管理インターフェイスの設定

- 管理インターフェイスについて，1 ページ
- 管理インターフェイスの設定（GUI），3 ページ
- 管理インターフェイスの設定（CLI），5 ページ

管理インターフェイスについて

管理インターフェイスは、コントローラのインバンド管理や、AAA サーバなどのエンタープライズ サービスへの接続に使用されるデフォルト インターフェイスです。 また、コントローラとアクセス ポイント間の通信にも使用されます。 管理インターフェイスには、唯一常時「ping 可能」な、コントローラのインバンド インターフェイス IP アドレスが設定されています。 コントローラの GUI にアクセスするには、ブラウザのアドレス フィールドに、コントローラの管理インターフェイスの IP アドレスを入力します。

CAPWAP の場合、ポートの数に関係なく、このコントローラには、コントローラ間の全通信を制御する管理インターフェイスが 1 つと、コントローラとアクセス ポイント間の全通信を制御する AP マネージャ インターフェイスが 1 つ必要です。

（注） 有線または無線クライアントによる（無線クライアントの動的インターフェイスまたはVLAN からの）コントローラの管理ネットワークへのアクセスを拒否またはブロックするには、許可されたクライアントだけが適切な CPU ACL によって管理ネットワークへのアクセス権を持つように、またはクライアントの動的インターフェイスと管理ネットワーク間のファイアウォールを使用するように、ネットワーク管理者が設定する必要があります。

注意 ゲスト WLAN を管理インターフェイスにマッピングしないでください。 EoIP トンネルが切断すると、クライアントが IP を取得し、管理サブネット内に配置されてしまう可能性があります。

注意　ネットワークのコントローラのサービス ポートの同じ VLAN またはサブネットに有線クライアントを設定しないでください。 サービス ポートと同じサブネットまたは VLAN に有線クライアントを設定すると、コントローラの管理インターフェイスにアクセスできなくなります。

管理インターフェイスの認証タイプ

コントローラへの管理アクセスのタイプが SSH、Telnet、または HTTP の場合は、TACACS+、RADIUS、またはローカルのいずれかの認証タイプを使用し、これらを混在させないことをお勧めします。 次の要件を確認してください。

- 認証タイプ（TACACS+、RADIUS、またはローカル）は、すべての管理アクセスとすべての AAA 認証パラメータおよび認可パラメータで同じにする必要があります。
- HTTP 認証ではメソッド リストを明示的に指定する必要があります。

例

Telnet を設定するには、次の手順を実行します。

1. 次のコマンドを入力して、TACACS+ サーバを設定します。
   a. **tacacs server***server-name*
   b. **address ipv4***ip-address*
   c. **key***key-name*
2. 次のコマンドを入力して、サーバ グループ名を設定します。
   a. **aaa group server tacacs+***group-name*
   b. **server name***name*
3. 次のコマンドを入力して、認証と認可を設定します。
   a. **aaa authentication login***method-list***group***server-group*
   b. **aaa authorization exec***method-list***group***server-group*

（注）　これらとその他のすべての認証および認可パラメータは、同じデータベース（RADIUS、TACACS+、またはローカル）を使用する必要があります。 たとえば、コマンド認可を有効にする必要がある場合は、それが同じデータベースを指している必要もあります。

4. 上記のメソッド リストを使用するように HTTP を設定します。
   1. **ip http authentication aaa login-auth***method-list*
      メソッド リストが「default」の場合でもメソッド リストを明示的に指定する必要があります。
   2. **ip http authentication aaa exec-auth***method-list*

（注）
- 「line vty」設定パラメータに対してメソッド リストを設定しないでください。 上記手順と line vty の設定が異なる場合は、line vty の設定が優先されます。
- データベースは SSH/Telnet や webui などのすべての管理設定タイプで同じにする必要があります。
- HTTP 認証用のメソッド リストを明示的に定義する必要があります。

回避策

回避策として、次のコマンドを入力してください。

1 **aaa authentication login default group***server-group***local**
2 **aaa authorization exec default group***server-group***local**

管理インターフェイスの設定（GUI）

ステップ 1 [Controller] > [Interfaces] の順に選択して、[Interfaces] ページを開きます。

ステップ 2 [management] リンクをクリックします。
[Interfaces > Edit] ページが表示されます。

ステップ 3 管理インターフェイスのパラメータを設定します。

（注） 管理インターフェイスでは、工場出荷時にコントローラに設定されたディストリビューション システム MAC アドレスが使用されます。

- 該当する場合、検疫および検疫 VLAN ID

  （注） [Quarantine] チェックボックスは、この VLAN を正常に動作していない VLAN として設定する場合、またはネットワーク アクセス コントロール（NAC）アウトオブバンドを設定する場合にオンにします。 このように設定すると、この VLAN に割り当てられているあらゆるクライアントのデータ トラフィックがコントローラを通るようになります。

- NAT アドレス（Cisco 2500 シリーズ コントローラと Cisco 5500 シリーズ コントローラのみが動的 AP 管理用に設定されます）

  （注） 1 対 1 のネットワーク アドレス変換（NAT）を使用するルータまたは他のゲートウェイ デバイスの背後に Cisco 2500 シリーズ コントローラまたは Cisco 5500 シリーズ コントローラを展開できるようにする場合は、[Enable NAT Address] チェックボックスをオンにして、外部 NAT IP アドレスを入力します。 NAT を使用すると、ルータなどのデバイスがインターネット（パブリック）とローカル ネットワーク（プライベート）間のエージェントとして動作します。 この場合、コントローラのイントラネット IP アドレスは対応する外部アドレスにマッピングされます。 コントローラが Discovery Response で適切な IP アドレスを送信できるように、外部 NAT IP アドレスを使用してコントローラの動的 AP マネージャ インターフェイスを設定する必要があります。

（注） 管理インターフェイスで Cisco 2500 シリーズ コントローラまたは Cisco 5500 シリーズ コントローラに外部 NAT IP アドレスが設定されている場合、ローカル モードの AP はコントローラにアソシエートできません。 この問題を回避するには、グローバルに有効な IP アドレスが管理インターフェイスに設定されるようにするか、外部 NAT IP アドレスをローカル AP に対して内部的に有効なものにします。

（注） NAT パラメータの使用は、1 対 1 のマッピングの NAT を使用する場合にだけサポートされています。これにより、各プライベートクライアントはグローバルアドレスに直接かつ固定的にマッピングされます。 NAT パラメータでは、クライアントのグループを単一の IP アドレスで表すために送信元ポート マッピングを使用する 1 対多 NAT はサポートしていません。

- VLAN 識別子

（注） タグなし VLAN については 0、タグ付き VLAN についてはゼロ以外の値を入力します。 管理インターフェイスでは、タグ付きの VLAN を使用することをお勧めします。

- IPv4 を使用した管理インターフェイスの設定：固定 IP アドレス、IP ネットマスク、およびデフォルト ゲートウェイ。
  - IPv6 を使用した管理インターフェイスの設定： 固定 IPv6 アドレス、プレフィックス長（IPv6 のインターフェイス サブネット マスク）および IPv6 ゲートウェイ ルータのリンクローカル アドレス。

（注） 一度プライマリ IPv6 アドレス、プレフィックス長、プライマリ IPv6 ゲートウェイを管理インターフェイスで設定すると、設定をデフォルト値に戻すことはできません（::/128）。

（注） ユーザが IPv4 専用管理インターフェイスに戻す場合に備えて、IPv6 を設定する前に、設定のバックアップを実行する必要があります。

（注） 単一の Catalyst 6000 スイッチで 1300 を超える IPv6 AP が使用されている場合は、複数の VLAN 上で AP を割り当てます。

- 動的 AP 管理（Cisco 2500 シリーズ コントローラまたは Cisco 5500 シリーズ コントローラに対してのみ）

（注） Cisco 5500 シリーズ コントローラの場合、管理インターフェイスはデフォルトで AP マネージャ インターフェイスのように動作します。 必要に応じて、管理インターフェイスを AP マネージャ インターフェイスとして無効にし、別の動的インターフェイスを AP マネージャとして作成できます。

- 物理ポートの割り当て（Cisco 2500 シリーズ コントローラまたは Cisco 5500 シリーズ コントローラを除くすべてのコントローラ）
- プライマリおよびセカンダリの DHCP サーバ
- 必要に応じて、アクセス コントロール リスト（ACL）の設定

ステップ 4 [Save Configuration] をクリックします。

ステップ 5 管理インターフェイスまたは仮想インターフェイスに何らかの変更を行ったときに変更を有効にするには、コントローラをリブートします。

管理インターフェイスの設定（CLI）

ステップ 1 **show interface detailed management** コマンドを入力し、現在の管理インターフェイスの設定を表示します。

（注） 管理インターフェイスでは、工場出荷時にコントローラに設定されたディストリビューション システム MAC アドレスが使用されます。

ステップ 2 **config wlan disable***wlan-number* コマンドを入力して、ディストリビューション システム通信用に管理インターフェイスを使用する各 WLAN を無効にします。

ステップ 3 次のコマンドを入力し、管理インターフェイスを定義します。

a) **IPv4 アドレスの使用**

- **config interface address management***ip-addr ip-netmaskgateway*
- **config interface quarantine vlan management***vlan_id*

  （注） 隔離 VLAN を管理インターフェイスに設定するには、**config interface quarantine vlan management***vlan_id* コマンドを使用します。

- **config interface vlan management** {*vlan-id* | *0*}

  （注） タグなしVLANについては0、タグ付きVLANについてはゼロ以外の値を入力します。管理インターフェイスでは、タグ付きの VLAN を使用することをお勧めします。

- **config interface ap-manager management**{**enable** | **disable**}（Cisco 5500 シリーズ コントローラの場合のみ）

  （注） 管理インターフェイスに対して動的AP管理を有効または無効にするには、**config interface ap-manager management**{**enable** | **disable**} コマンドを使用します。 Cisco 5500 シリーズ コントローラの場合、管理インターフェイスはデフォルトで AP マネージャ インターフェイスのように動作します。 必要に応じて、管理インターフェイスを AP マネージャ インターフェイスとして無効にし、別の動的インターフェイスを AP マネージャとして作成できます。

- **config interface port management***physical-ds-port-number*（5500 シリーズを除くすべてのコントローラ）
- **config interface dhcp management***ip-address-of-primary-dhcp-server* [*ip-address-of-secondary-dhcp-server*]
- **config interface acl management***access-control-list-name*

b) **IPv6 アドレスの使用**

- **config ipv6 interface address management***primaryip-addressprefix-lengthIPv6_Gateway_Address*

  （注） 一度プライマリ IPv6 アドレス、プレフィックス長、プライマリ IPv6 ゲートウェイを管理インターフェイスで設定すると、設定をデフォルト値に戻すことはできません（::/128）。

  （注） ユーザが IPv4 専用管理インターフェイスに戻す場合に備えて、IPv6 を設定する前に、設定のバックアップを実行する必要があります。

- **config interface quarantine vlan management***vlan_id*

（注） 隔離 VLAN を管理インターフェイスに設定するには、**config interface quarantine vlan management***vlan_id* コマンドを使用します。

- **config interface vlan management** {*vlan-id* | *0*}

（注） タグなし VLAN については 0、タグ付き VLAN についてはゼロ以外の値を入力します。管理インターフェイスでは、タグ付きの VLAN を使用することをお勧めします。

- **config interface ap-manager management** {**enable** | **disable**}（Cisco 5500 シリーズ コントローラの場合のみ）

（注） 管理インターフェイスに対して動的 AP 管理を有効または無効にするには、**config interface ap-manager management** {**enable** | **disable**} コマンドを使用します。 Cisco 5500 シリーズ コントローラの場合、管理インターフェイスはデフォルトで AP マネージャ インターフェイスのように動作します。 必要に応じて、管理インターフェイスを AP マネージャ インターフェイスとして無効にし、別の動的インターフェイスを AP マネージャとして作成できます。

- **config interface port management***physical-ds-port-number*（5500 シリーズを除くすべてのコントローラ）
- **config interface dhcp management***ip-address-of-primary-dhcp-server* [*ip-address-of-secondary-dhcp-server*]
- **config ipv6 interface acl management***access-control-list-name*

ステップ 4 1 対 1 のネットワーク アドレス変換（NAT）を使用するルータまたは他のゲートウェイ デバイスの背後に Cisco 5500 シリーズ コントローラを展開できるようにする場合は、次のコマンドを入力します。

- **config interface nat-address management** {**enable** | **disable**}
- **config interface nat-address management set***public_IP_address*

NAT を使用すると、ルータなどのデバイスがインターネット（パブリック）とローカル ネットワーク（プライベート）間のエージェントとして動作します。 この場合、コントローラのイントラネット IP アドレスは対応する外部アドレスにマッピングされます。 コントローラが Discovery Response で適切な IP アドレスを送信できるように、外部 NAT IP アドレスを使用してコントローラの動的 AP マネージャ インターフェイスを設定する必要があります。

（注） これらのコマンドは、1 対 1 マッピング NAT での使用に対してだけサポートされています。各プライベート クライアントはグローバル アドレスに対して直接的かつ固定的にマッピングされます。 これらのコマンドでは、クライアントのグループを単一の IP アドレスで表すために送信元ポート マッピングを使用する 1 対多 NAT はサポートされません。

ステップ 5 **save config** コマンドを入力します。

ステップ 6 **show interface detailed management** コマンドを入力して、変更内容が保存されていることを確認します。

ステップ 7 管理インターフェイスに何らかの変更を行った場合に、変更を有効にするためにコントローラをリブートするには、**reset system** コマンドを入力します。