコ アクセス ポイントと 16,000 台のクライアントの規模の中規模キャンパスのワイヤレスの実装については、図 11 に示すように、7 台のモビリティ コントローラ スイッチ（SPG のモビリティ エージェントとして動作するモビリティ エージェントスイッチ）を、DMZ のゲストのアンカー コントローラで提供されるゲスト アクセスを持つモビリティ グループにグループ化できます。動作しているゲスト アクセスがない場合は 8 台のモビリティ コントローラ スイッチをモビリティ グループにグループ化できます。

図 11　中規模から大規模のキャンパスの有線/ワイヤレスのための複数のモビリティ コントローラと Cisco Catalyst 3850 スイッチ



最大 250 台のシスコ アクセス ポイントと 16,000 台のクライアントの規模の一般的な大規模キャンパスのワイヤレスの実装については、図 12 に示すように、統合アクセスにより、Cisco Catalyst 3850 スイッチをモビリティ エージェントとして運用し、ソフトウェアをアップグレードした Cisco 5508 または WiSM2 ワイヤレス LAN コントローラ、またはモビリティ コントローラとして動作する Cisco 5760 WLC を使用してピアリングできます。

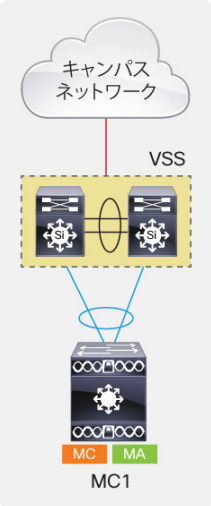
図 12　大規模なキャンパス用の Cisco Catalyst 3850 スイッチによる 5508/WiSM2/5760 コントローラ機器



Cisco Catalyst 3850 による統合アクセスの設定

ここでは、Cisco Catalyst 3850 でワイヤレス サービスを設定する方法について説明します。Cisco Catalyst 3850 スイッチのみを使用して実装可能な最大 250 台のアクセス ポイントと 16,000 台のクライアントがある大規模ブランチまたは小規模キャンパスを想定します。統合アクセスの実装は、初期フェーズでは小規模ブランチからスタートし、大規模ブランチ/中規模キャンパスでの実装にまで成長するケース スタディを使用して説明します。（図 13 を参照）。

図 13　Cisco Catalyst 3850 のモビリティ コントローラの設定



シスコのアクセス ポイントは Cisco Catalyst 3850 スイッチに直接接続する必要があります。1 台の Cisco Catalyst 3850 スイッチがアクセス レイヤを形成します。この例での分散は、仮想スイッチング システム（VSS）設定の Cisco Catalyst 4500E Supervisor 7-E システムで構成されています。アクセス中の L2 VLAN の L3 SVI が VSS システムに定義されているのは、階層型ネットワーク設計です。Cisco Catalyst 3850 はすべての VLAN を伝送する 802.1Q トランクとして設定されている L2 ポート チャネルを通じて VSS に接続します。有線クライアント用の VLAN 501、ワイヤレス クライアント用の VLAN 500、およびスイッチとワイヤレスの管理用の VLAN 601 という、3 つの VLAN が使用されます。アクセス ポイントは、ワイヤレス VLAN において、Cisco Catalyst 3850（この場合は VLAN 601）によって管理されるように設定する必要があります。

Cisco Catalyst 3850 スイッチでワイヤレス終端をイネーブルにする設定は次のようになります。

```
ap cdp
ap country US
wireless management interface Vlan601
wireless mobility controller
```

「ap cdp」コマンドは Cisco Catalyst 3850 スイッチに接続されている Cisco アクセス ポイントで CDP プロセスをイネーブルにします。「ap country US」はアクセス ポイントの国番号を定義します。「wireless management interface」コマンドは、アクセス ポイントの CAPWAP およびその他の CAPWAP モビリティ トンネルのソースとして使用されます。その次のコマンドで、統合アクセス展開のモビリティ コントローラのロールとして機能するスイッチをイネーブルにします。前述のコマンドは、スイッチを再起動する必要があります。設定を保存し、スイッチをリロードします。

初めてスイッチにアクセスポイントが加わると、Cisco Catalyst 3850 はそのアクセス ポイントにソフトウェアをダウンロードします。アクセス ポイントがスイッチに加わるためには、コードをダウンロードして再起動する必要があるため、このプロセスには長い時間がかかります。この動作は、アクセスポイントが初めてスイッチに接続する際にも行われます。その後のリロードには、このコードを使用して起動し、スイッチに加わるアクセス ポイントも含まれます。

次の手順は、ワイヤレス クライアントで使用する対応する VLAN、認証と暗号化方式、およびこの WLAN に使用する AAA サーバ プロファイルに従って、SSID を設定し、スイッチのワイヤレス LAN（WLAN）の認証を定義します。次の例では、SSID の名前は Predator で、ワイヤレス クライアントたのめに定義したクライアント VLAN 500 を使用し、TKIP で WPA、WPA2 をイネーブルにし、設定の他の場所で定義された AAA サーバで 802.1X 認証を使用しています。

オープンな SSID の場合は、WLAN 設定の後に「no security wpa」の後を設定します。事前共有キー（PSK）セキュリティの場合は、WLAN 設定で設定します。

```
wlan Predator 1 Predator
 aaa-override
 client association limit 2000
 client vlan 500
 security wpa wpa2 ciphers tkip
 security dot1x authentication-list ise
 no shutdown
 no security wpa akm dot1x
 security wpa akm psk set-key ascii 0 skunkworks
```

Cisco Catalyst 3850 のワイヤレス設定に関する出力からの抜粋を、次に示します。

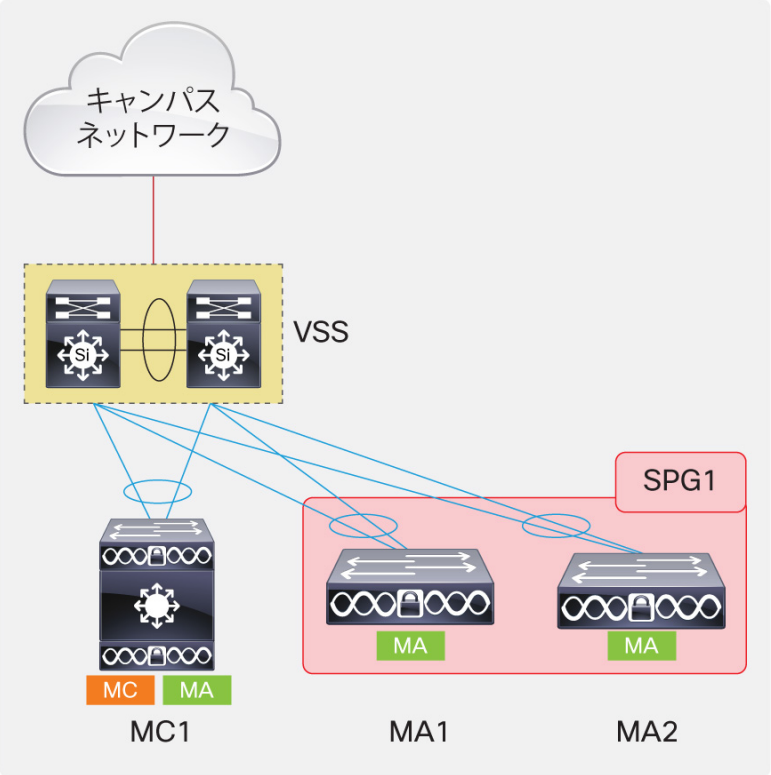
```
MC1#show wireless mobility summary
Mobility Controller Summary:
```

```
Mobility Role                                    : Mobility Controller
Mobility Protocol Port                           : 16666
Mobility Group Name                              : default
Controllers configured in the Mobility Domain:
IP              Public IP       Group Name       Multicast IP
Link Status
------------------------------------------------------------------------------
-
20.1.3.2        -               default              -          UP    : UP

MC1#show wlan summary
Number of WLANs: 1
WLAN Profile Name                SSID                          VLAN    Status
------------------------------------------------------------------------------
1    Predator                    Predator                       500      UP
MC1#show capwap summary
CAPWAP Tunnels General Statistics:
  Number of Capwap Data Tunnels       = 2
  Number of Capwap Mobility Tunnels   = 0
  Number of Capwap Multicast Tunnels  = 0
Name   APName                           Type PhyPortIf Mode       McastIf
------ -------------------------------- ---- --------- ---------- -------
Ca5    3502E_G2/0/25_83A9               data Gi2/0/25  unicast    -
Ca4    3602I_G2/0/1_3A04                data Gi2/0/1   unicast    -
Name   SrcIP           SrcPort DestIP          DstPort DtlsEn MTU
------ --------------- ------- --------------- ------- ------ -----
Ca5    20.1.3.2        5247    20.1.3.54       63548   No     1657
Ca4    20.1.3.2        5247    20.1.3.53       58274   No     1657
```

この出力は、2 種類のデータ CAPWAP トンネルが、シスコ アクセス ポイント、GigabitEthernet 2/0/25（スタックの 2 番目のスイッチ）の 3502E、および GigabitEthernet 2/0/1 の 3602I によって形作られることを示しています。20.1.3.2 は、このスイッチのスイッチ/ワイヤレス管理 IP アドレスです。「show capwap summary」の出力の最後の部分は、宛先ポート 63584 上の 20.1.3.54 および宛先ポート 58274 上の 20.1.3.53 としてリストされた IP アドレスのアクセス ポイントを持つデータ CAPWAP トンネルをスイッチが形作るソース IP アドレスを示します。

1 スイッチのスタック ネットワークの利用の増加を考慮すると、ネットワーク管理者はさらに Cisco Catalyst 3850 スイッチを追加して、より多くのエンドポイントとデバイスにワイヤレス カバレッジを拡張する必要があります。（図 14 を参照）。

図 14　Cisco Catalyst 3850 のモビリティ エージェントとスイッチのピア グループの設定



この場合、追加の Cisco Catalyst 3850 スイッチは、すでにモビリティ コントローラとして設定されたスイッチを含むモバイル エージェントとして追加および設定できます。モビリティ エージェントは 1 つの SPG 内に設定できます。

モビリティ コントローラに関連する設定を次に示します。

```
wireless mobility controller peer-group SPG1
wireless mobility controller peer-group SPG1 member ip 20.1.5.2 public-ip
20.1.5.2
wireless mobility controller peer-group SPG1 member ip 20.1.7.2 public-ip
20.1.7.2
```

この SPG および SPG1 はモビリティ コントローラで定義されます。20.1.5.2 と 20.1.7.2 は SPG1 のメンバとして設定されているモビリティ エージェントのスイッチ/ワイヤレス管理 IP アドレスです。

モビリティ エージェントのスイッチで、モビリティ コントローラ、SSID、WLAN、および認証方式を設定します。次は、前述のネットワーク図で示した MA1 スイッチ上に表示される設定です。

```
wireless mobility controller ip 20.1.3.2 public-ip 20.1.3.2
wireless management interface Vlan602
wlan Predator 1 Predator
 aaa-override
 client association limit 2000
 client vlan 500
 security wpa wpa2 ciphers tkip
 security dot1x authentication-list ise
 no shutdown
ap cdp
```

ここで 20.1.3.2 はモビリティ コントローラ スイッチのスイッチ/ワイヤレス管理 IP アドレス、VLAN 602 はスイッチ/ワイヤレス管理インターフェイス、VLAN 500 はモビリティ コントローラ スイッチからスパンされたクライアント VLAN です。

次に示すように、MA2 スイッチの SPG1 の他のメンバで類似の設定を行うことができます。

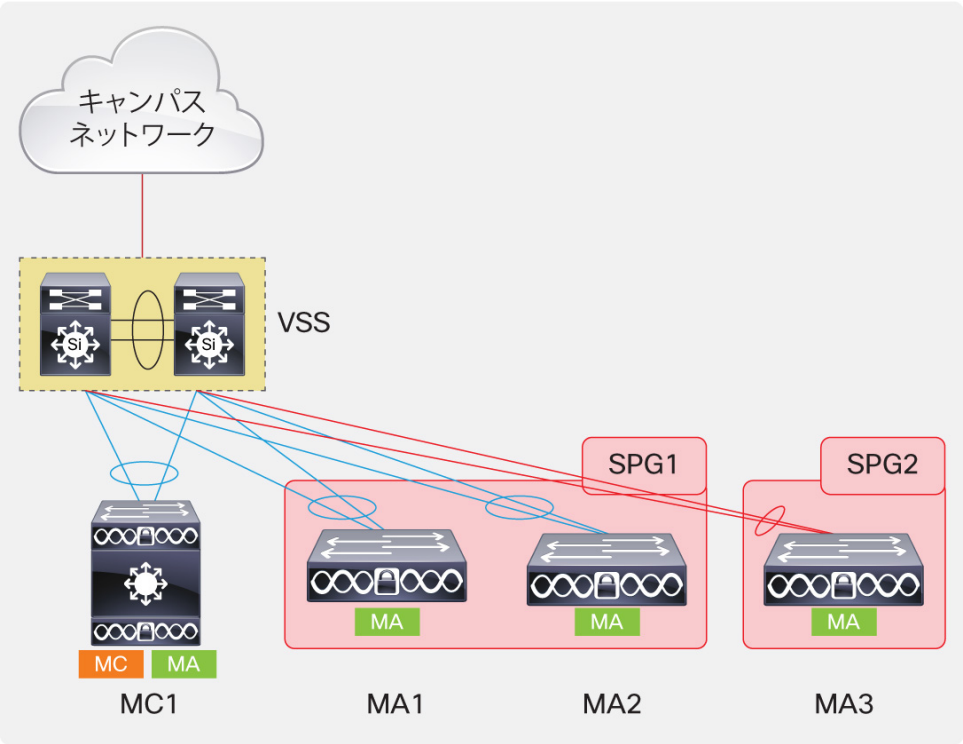
```
wireless mobility controller ip 20.1.3.2 public-ip 20.1.3.2
wireless management interface Vlan603
wlan Predator 1 Predator
 client vlan 500
 security wpa wpa2 ciphers tkip
 security dot1x authentication-list ise
 no shutdown
ap cdp
```

ここで 20.1.3.2 はモビリティ コントローラ スイッチのスイッチ/ワイヤレス管理 IP アドレス、VLAN 603 はワイヤレス管理インターフェイス、VLAN 500 はモビリティ コントローラ スイッチからスパンされたクライアント VLAN です。

SPG 定義および SPG のメンバーシップがモビリティ コントローラ スイッチだけに設定されていることに注意してください。モビリティ コントローラ定義だけが実際のモビリティ エージェントのスイッチに設定されます。

モビリティ コントローラに定義された SPG のメンバーシップは、モビリティ コントローラとモビリティ エージェントのスイッチ間の接続には関係ありません。アクセス ネットワークは、分散にレイヤ 2 接続されている場合や、分散へのルーテッド アクセス設計内で動作している可能性があります。(図 15 を参照)。

図 15　Cisco Catalyst 3850 の複数のモビリティ コントローラのモビリティ グループの設定



隣の会社を買収したために、現在のネットワーク内で 2 つのネットワークを統合しなければならないと仮定します。買収した企業のネットワークは、図で示すように、ルーテッド アクセス設計モードで動作します。新しいスイッチは、ネットワーク内の事前に定義されたモビリティ コントローラ スイッチの下でモビリティ エージェントを実行するように設定できます。

SPG メンバーシップに関しては、選択肢があります。2 つのユーザ グループを統合しようとする場合、またはローミングを単純にしておきたい場合は、Cisco Catalyst 3850 を基礎とするモビリティ コントローラで設定できる SPG は 1 つのみです。Cisco Catalyst 3850 のモビリティ コントローラ スイッチで定義された SPG は、1 台につき最大 16 のメンバのモビリティ エージェントを含むことができます。

もうひとつの選択肢は、モビリティ コントローラ スイッチに別の SPG を作成し、この新しい SPG に新しいモビリティ エージェント スイッチを挿入することです。現在の会社と買収された企業のユーザ グループがそれぞれのワークスペースでローミングしない場合、新しい SPG を作成できます。上記のネットワーク例では、ネットワーク管理者が 2 番目の SPG を作成することを選択します。クライアント上でのローミングの影響を説明するには、この仮定が便利です。

この場合にモビリティ コントローラで実行する必要のある設定を次に示します。

```
wireless mobility controller peer-group SPG2
wireless mobility controller peer-group SPG2 member ip 20.1.8.2 public-ip
20.1.8.2
```

この SPG および SPG2 はモビリティ コントローラで定義されます。20.1.8.2 は SPG2 のメンバとして設定されているモビリティ エージェント スイッチのスイッチ/ワイヤレス管理 IP アドレスです。

この場合に MA3 スイッチで実行する設定を次に示します。

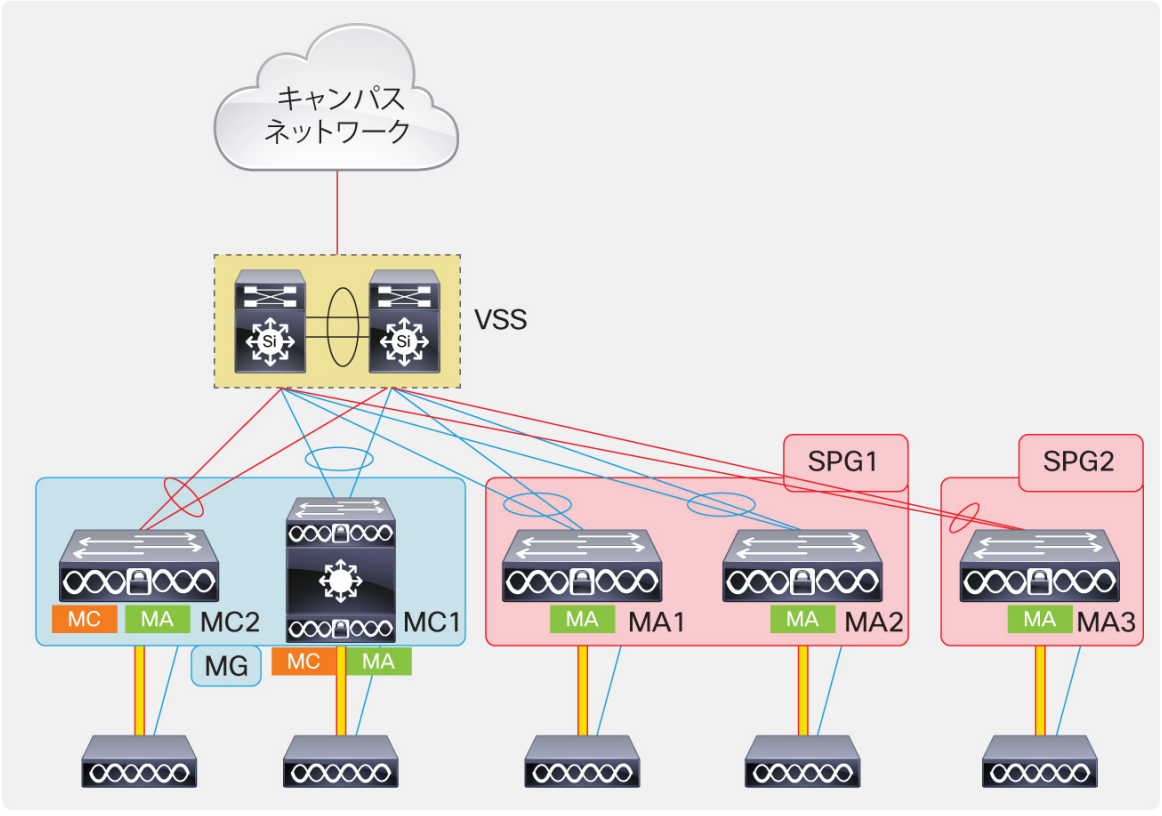
```
wireless mobility controller ip 20.1.3.2 public-ip 20.1.3.2
wireless management interface Vlan604
```

```
wlan Predator 1 Predator
 aaa-override
 client vlan 701
 security wpa wpa2 ciphers tkip
 security dot1x authentication-list ise
 no shutdown
ap cdp
```

ここで 20.1.3.2 はモビリティ コントローラ スイッチのスイッチ/ワイヤレス管理 IP アドレス、VLAN 604 はワイヤレス管理インターフェイス、VLAN 701 はルーテッド アクセス モードで動作するモビリティ エージェント上のクライアント VLAN です。

事業が順調であり、会社の業績がこれまでよりも成長しているとします。小規模ブランチとして始まったものがより大規模なブランチに発展し、50 以上のアクセス ポイントへの拡張が必要になっています。このブランチ内には 1 台しかモビリティ コントローラ スイッチがないため、実装可能なアクセス ポイントは 50 台に限られます。ネットワーク管理者は、50 台のアクセス ポイントに類似した実装をサポートするモビリティ コントローラとして動作する別の Cisco Catalyst 3850 スイッチを設定できます。（図 16 を参照）。

図 16　Cisco Catalyst 3850 での複数のモビリティ コントローラ設定



これら 2 つのモビリティ コントローラ スイッチを 1 個のモビリティ グループにグループ化することで、それぞれのサブドメインのクライアント間の高速ローミングを有効にできます。

既存のモビリティ コントローラ スイッチで行う必要がある設定を、次に示します。

```
wireless mobility group member ip 20.1.9.2 public-ip 20.1.9.2 group MG
wireless mobility group name MG
```

MG は作成されるモビリティ グループ名で、20.1.9.2 はモビリティ グループに追加された新しいモビリティ コントローラのスイッチ/ワイヤレス管理 IP アドレスです。

オンラインになった新しいモビリティ コントローラ スイッチで行う必要がある設定を、次に示します。

```
wireless mobility controller
wireless mobility group member ip 20.1.3.2 public-ip 20.1.3.2 group MG
wireless mobility group name MG
wireless management interface Vlan605
wlan Predator 1 Predator
 aaa-override
 client vlan 702
 security wpa wpa2 ciphers tkip
 security dot1x authentication-list ise
 no shutdown
ap cdp
```

20.1.3.2 は既存のモビリティ コントローラ スイッチのスイッチ/ワイヤレス管理 IP アドレス、MG は作成されたモビリティ グループの名前、VLAN605 はこのモビリティ コントローラ スイッチのワイヤレス管理インターフェイスで、Predator という名前の SSID が作成されています。VLAN702 はこのスイッチのワイヤレス エンドポイントのクライアント VLAN で、認証および暗号化パラメータはこの WLAN に対して定義され、このスイッチに接続されているすべてのアクセス ポイントで CDP がイネーブルになっています。

各スイッチが 40 Gbps のワイヤレス トラフィックの終端を実行できるため、この方法は Cisco Catalyst 3850 スイッチで統合アクセスを展開するためのスケーラブルな方法です。上記のネットワークは全体として、最大 320 Gbps のワイヤレス ワイヤレス トラフィック（スイッチ 8 台（スタックの 4 台、スタンドアロンとして動作する 4 台））を終端できます。これにより、将来 802.11ac 標準が実装された場合に Cisco Catalyst 3850 スイッチの機能が保証されることが十分示されます。

Cisco Unified Wireless Network のローミング

ここでローミングについて説明する前に、Point of Presence（PoP）および Point of Attachment（PoA）で始まる統合アクセスの実装におけるローミングについての説明で使用される用語を理解しておくことが必要です。

Point of Presence（PoP）は、有線インフラストラクチャが最初にワイヤレス トラフィックを確認するネットワークのポイントとして定義されます。802.11（ワイヤレス）から 802.3（イーサネット）、またはその逆のパケット変換がここで行われます。PoP は複数の機能を提供します。これは、対称ルーティングのポイントとして、またネットワーク セキュリティ ポリシーがワイヤレス トラフィックに適用されるポイントとして機能します。Cisco Unified Wireless Network では、コントローラに PoP が定義されます。これは、ワイヤレス トラフィックがコントローラでイーサネット フレームに終端および変換され、この時点で有線インフラストラクチャがワイヤレス エンドポイントからのフレームを探すためです。

Point of Attachment（PoA）はユーザ モビリティとともに移動し、ユーザを組み合わせる、またはローミングするアクセス ポイントとして定義されます。

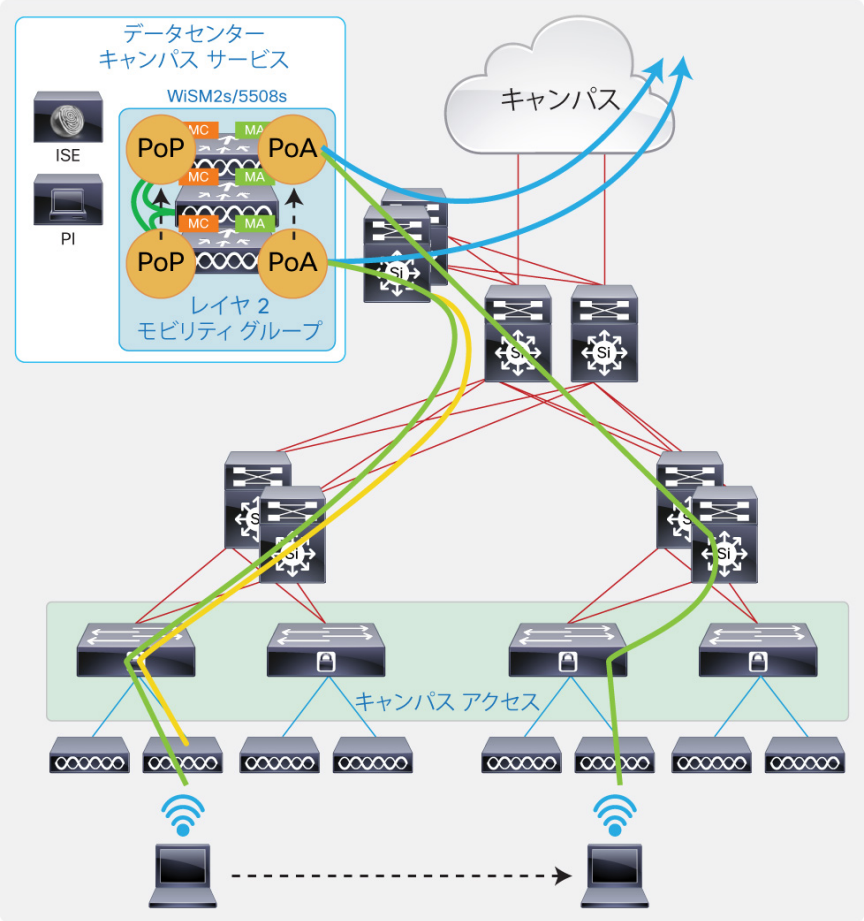
ワイヤレス ネットワーク内のローミングには、コントローラ内のローミングとコントローラ間のローミングという 2 種類があります。

- **コントローラ内のローミング**は、あるアクセス ポイントから、同じコントローラに接続されている別のアクセス ポイントへユーザがローミングすると発生します。
- **コントローラ間のローミング**は、あるコントローラに接続されているアクセス ポイントから、別のコントローラに接続されている別のアクセス ポイントへユーザがローミングすると発生します。

コントローラ間のローミングで発生する可能性のあるローミングには、L2 と L3 の 2 種類があります。

- **L2 ローミング**は、コントローラに接続されているアクセス ポイントから別のコントローラに接続されているアクセス ポイントへユーザがローミングし、この 2 台のコントローラが互いに L2 で隣接している場合に発生します。これは通常、WLC がデータセンターまたはキャンパス サービス ブロックに集中的に実装され、クライアント VLAN がコントローラ間にまたがっている場合に発生します。Cisco Unified Wireless Network の場合、L2 ローミングでは、PoP と PoA の両方が、ユーザがローミングしたコントローラに移動します。このコントローラは、クライアントのローミング先の新しいコントローラに、全体のクライアントの状況（MAC アドレス、IP アドレス、ACL ポリシー、QoS ポリシー、IGMP グループ メンバーシップなど）を転送します。（図 17 を参照）

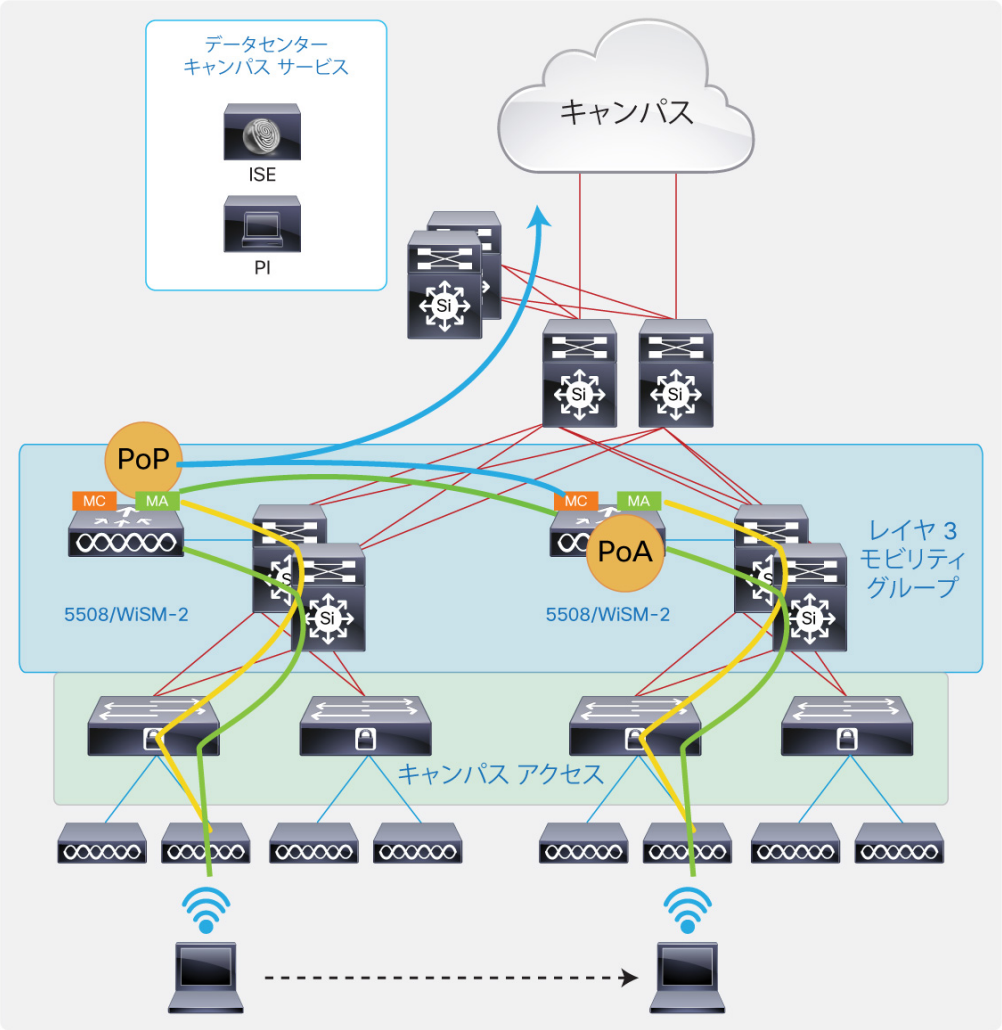
図 17　Cisco Unified Wireless Network の L2 ローミング



前述のコントローラは、別のコントローラへローミングしたクライアントの状態を保持しません。この場合は、クライアント トラフィックはアクセス ポイントで CAPWAP カプセル化され、アクセス ポイントが関連づけられている新しいコントローラで終端されます。

- **L3 ローミング**は、コントローラに接続されているアクセス ポイントから別のコントローラに接続されているアクセス ポイントへユーザがローミングし、この 2 台のコントローラが互いに L3 で隣接している場合に発生します。（図 18 を参照）

図 18　Cisco Unified Wireless Network の L3 ローミング



これは、個々のコントローラがキャンパス ネットワークの各ディストリビューション ブロックに実装され、クライアント VLAN がコントローラ間にまたがっていない場合です。既存の Cisco Unified Wireless Network では、PoA のみがユーザのモビリティとともに移動し、PoA はクライアントが最初に加わった最初のコントローラに残ります。この場合、PoP はアンカー コントローラと呼び、PoA は外部コントローラと呼びます。アンカー コントローラと外部コントローラはクライアントの状態を保持します。これは、クライアントが別のコントローラに物理的に移動しても、対称ルーティングおよびポリシーの適用のアンカーでトラフィックが送り返されるためです。

統合アクセスにおけるローミングに関する理解

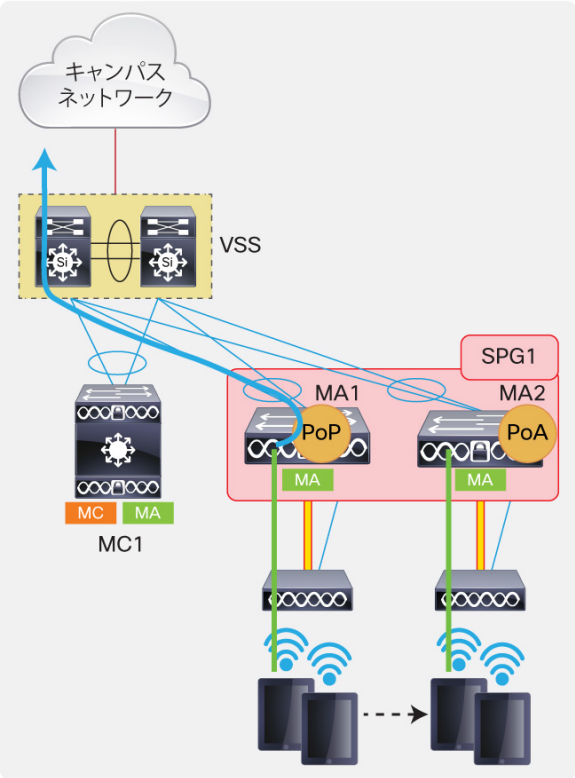
Cisco Unified Wireless Network におけるローミングについては前述しているため、このセクションでは統合アクセス モードで発生するローミングについて説明します。統合アクセスの実装におけるローミングと、既存の Cisco Unified Wireless Network で発生するローミングの間に違いがないことが分かるでしょう。統合アクセスの実装では、QoS ポリシーは外部のスイッチまたは PoA のスイッチで適用され、ACL ポリシーはアンカーまたは PoP スイッチで適用されます。

統合アクセス モードでは、トンネリング（スティッキ）モードと非トンネリング（非スティッキ）モードという 2 種類のローミング方法がサポートされています。

トンネリング モードは L2 のローミングをサポートするデフォルトの方式で、統合アクセスの実装において L3 をサポートする唯一の方式です。これは、L2 ローミングでも PoA はデフォルトでユーザ モビリティとともに移動し、PoP はステートフルなポリシー アプリケーションのアンカー スイッチで管理されることを意味します。

図 19 は、分散 VSS にスイッチがトランクとして設定され、クライアントのワイヤレス VLAN 500 が複数のアクセス スイッチにまたがっていることを示しています。最初のクライアント接続は MA1 スイッチで行われます。最初のクライアント トラフィック プロファイルはスイッチに CAPWAP カプセル化されます。スイッチは、ワイヤレス トラフィックを終端し、変換されたイーサネット フレームを送信します。したがって、PoP と PoA の両方は最初のクライアント接続用の MA1 にあります。クライアントが MA2 にローミングすると、前述のように PoP は MA1 にとどまり、PoA は MA2 に移動します。したがって、ローミングされたトラフィックは新しいモビリティ エージェントに CAPWAP カプセル化されます。新しいモビリティ エージェントは、フル メッシュ SPG1 トンネル上のトラフィックを PoP スイッチにカプセル化します。PoP スイッチに到着すると、トラフィックは終端および変換され、MA1 によって有線で送信されます。クライアントが SPG 内でローミングするため、ローミングされたトラフィックがモビリティ コントローラ スイッチを通過する必要はありません。通常、SPG は建物内の分散ブロック内のスイッチまたはフロア、すなわちほとんどのユーザがローミングするエリアに形成されます。

図 19　統合アクセスでのトンネリング モードでの L2 ローミング



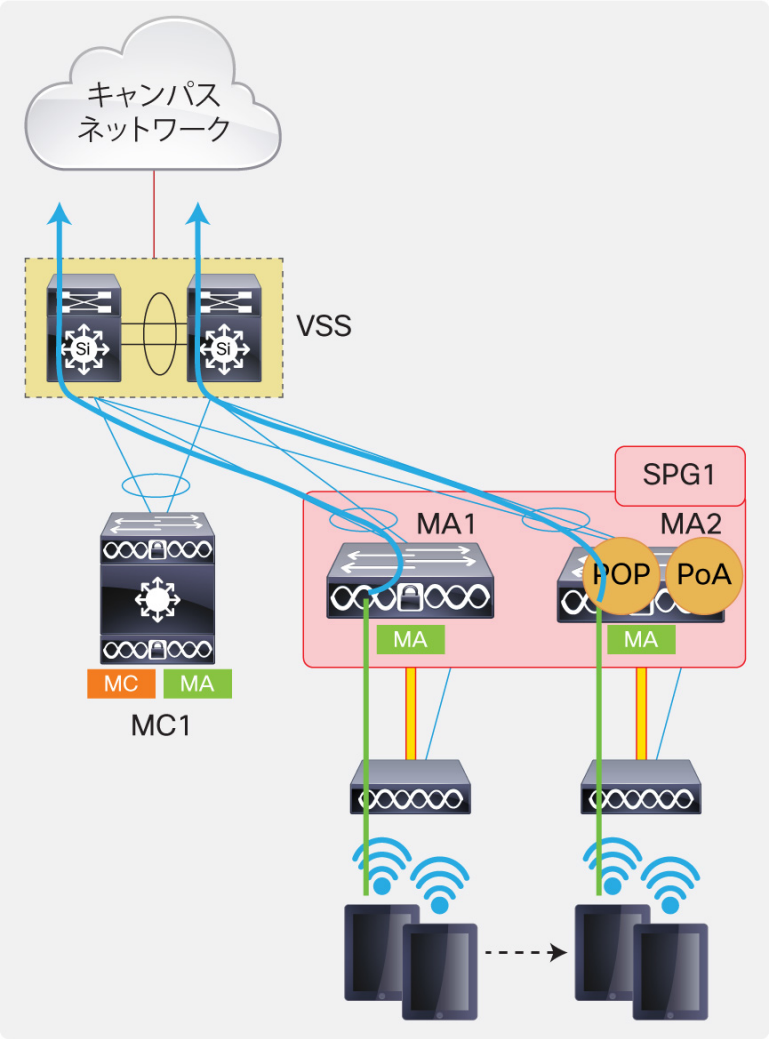
WLAN ごとに、ユーザの PoP と PoA の両方が移動する Cisco Unified Wireless Network のような L2 移動が必要な場合は、WLAN ごとに管理者が設定できるようになっています。これは非トンネリング（非スティッキ）L2 ローミングです。

このローミングのメリットは、PoP がユーザ モビリティとともに移動するため、ローミングされたトラフィックを PoP のスイッチに送り返す必要がないことです。ローミングされたトラフィックは、新しいモビリティ エージェントでローカルで終端されて有線で配信されるため、アプリケーション トラフィックの遅延が短縮されます。このローミングのタイプにより、アプリケーションの遅延は短縮されますが、クライアントのローミング時間が増加する可能性があります。

図 20 で示すとおり、MA1 に最初のクライアントが接続されます。このワイヤレス トラフィックはローカルで終端され、有線に切り替わります。クライアントが MA2 に接続されたアクセス ポイントにローミングすると、PoP と PoA の両方が新しいモビリティ エージェント スイッチに移動します。クライアントの状態は、クライアントが最初に結合された MA1 では維持されません。

このローミングは、既存の Cisco Unified Wireless Network L2 ローミングと同じです。

図 20　統合アクセスでの非トンネリング モードでの L2 ローミング

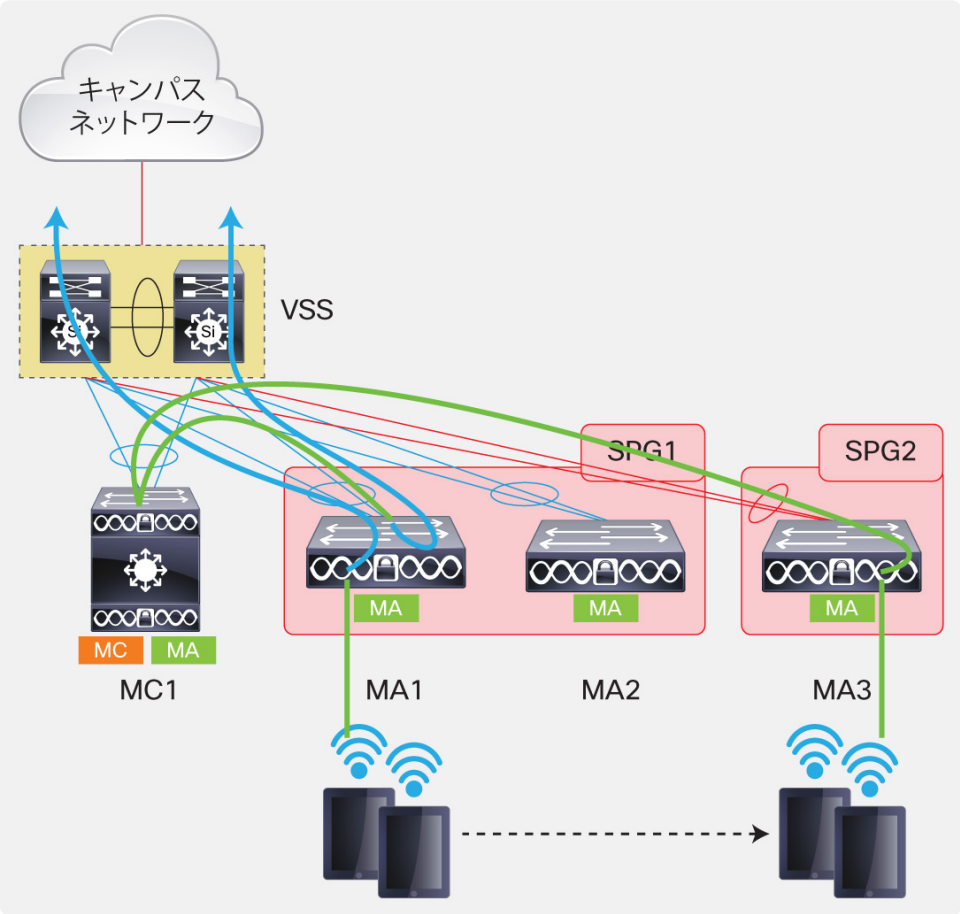


前述のとおり、L3 ローミングはトンネリング（スティッキ）方式でサポートされます。

統合アクセスにおけるトラフィック パス

このセクションでは、異なる SPG とモビリティ コントローラにまたがる、ローカルおよびローミングされたワイヤレス クライアントのトラフィック パス（プロファイル）について説明します。（図 21 を参照）。

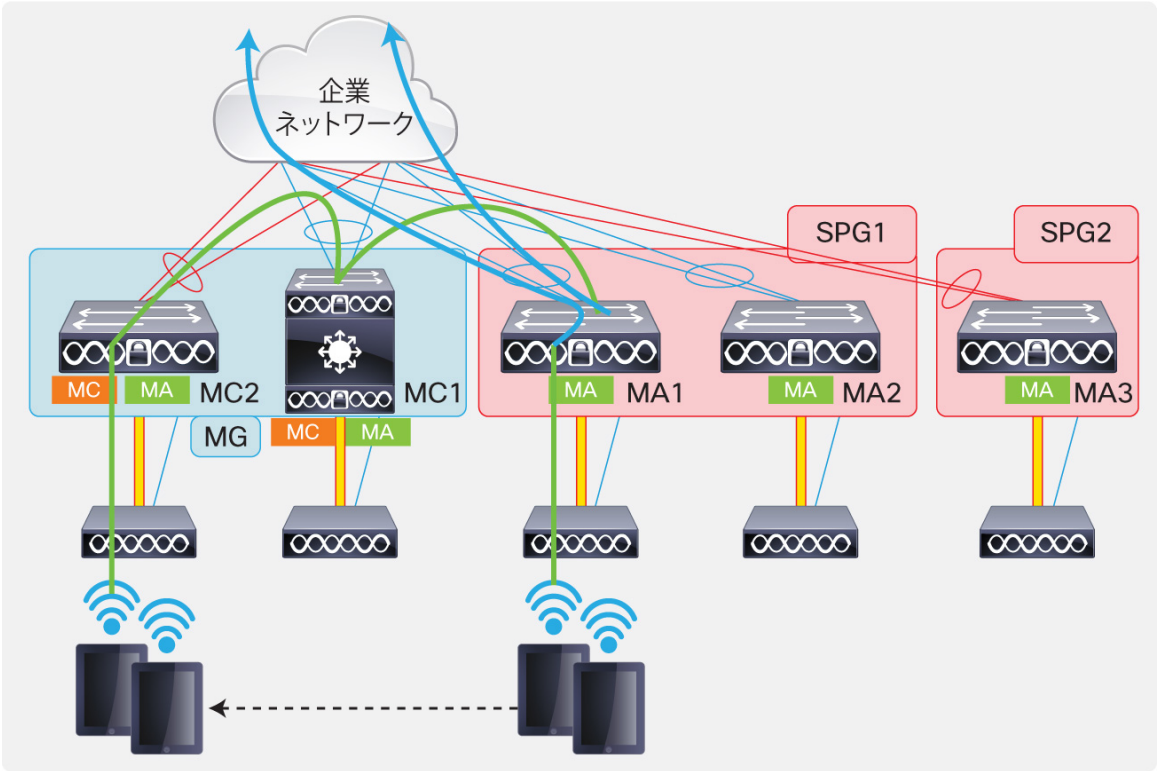
図 21　統合されたアクセスの SPG 内でのクライアントのローミング



前述のとおり、SPG 内でのローミングは SPG のアンカー スイッチおよび外部スイッチ内に制限されます。

前述のとおり、SPG を通してローミングされるワイヤレス クライアントのトラフィックは、モビリティ コントローラを経由しなければなりません。モビリティ コントローラが SPG 経由でローミングされるトラフィックのルーティングを行うとします。図 21 では、クライアントは SPG1 の最初の MA1 から SPG2 の MA3 にローミングしています。この場合、ローミングされたトラフィックは、モビリティ エージェントとモビリティ コントローラの間の CAPWAP トンネル内の新しいモビリティ エージェントで終端およびカプセル化され、MC1 にスイッチングされます。モビリティ コントローラはこのクライアントのアンカー（PoP）スイッチを認識し、トラフィックをカプセル化して、アンカー（MA1）にスイッチングします。アンカー スイッチは、このトラフィックに ACL を適用し、ローミングが L3 ローミングの場合には対称ルーティングを行います。（図 22 を参照）。

図 22　統合されたアクセスのモビリティ コントローラをまたぐクライアントのローミング



上記のシナリオでは、サブドメイン間（モビリティ コントローラ間）でのローミングについて説明します。最初のクライアント接続は SPG1 の MA1 で行われます。ワイヤレス トラフィックは MA1 でローカルで終端され、クライアントが静的なときに有線側に送信されます。クライアントが MC2 に接続されたアクセス ポイントにローミングすると、そのアクセス ポイントはマスターが MC1 であるサブドメインにローミングを行います。この場合、ローミングされたクライアントのトラフィック パスは外部（PoA）MC2 スイッチで終端されます。外部（PoA）MC2 スイッチは、モビリティ コントローラとモビリティ コントローラ間の CAPWAP トンネルにこのトラフィックをカプセル化し、MC1 にトラフィックを切替えます。このスイッチは、モビリティ コントローラとモビリティ エージェント間の CAPWAP トンネルにこのトラフィックをカプセル化し、アンカー（PoP）MA1 スイッチにトラフィックを送り返します。ACL ポリシーはアンカー スイッチ（MA1）に適用されるため、このスイッチはトラフィックをネットワークの有線部分に転送します。

統合アクセスにおけるクライアントのローミングを追跡するための出力

このセクションでは、前述のすべての理論を実際にどのように表示されるかを説明します。ここでは、ワイヤレス ネットワークに最初に接続されるワイヤレス クライアントの出力について説明し、その後ワイヤレス ネットワークを通じてローミングされる出力について説明します。

ワイヤレス クライアント VLAN は、3 台のスイッチ（MC1、MA1 および MA2）にまたがっています。4 番目のモビリティ エージェントのスイッチ（MA3）は、クライアントのワイヤレス VLAN がまたぐことのできないルーテッド アクセス設計にあります。

2 番目のモビリティ コントローラのスイッチ（MC2）も、クライアントのワイヤレス VLAN がまたぐことのできないルーテッド アクセス設計です。

統合アクセスの L2 ローミングはデフォルトでトンネリングされます。このネットワーク例では、最初にトンネリング L2 ローミング、次に L3 ローミング、最後に非トンネリング L2 ローミングが発生するシナリオについて説明します。

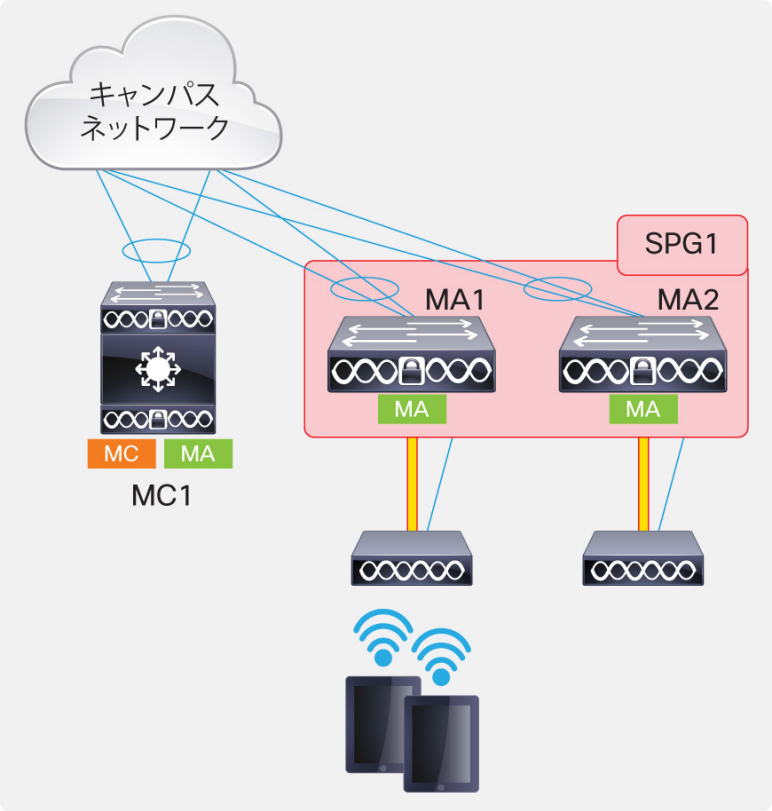
表 3 は、ネットワーク例を構成するスイッチ名、IP アドレス、SPG におけるスイッチのロール、およびモビリティ グループのリストです。これを理解することにより、あるスイッチから別のスイッチへローミングするクライアントのローミングの説明が可能になります。

表 3　トポロジ例におけるスイッチのロールとその他の詳細

スイッチ名	IP アドレス	モビリティ ロール	スイッチのピア グループ	モビリティ グループ
MC1	20.1.3.2	モビリティ コントローラ	-	MG
MA1	20.1.5.2	モビリティ エージェント	SPG1	MG
MA2	20.1.7.2	モビリティ エージェント	SPG1	MG
MA3	20.1.8.2	モビリティ エージェント	SPG2	MG
MC2	20.1.9.2	モビリティ コントローラ	-	MG

図 23 は MA1 の最初のクライアント接続を示します。

図 23　MA1 の最初のクライアント接続




```
MA1#show wireless client summary
Number of Local Clients : 2
MAC Address     AP Name                          WLAN State            Protocol
-------------------------------------------------------------------------------
b065.bdb0.a1ad 3602I_G1/0/1_66BC                  1     UP              11n(5)
b065.bdbf.77a3 3602I_G1/0/1_66BC                  1     UP              11n(5)
```

スイッチ上の CLI に表示される MA1 の最初のクライアント接続。アクセス ポイントが接続されているクライアントの MAC アドレス、5GHz の WLAN および 11n クライアントの MAC アドレスが示されています。

```
MA1#show wcdb database all
  Total Number of Wireless Clients = 2
       Clients Waiting to Join    = 0
       Local Clients              = 2
       Anchor Clients             = 0
```

```
        Foreign Clients            = 0
        MTE Clients                = 0

Mac Address    VlanId IP Address      Src If              Auth     Mob
-------------- ------ --------------- ------------------- -------- -------
b065.bdbf.77a3    500 20.1.1.53       0x00DC7DC000000005 RUN      LOCAL
b065.bdb0.a1ad    500 20.1.1.52       0x00DC7DC000000005 RUN      LOCAL

MA1#show wireless client mac b065.bdbf.77a3 detail
Client MAC Address : b065.bdbf.77a3
Client Username : blackbird
AP MAC Address : 203a.076f.abe0
AP Name: 3602I_G1/0/1_66BC
Client State : Associated
Wireless LAN Id : 1
Wireless LAN Name: Predator
Protocol : 802.11n - 5 GHz
Channel : 157
IPv4 Address : 20.1.1.53
Mobility State : Local
EAP Type : PEAP
Interface : WIRELESS_VLAN
VLAN : 500
Access VLAN : 500

MA1#show mac address dynamic | include Ca1
 Vlan    MAC Address          Type        Ports
-----    -----------       -------     -----
 500     b065.bdb0.a1ad    DYNAMIC     Ca1
 500     b065.bdbf.77a3    DYNAMIC     Ca1
```

「Ca1」はアクセス ポイントの CAPWAP データ トンネルで、クライアントの MAC アドレスが Ca1 インターフェイスの背後に表示されることを示します。

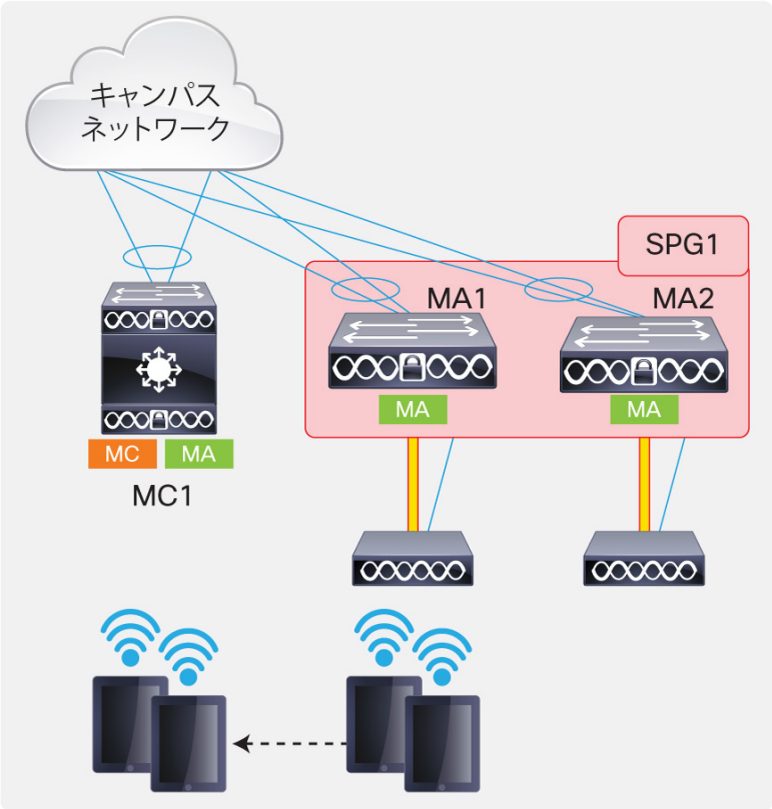
前述のとおり、モビリティ コントローラにすべてのモビリティ エージェントに関するすべてのクライアントの可視性があるため、モビリティ エージェント上のローカルのクライアントのモビリティ コントローラのクライアントの可視性 CLI を次に示します。

```
MC1#sh wireless mobility controller client summary
Number of Clients : 2
State is the Sub-Domain state of the client.
* indicates IP of the associated Sub-domain
Associated Time in hours:minutes:seconds
MAC Address      State      Anchor IP      Associated IP    Associated Time
-------------------------------------------------------------------------
b065.bdb0.a1ad  Local      0.0.0.0        20.1.5.2         00:00:23
b065.bdbf.77a3  Local      0.0.0.0        20.1.5.2         00:00:35
```

IP アドレスが 20.1.5.2（MA1）のモビリティ エージェントのスイッチ上でこれらのクライアントがローカルで接続されていることが、アンカー IP 0.0.0.0 で示されていることに注意してください。

クライアントがモビリティ エージェントからモビリティ コントローラのスイッチ（図 24）にローミングした場合を想定します。

図 24　統合されたアクセスの SPG 内でのクライアントのローミング



クライアントのローミングを示す出力を次に示します。この場合、MA1 はアンカー スイッチになり、MC1 は外部スイッチになります。

```
MC1#show wireless client summary
Number of Local Clients : 2
MAC Address    AP Name                          WLAN State          Protocol
-------------------------------------------------------------------------------
b065.bdb0.a1ad 3602I_G2/0/1_3A04                 1    UP             11n(5)
b065.bdbf.77a3 3602I_G2/0/1_3A04                 1    UP             11n(5)

MC1#show wcdb database all
  Total Number of Wireless Clients = 2
       Foreign Clients           = 2
       MTE Clients               = 0

Mac Address    VlanId IP Address      Src If             Auth     Mob
-------------- ------ --------------- ------------------ -------- -------
b065.bdbf.77a3    500 20.1.1.53       0x00E685C000000006 RUN      FOREIGN
b065.bdb0.a1ad    500 20.1.1.52       0x00E685C000000006 RUN      FOREIGN
MC1#show wireless client mac b065.bdbf.77a3 detail
Client MAC Address : b065.bdbf.77a3
Client Username : blackbird
AP MAC Address : 8875.5687.b830
AP Name: 3602I_G2/0/1_3A04
Wireless LAN Name: Predator
Protocol : 802.11n - 5 GHz
IPv4 Address : 20.1.1.53
Mobility State : Foreign
Mobility Anchor IP Address : 20.1.5.2
Mobility Move Count : 1
Interface : WIRELESS_VLAN
VLAN : 500
```

クライアントがローミングするスイッチのクライアント データベースのモビリティの状態が「外部」であることに注意してください。また、ローミング先のスイッチに関するクライアントの詳細が、ローカルのアクセス ポイント名、モビリティの状態、およびモビリティ アンカーの IP アドレス(20.1.5.2)を示していることに注意してください。20.1.5.2 は、クライアントが最初に結合されたスイッチのスイッチ/ワイヤレス管理スイッチ(MA1)です。

アンカー スイッチ(この場合は MA1)の出力を次に示します。

```
MA1#show wireless client summary
Number of Local Clients : 2
MAC Address    AP Name                        WLAN State            Protocol
-------------------------------------------------------------------------------
b065.bdb0.a1ad 20.1.3.2                       1    UP               Mobile
b065.bdbf.77a3 20.1.3.2                       1    UP               Mobile
```

最初のクライアント接続の出力と前述の出力を比較する際は、クライアントがローミングしたスイッチの IP アドレス(この場合は MC1 のスイッチ/ワイヤレス管理 IP アドレス)にアクセス ポイント名が変更され、プロトコルのステータスが「Mobile」に変わることに注意してください。

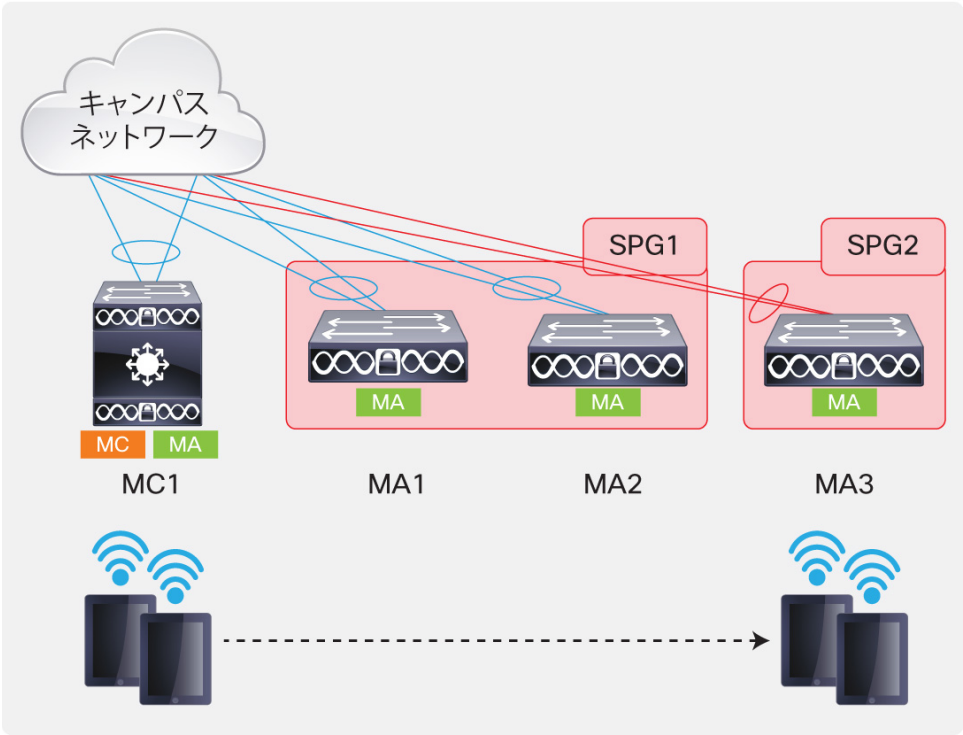
```
MA1#sh wcdb data all
  Total Number of Wireless Clients = 2
       Clients Waiting to Join   = 0
       Local Clients             = 0
       Anchor Clients            = 2
       Foreign Clients           = 0
       MTE Clients               = 0
Mac Address    VlanId IP Address      Src If             Auth     Mob
-------------- ------ --------------- ------------------ -------- -------
b065.bdbf.77a3    500 20.1.1.53       0x00D03BC000000002 RUN      ANCHOR
b065.bdb0.a1ad    500 20.1.1.52       0x00D03BC000000002 RUN      ANCHOR
```

アンカー スイッチ（MA1）に関するクライアントの詳細を示す出力を次に示します。

```
MA1#sh wireless client mac b065.bdbf.77a3 detail
Client MAC Address : b065.bdbf.77a3
Client Username : blackbird
AP MAC Address : 0000.0000.0000
AP Name: 20.1.3.2
Client State : Associated
Wireless LAN Id : 1
Wireless LAN Name: Predator
Protocol : Mobile
Channel :
IPv4 Address : 20.1.1.53
Mobility State : Anchor
Mobility Foreign IP Address : 20.1.3.2
Interface : WIRELESS_VLAN
VLAN : 500
Access VLAN : 500
```

ここでは、モビリティの状態が「anchor」で、アクセス ポイント名は外部スイッチ（MC1）のスイッチ/ワイヤレス管理 IP アドレス（20.1.3.2）です。（図 25 を参照）。

図 25　統合されたアクセスの SPG 上でのクライアントのローミング



前述のシナリオでは、エンドポイントは、モビリティ コントローラから SPG2 の別のモビリティ エージェントにローミングします。ここで注意すべき点は、クライアントのワイヤレス VLAN 500 がこのモビリティ エージェントにまたがっていないため、これは L3 ローミングであることです。クライアントは MA1 での最初のクライアント接続で受信した IP アドレスを保持します。トラフィックは、新しいモビリティ エージェント（MA3）から、モビリティ コントローラ（MC1）へ、さらにアンカー モビリティ エージェントのスイッチ（MA1）へと送り返されます。この場合、トラフィックは、ネットワークの有線部分にイーサネット フレームとして転送されます。

クライアントのローミング先のスイッチ上の出力は次のように開始します。

```
MA3#show wireless client summary
Number of Local Clients : 2
MAC Address    AP Name                          WLAN State            Protocol
-------------------------------------------------------------------------------
b065.bdb0.a1ad 3602I_G1/0/1_3A2A                1    UP               11n(5)
b065.bdbf.77a3 3602I_G1/0/1_3A2A                1    UP               11n(5)

MA3#show wcdb database all
  Total Number of Wireless Clients = 2
       Foreign Clients           = 2
       MTE Clients               = 0

Mac Address    VlanId IP Address       Src If             Auth     Mob
-------------- ------ --------------- ------------------ -------- -------
b065.bdbf.77a3    701 20.1.1.53        0x00C9D9C000000004 RUN      FOREIGN
```

```
b065.bdb0.a1ad    701 20.1.1.52       0x00C9D9C000000004 RUN      FOREIGN
```

ローミングが SPG にまたがって存在するため、この場合のモビリティ コントローラはモビリティに関わっています。クライアントの可視性を提供するモビリティ コントローラからの出力を次に示します。

```
MC1#show wcdb database all
  Total Number of Wireless Clients = 2
       MTE Clients                 = 2

Mac Address    VlanId IP Address      Src If             Auth     Mob
-------------- ------ --------------- ------------------ -------- -------
b065.bdbf.77a3      0 0.0.0.0         0x00CB4E4000000004 RUN      MTE
b065.bdb0.a1ad      0 0.0.0.0         0x00CB4E4000000004 RUN      MTE

MC1#
MC1#show wireless mobility controller summary
Number of Clients : 2
State is the Sub-Domain state of the client.
* indicates IP of the associated Sub-domain
Associated Time in hours:minutes:seconds
MAC Address     State       Anchor IP      Associated IP    Associated Time
-------------------------------------------------------------------------
b065.bdb0.a1ad  Local       20.1.5.2        20.1.8.2          00:01:24
b065.bdbf.77a3  Local       20.1.5.2        20.1.8.2          00:01:29
```

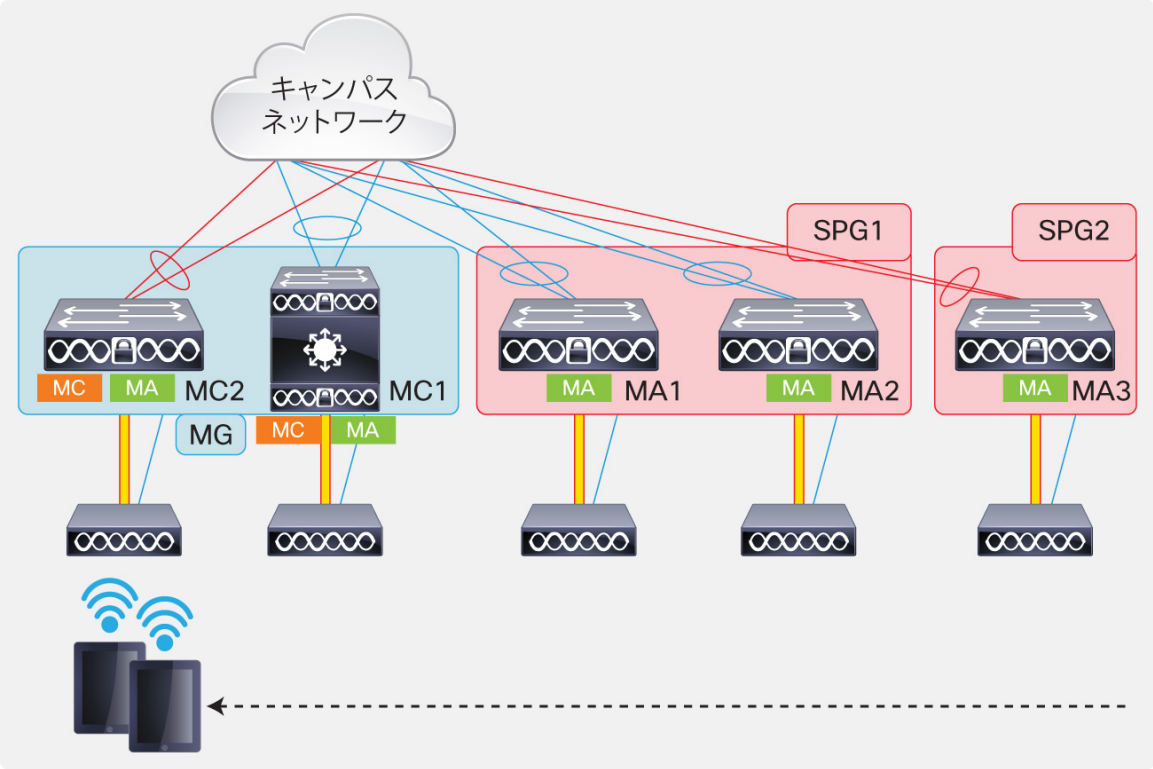
前述の出力には MTE という新しいオプションが表示されます。MTE はモビリティ トンネルのエンドポイントとして定義され、モビリティ エージェントからモビリティ コントローラへのトンネルで入力され、モビリティ エージェントからモビリティ コントローラへのトンネルからアンカーへ出力されるこれらのクライアントのパケットを、モビリティ コントローラで切り替える必要があることを指しています。

アンカー スイッチの出力は次のとおりです。

```
MA1#show wireless client summary
Number of Local Clients : 2
MAC Address    AP Name                       WLAN State              Protocol
-------------------------------------------------------------------------------
b065.bdb0.a1ad 20.1.8.2                      1    UP                 Mobile
b065.bdbf.77a3 20.1.8.2                      1    UP                 Mobile

MA1#
MA1#show wcdb database all
  Total Number of Wireless Clients = 2
       Anchor Clients              = 2

Mac Address    VlanId IP Address      Src If             Auth     Mob
-------------- ------ --------------- ------------------ -------- -------
b065.bdbf.77a3    500 20.1.1.53       0x00D03BC000000002 RUN      ANCHOR
b065.bdb0.a1ad    500 20.1.1.52       0x00D03BC000000002 RUN      ANCHOR
```

図 26 では、複数の MC にまたがるクライアントのローミングを示します。

図 26　統合されたアクセスのモビリティ コントローラ（サブドメイン間）をまたぐクライアントのローミング



上記のシナリオでは、ワイヤレス クライアントはサブドメイン間で SPG2 のモビリティ エージェントから同じモビリティ グループの別のモビリティ コントローラ（MC2）に接続されたアクセス ポイントにローミングします。

このローミングは、モビリティ コントローラとモビリティ コントローラ間の CAPWAP モビリティ トンネルを介してモビリティ コントローラを使用して送り返し、その後モビリティ コントローラとモビリティ エージェント間の CAPWAP モビリティ トンネルからアンカー モビリティ エージェントに送り返す必要があります。出力は、外部スイッチ、すなわちこの場合は新しいモビリティ コントローラのスイッチ（MC2）から開始されます。

```
MC2#show wireless client summary
Number of Local Clients : 2
MAC Address    AP Name                          WLAN State
Protocol
-------------------------------------------------------------------------------
----
b065.bdb0.a1ad 1042_G1/0/1_BD0C                 1    UP
11n(5)
b065.bdbf.77a3 1042_G1/0/1_BD0C                 1    UP
11n(5)

MC2#show wcdb database all
  Total Number of Wireless Clients = 2
       Clients Waiting to Join    = 0
       Foreign Clients            = 2
       MTE Clients                = 0

Mac Address    VlanId IP Address      Src If             Auth     Mob
-------------- ------ --------------- ------------------ -------- -------
```

```
b065.bdbf.77a3    702 20.1.1.53       0x00C33C0000000004 RUN      FOREIGN
b065.bdb0.a1ad    702 20.1.1.52       0x00C33C0000000004 RUN      FOREIGN

MC2#show wireless client mac b065.bdbf.77a3 detail
Client MAC Address : b065.bdbf.77a3
Client Username : blackbird
AP MAC Address : 8875.56da.2010
AP Name: 1042_G1/0/1_BD0C
Wireless LAN Id : 1
Wireless LAN Name: Predator
IPv4 Address : 20.1.1.53
Mobility State : Foreign
Mobility Anchor IP Address : 20.1.5.2
Mobility Move Count : 2
Interface : WIRELESS_VLAN_GRAIL
VLAN : 702
```

次の一連の出力は SPG1 のモビリティ コントローラ（MC1）からのものです。

```
MC1#show wcdb database all
  Total Number of Wireless Clients = 2
       Clients Waiting to Join    = 0
       MTE Clients                = 2

Mac Address     VlanId IP Address      Src If             Auth     Mob
--------------- ------ --------------- ------------------ -------- -------
b065.bdbf.77a3      0 0.0.0.0         0x00DAC94000000001 RUN      MTE
b065.bdb0.a1ad      0 0.0.0.0         0x00DAC94000000001 RUN      MTE
```

統合アクセスにおける非トンネリング ローミング

ここでは、既存の Cisco Unified Wireless Network 内のローミングと同じように動作する L2 ローミングについて説明します。管理者は、非トンネリング（非スティッキ）モードを設定したいアクセス スイッチをまたいでクライアントのワイヤレス VLAN を設定することができます。前述したように、このモードでは、L2 ローミングによって PoA に PoP を移動します。クライアントが最初に結合された古いスイッチに保持されるクライアントの状態はありません。この場合、ローミングされたトラフィックにおいて逆送はありません。この場合はアンカーや外部という概念がなく、クライアントがローミングしたスイッチに ACL と QoS の両方が適用されます。

2 台のモビリティ エージェントのスイッチと 1 台のモビリティ コントローラ スイッチで非トンネリング モードをイネーブルにするには、次のように端末を設定します。

```
wlan Predator
shutdown
no mobility anchor sticky

no shutdown
```

MA1 での最初のクライアント接続の追跡:

```
MA1#show wireless client summary
Number of Local Clients : 2
```

```
MAC Address    AP Name                          WLAN State            Protocol
-------------------------------------------------------------------------------
b065.bdb0.a1ad 3602I_G1/0/1_66BC                1    UP               11n(5)
b065.bdbf.77a3 3602I_G1/0/1_66BC                1    UP               11n(5)

MA1#show wcdb database all
  Total Number of Wireless Clients = 2
       Clients Waiting to Join    = 0
       Local Clients              = 2
       Anchor Clients             = 0
       Foreign Clients            = 0
       MTE Clients                = 0

Mac Address    VlanId IP Address      Src If             Auth     Mob
-------------- ------ --------------- ------------------ -------- -------
b065.bdbf.77a3    500 20.1.1.54       0x00DC7DC000000005 RUN      LOCAL
b065.bdb0.a1ad    500 20.1.1.55       0x00DC7DC000000005 RUN      LOCAL
```

モビリティ コントローラ(MC1)には現時点でクライアントの可視性があるため、次のように表示されます。

```
MC1#show wireless mobility controller client summary
Number of Clients : 2

State is the Sub-Domain state of the client.
* indicates IP of the associated Sub-domain
Associated Time in hours:minutes:seconds

MAC Address     State      Anchor IP       Associated IP    Associated Time
-------------------------------------------------------------------------
b065.bdb0.a1ad  Local      0.0.0.0         20.1.5.2         00:01:04
b065.bdbf.77a3  Local      0.0.0.0         20.1.5.2         00:02:40
```

これが 20.1.5.2 の最初のクライアント接続であるため、アンカー IP が 0.0.0.0 であることに注意してください。

クライアントは MA1 から MA2 に接続されたアクセス ポイントにローミングしていることを考慮して、このタイプの非トンネリング L2 ローミングで発生する変化に注意してください。

```
MA1#show wcdb database all
  Total Number of Wireless Clients = 0

Mac Address    VlanId IP Address      Src If             Auth     Mob
-------------- ------ --------------- ------------------ -------- -------
```

前述のように、最初にクライアントが結合されたスイッチではローミング後のクライアントは 0 です。

```
MA2#show wireless client summary
Number of Local Clients : 2
MAC Address    AP Name                      WLAN State            Protocol
-------------------------------------------------------------------------
b065.bdb0.a1ad AP6073.5c90.4e87             1    UP               11n(5)
```

```
b065.bdbf.77a3 AP6073.5c90.4e87                  1    UP
11n(5)

MA2#show wcdb database all
  Total Number of Wireless Clients = 2
       Clients Waiting to Join    = 0
       Local Clients              = 2
       Anchor Clients             = 0
       Foreign Clients            = 0
       MTE Clients                = 0

Mac Address    VlanId IP Address      Src If              Auth     Mob
-------------- ------ --------------- ------------------- -------- -------
b065.bdbf.77a3    500 20.1.1.54       0x00EC328000000005 RUN      LOCAL
b065.bdb0.a1ad    500 20.1.1.55       0x00EC328000000005 RUN      LOCAL
```

前述のように、クライアントのローミング先の新しいモビリティ エージェントのスイッチでは、2 つのクライアントのモビリティ ステータスを「LOCAL」と表示します。

```
MC1#show wireless mobility controller client summary
Number of Clients : 2

State is the Sub-Domain state of the client.
* indicates IP of the associated Sub-domain
Associated Time in hours:minutes:seconds

MAC Address     State      Anchor IP      Associated IP    Associated Time
-------------------------------------------------------------------------
b065.bdb0.a1ad  Local      0.0.0.0        20.1.7.2         00:00:50
b065.bdbf.77a3  Local      0.0.0.0        20.1.7.2         00:00:50
```

モビリティ コントローラのスイッチは、クライアントがローミングされ、20.1.7.2（MA2 のスイッチ/管理 IP）でそのクライアントのモビリティ ステータスが「ローカル」であるスイッチの変更を反映しています。一方、アンカーのカラムには引き続き 0.0.0.0 と表示されます。

統合アクセスのトンネルのロール

このセクションでは、統合型アクセスの実装においてそれぞれの CAPWAP トンネルが果たす機能について説明します。

MA1 からの出力を次に示します。

```
MA1#show capwap summary

CAPWAP Tunnels General Statistics:
  Number of Capwap Data Tunnels       = 1
  Number of Capwap Mobility Tunnels   = 2
  Number of Capwap Multicast Tunnels  = 0
Name   APName                           Type PhyPortIf Mode      McastIf
------ -------------------------------- ---- --------- --------- -------
Ca1    3602I_G1/0/1_66BC                data Gi1/0/1   unicast   -
```

```
Ca0    -                                   mob  -          unicast    -
Ca2    -                                   mob  -          unicast    -

Name   SrcIP           SrcPort DestIP          DstPort DtlsEn MTU
------ --------------- ------- --------------- ------- ------ -----
Ca1    20.1.5.2        5247    20.1.5.52       38508   No     1449
Ca0    20.1.5.2        16667   20.1.3.2        16667   No     1464
Ca2    20.1.5.2        16667   20.1.7.2        16667   No     1464
```

値は次のとおりです。

Ca1、または CAPWAP トンネル 1 は、Gi1/0/1 に接続された Cisco アクセス ポイント 3602I（20.1.5.52）で形成されるデータ トンネルです。

Ca0 は、モビリティ コントローラのスイッチ（20.1.3.2）によって形成されるモビリティ エージェントとモビリティ コントローラ間の CAPWAP モビリティ トンネルです。

Ca2 は、同じ SPG（SPG1）内の異なるモビリティ エージェントのスイッチ（20.1.7.2）によって形成されるモビリティ エージェントとモビリティ エージェント間の CAPWAP モビリティ トンネルです。

モビリティ コントローラのスイッチからの出力を次に示します。

```
MC1#show capwap summary
CAPWAP Tunnels General Statistics:
  Number of Capwap Data Tunnels        = 2
  Number of Capwap Mobility Tunnels    = 4
  Number of Capwap Multicast Tunnels   = 0
Name   APName                           Type PhyPortIf Mode      McastIf
------ -------------------------------- ---- --------- --------- -------
Ca1    -                                mob  -         unicast   -
Ca2    -                                mob  -         unicast   -
Ca3    -                                mob  -         unicast   -
Ca0    -                                mob  -         unicast   -
Ca5    3502E_G2/0/25_83A9               data Gi2/0/25  unicast   -
Ca4    3602I_G2/0/1_3A04                data Gi2/0/1   unicast   -

Name   SrcIP           SrcPort DestIP          DstPort DtlsEn MTU
------ --------------- ------- --------------- ------- ------ -----
Ca1    20.1.3.2        16667   20.1.5.2        16667   No     1464
Ca2    20.1.3.2        16667   20.1.7.2        16667   No     1464
Ca3    20.1.3.2        16667   20.1.8.2        16667   No     1464
Ca0    20.1.3.2        16667   20.1.9.2        16667   No     1464
Ca5    20.1.3.2        5247    20.1.3.54       63548   No     1657
Ca4    20.1.3.2        5247    20.1.3.53       58274   No     1657
```

値は次のとおりです。

Ca4 および Ca5 は、Gi2/0/1 に接続された Cisco Access Point 3602I（20.1.3.53）および Gi2/0/25 に接続された 3502E（20.1.3.54）で形作られるデータ トンネルです。

Ca0 は、モビリティ コントローラのスイッチ（20.1.9.2）によって形成されるモビリティ コントローラとモビリティ コントローラ間の CAPWAP モビリティ トンネルです。

Ca1 は、モビリティ エージェントのスイッチ（20.1.5.2）によって形成されるモビリティ コントローラとモビリティ エージェント間の CAPWAP モビリティトンネルです。

Ca2 は、モビリティ エージェントのスイッチ（20.1.7.2）によって形成されるモビリティ コントローラとモビリティ エージェント間の CAPWAP モビリティトンネルです。

Ca3 は、モビリティ エージェントのスイッチ（20.1.8.2）によって形成されるモビリティ コントローラとモビリティ エージェント間の CAPWAP モビリティトンネルです。

モビリティ コントローラのスイッチでは、ゲスト アクセスが設定されている場合、ゲストのアンカー コントローラ（WiSM2、リリース 7.3 にアップグレードされた 5508、または 5760 コントローラ）で、同様の CAPWAP モビリティトンネルも構築します。

注: これらの CAPWAP モビリティトンネルは、モビリティに対する設定に基づく秘密のソフトウェアによって自動的に作成されます。

付録 A：FnF フィールドのサポートの詳細

フィールド	L2 In	L2 Out	IPv4 In	IPV4 Out	IPv6 In	IPv6 Out	備考
interface input	Yes	-	Yes	-	Yes	-	
interface output	-	Yes	-	Yes	-	Yes	
flow direction	Yes	Yes	Yes	Yes	Yes	Yes	
Ethertype	Yes	Yes	-	-	-	-	
vlan input	Yes	-	Yes	-	Yes	-	スイッチポートにのみサポートされる
vlan output	-	Yes	-	Yes	-	Yes	スイッチポートにのみサポートされる
dot1q vlan input	Yes	-	Yes	-	Yes	-	スイッチポートにのみサポートされる
dot1q vlan output	-	Yes	-	Yes	-	Yes	スイッチポートにのみサポートされる
dot1q priority	Yes	Yes	Yes	Yes	Yes	Yes	スイッチポートにのみサポートされる
mac source address input	Yes	Yes	Yes	Yes	Yes	Yes	
mac source address output	-	-	-	-	-	-	
mac destination address input	Yes	-	Yes	-	Yes	-	
mac destination address output	-	Yes	-	Yes	-	Yes	
ipv4 version	-	-	Yes	Yes	Yes	Yes	
ipv4 tos	-	-	Yes	Yes	Yes	Yes	
ipv4 protocol	-	-	Yes	Yes	Yes	Yes	送信元/宛先ポート、ICMP コード/タイプ、IGMP タイプ、TCP フラグのいずれかが使用されている場合に使用する必要があります。
ipv4 ttl	-	-	Yes	Yes	Yes	Yes	
ipv4 version	-	-	Yes	Yes	Yes	Yes	IP_VERSION と同じ
ipv4 tos	-	-	Yes	Yes	Yes	Yes	IP_TOS と同じ
ipv4 ttl	-	-	Yes	Yes	Yes	Yes	IP_TTL と同じ
ipv4 protocol	-	-	Yes	Yes	Yes	Yes	IP_PROT と同じ 送信元/宛先ポート、ICMP コード/タイプ、IGMP タイプ、TCP フラグのいずれかが使用されている場合に使用する必要があります。
ipv4 source address	-	-	Yes	Yes	-	-	
ipv4 destination address	-	-	Yes	Yes	-	-	
icmp ipv4 type	-	-	Yes	Yes	-	-	
icmp ipv4 code	-	-	Yes	Yes	-	-	
igmp type	-	-	Yes	Yes	-	-	

フィールド	L2 In	L2 Out	IPv4 In	IPV4 Out	IPv6 In	IPv6 Out	備考
ipv6 version	-	-	Yes	Yes	Yes	Yes	IP_VERSION と同じ
ipv6 protocol	-	-	Yes	Yes	Yes	Yes	IP_PROT と同じ 送信元/宛先ポート、ICMP コード/タイプ、IGMP タイプ、TCP フラグのいずれかが使用されている場合に使用する必要があります。
ipv6 source address	-	-	-	-	Yes	Yes	
ipv6 destination address	-	-	-	-	Yes	Yes	
ipv6 traffic-class	-	-	Yes	Yes	Yes	Yes	IP_TOS と同じ
ipv6 hop-limit	-	-	Yes	Yes	Yes	Yes	IP_TTL と同じ
icmp ipv6 type	-	-	-	-	Yes	Yes	
icmp ipv6 code	-	-	-	-	Yes	Yes	
source-port	-	-	Yes	Yes	Yes	Yes	
destination-port	-	-	Yes	Yes	Yes	Yes	
bytes long	Yes	Yes	Yes	Yes	Yes	Yes	パケット サイズ =（FCS を含むイーサネット フレーム サイズ - 18 バイト） 推奨：このフィールドを回避し、CNT_BYTES_LAYER2_LONG を使用します。
packets long	Yes	Yes	Yes	Yes	Yes	Yes	
timestamp absolute first	Yes	Yes	Yes	Yes	Yes	Yes	
timestamp absolute last	Yes	Yes	Yes	Yes	Yes	Yes	
tcp flags	Yes	Yes	Yes	Yes	Yes	Yes	すべてのフラグを収集する
bytes layer2 long	Yes	Yes	Yes	Yes	Yes	Yes	

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先:シスコ コンタクトセンター
0120-092-255(フリーコール、携帯・PHS含む)
電話受付時間:平日10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

C07-727066-00JA 13.08