# NAC アウトオブバンド統合の設定



## NAC アウトオブバンドの前提条件

- NAC アウトオブバンド統合には、CCA のソフトウェア リリース 4.5 以降が必要です。
- NAC アプライアンスでは静的な VLAN マッピングがサポートされているため、コントローラ上で設定されているインターフェイスごとに一意の隔離 VLAN を設定する必要があります。 たとえば、コントローラ 1 で 110 という隔離 VLAN を設定し、コントローラ 2 で 120 という隔離 VLAN を設定します。 ただし、2 つの WLAN またはゲスト LAN が、コントローラのダイナミック インターフェイスとして同一の VLAN を使用している場合、ネットワーク内に導入された NAC アプライアンスが 1 つのときは、同じ隔離 VLAN を使用する必要があります。 NAC アプライアンスは、一意の隔離 - アクセス VLAN マッピングをサポートします。
- セッションの失効に基づくポスチャ再評価の場合、NAC アプライアンスと WLAN の両方にセッション タイムアウトを設定し、WLAN でのセッションの失効が NAC アプライアンスでの失効より大きいことを確認します。
- オープン WLAN でセッション タイムアウトが設定されると、Quarantine 状態にあるクライアントのタイムアウトは NAC アプライアンスのタイマーによって判定されます。 Web 認証を使用する WLAN においてセッションがタイムアウトすると、クライアントはコントローラから認証解除されるため、ポスチャ検証を再度実行する必要があります。
- レイヤ 2 およびレイヤ 3 認証はすべて、隔離 VLAN で実行されます。 外部 Web 認証を使用するには、外部 Web サーバからの HTTP トラフィックおよび外部 Web サーバへの HTTP ト

ラフィックを許可するとともに、隔離 VLAN でのリダイレクト URL を許可するように NAC アプライアンスを設定する必要があります。

（注） 設定の手順については、『Cisco NAC appliance configuration guides』を参照してください：http://www.cisco.com/en/US/products/ps6128/products_installation_and_configuration_guides_list.html。

- アクセス ポイント グループ VLAN 上で NAC を有効にする場合は、WLAN で NAC をまず有効にする必要があります。 アクセス ポイント グループ VLAN では、NAC を有効または無効にすることができます。 WLAN で NAC を無効にすることに決めた場合は、アクセス ポイント グループ VLAN でも NAC を必ず無効にします。
- NAC アプライアンスは最大 3,500 のユーザをサポートし、コントローラは最大 5,000 のユーザをサポートします。 複数の NAC アプライアンスの導入を必要とする場合があります。
- アクセス ポイント グループ VLAN 上で NAC を有効にする場合は、WLAN で NAC をまず有効にする必要があります。 アクセス ポイント グループ VLAN では、NAC を有効または無効にすることができます。 WLAN で NAC を無効にすることに決めた場合は、アクセス ポイント グループ VLAN でも NAC を必ず無効にします。
- NAC アプライアンスは最大 3,500 のユーザをサポートし、コントローラは最大 5,000 のユーザをサポートします。 複数の NAC アプライアンスの導入を必要とする場合があります。
- コントローラの 5.1 以前のソフトウェア リリースでは、コントローラはインバンド モードでのみ NAC アプライアンスと統合します。この場合、NAC アプライアンスはデータ パス内になければなりません。 インバンド モードでは、各認証場所で（たとえば、各ブランチで、またはコントローラごとに）、NAC アプライアンスが必要であり、すべてのトラフィックが NAC 適用ポイントを通過する必要があります。 コントローラのソフトウェア リリース 5.1 以降では、コントローラはアウトオブバンド モードで NAC アプライアンスと統合できます。この場合、NAC アプライアンスは、クライアントが解析およびクリーニングされるまでデータ パスに保持されます。 アウトオブバンド モードでは NAC アプライアンスのトラフィック負荷が削減されるので、NAC 処理の集中化が可能になります。
- NAC アウトオブバンド統合がサポートされるのは、WLAN が FlexConnect の中央スイッチングを行うように設定されている場合だけです。 FlexConnect のローカル スイッチングを行うように設定されている WLAN での使用はサポートされていません。

# NAC アウトオブバンドの制限

- NAC アウトオブバンド統合は、WLAN AAA Override 機能では使用できません。
- コントローラの 5.1 以前のソフトウェア リリースでは、コントローラはインバンド モードでのみ NAC アプライアンスと統合します。この場合、NAC アプライアンスはデータ パス内になければなりません。 インバンド モードでは、各認証場所で（たとえば、各ブランチで、またはコントローラごとに）、NAC アプライアンスが必要であり、すべてのトラフィックが

NAC 適用ポイントを通過する必要があります。 コントローラのソフトウェア リリース 5.1 以降では、コントローラはアウトオブバンドモードでNACアプライアンスと統合できます。この場合、NACアプライアンスは、クライアントが解析およびクリーニングされるまでデータ パスに保持されます。 アウトオブバンド モードではNAC アプライアンスのトラフィック負荷が削減されるので、NAC 処理の集中化が可能になります。

- NAC アウトオブバンド統合がサポートされるのは、WLAN が FlexConnect の中央スイッチングを行うように設定されている場合だけです。 FlexConnect のローカル スイッチングを行うように設定されている WLAN での使用はサポートされていません。

# NAC アウトオブバンド統合について

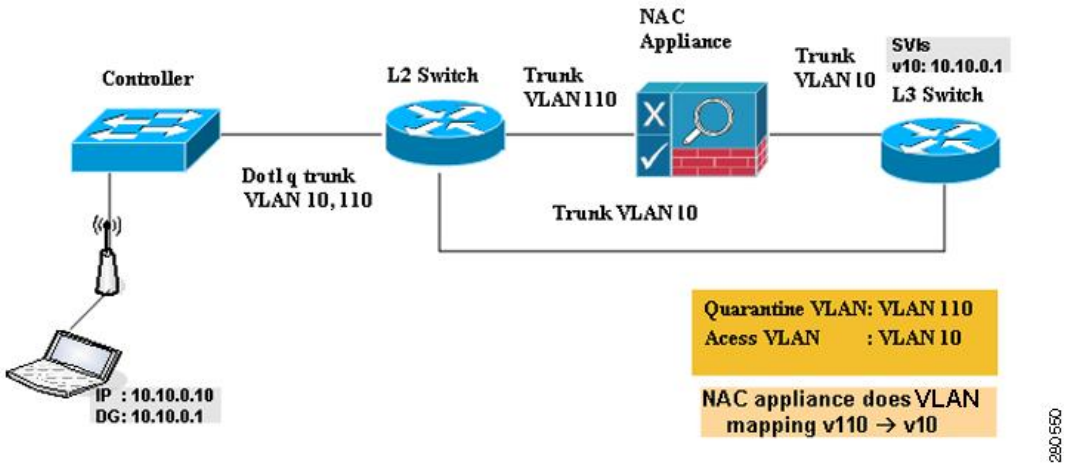
Cisco Clean Access（CCA）とも呼ばれる Cisco NAC アプライアンスはネットワーク アドミッション制御（NAC）製品です。この製品を使用して、ネットワーク管理者は、ユーザをネットワークに許可する前に、有線、無線、およびリモート ユーザおよびマシンを認証、許可、評価、修正できます。 NAC アプライアンスは、マシンがセキュリティ ポリシーに準拠しているかどうかを判別し、脆弱性を修復してから、ネットワークへのアクセスを許可します。

NAC アプライアンスは、インバンド モードとアウトオブバンド モードの 2 つのモードで利用できます。 お客様は、必要ならば両方のモードを導入して、それぞれが特定のタイプのアクセスを担当するようにすることもできます。たとえば、インバンドで無線接続ユーザをサポートし、アウトオブバンドで有線接続ユーザを担当するといった構成も可能です。

コントローラ上に NAC アウトオブバンド機能を実装するには、WLAN またはゲスト LAN 上で NAC のサポートを有効にしてから、この WLAN またはゲスト LAN を、隔離 VLAN（信頼できない VLAN）およびアクセス VLAN（信頼できる VLAN）で設定されたインターフェイスにマッピングする必要があります。 クライアントは、アソシエートしてレイヤ 2 認証を完了すると、アクセス VLAN サブネットから IP アドレスを取得しますが、クライアントの状態は Quarantine となります。 NAC アウトオブバンド機能の導入中は、コントローラが接続されたレイヤ 2 スイッチと NAC アプライアンスとの間でのみ隔離 VLAN が許可されること、および NAC アプライアンスが一意の隔離 - アクセス VLAN マッピングで設定されていることを確認します。 クライアントのトラフィックは、NAC アプライアンスにトランクされた隔離 VLAN に渡されます。 ポスチャ検証が終了すると、クライアントは修復のための処置を実行するように促されます。 クリーニングが完了すると、NAC アプライアンスはコントローラを更新してクライアントの状態を Quarantine から Access へ変更します。

コントローラとスイッチとの間のリンクをトランクとして設定することにより、隔離VLAN（110）とアクセス VLAN（10）を有効にしています。 レイヤ 2 スイッチ上では、隔離トラフィックがNAC アプライアンスにトランクされ、アクセス VLAN トラフィックがレイヤ 3 スイッチに直接送信されます。 NAC アプライアンス上の隔離 VLAN に到達するトラフィックは、静的なマッピング設定に基づいてアクセス VLAN にマップされます。

図 *1*：*NAC* アウトオブバンド統合の例




# NAC アウトオブバンド統合の設定（GUI）

**ステップ 1** 次の手順で、動的インターフェイスに対して隔離 VLAN を設定します。

a) [Controller] > [Interfaces] の順に選択して、[Interfaces] ページを開きます。

b) [New] をクリックして、新たに動的インターフェイスを作成します。

c) [Interface Name] テキスト ボックスに、"quarantine" など、このインターフェイスの名前を入力します。

d) [VLAN ID] テキスト ボックスでは、アクセス VLAN ID にゼロ以外の値（「10」など）を入力してください。

e) [Apply] をクリックして、変更を確定します。 [Interfaces > Edit] ページが表示されます。

f) [Quarantine] チェックボックスをオンにして、隔離 VLAN ID に「110」などのゼロ以外の値を入力します。

（注） ネットワーク全体で一意の隔離 VLAN を設定することを推奨します。同じモビリティ グループ内に複数のコントローラが設定されており、すべてのコントローラのアクセス インターフェイスが同じサブネット内にある場合、ネットワークに NAC アプリケーションが 1 つだけならば、同じ隔離 VLAN を保持する必要があります。 同じモビリティ グループ内に複数のコントローラが設定されており、すべてのコントローラのアクセス インターフェイスが別々のサブネット内にある場合、ネットワークに NAC アプリケーションが 1 つだけならば、別々の隔離 VLAN を保持する必要があります。

g) このインターフェイスの残りのテキスト ボックス（IP アドレス、ネットマスク、デフォルト ゲートウェイなど）を設定します。

h) [Apply] をクリックして変更内容を保存します。

**ステップ 2** 次の手順で、WLAN またはゲスト LAN に対して NAC アウトオブバンドのサポートを設定します。

a) [WLANs] を選択して、[WLANs] ページを開きます。

b) 必要な WLAN またはゲスト LAN の ID 番号をクリックします。 [WLANs > Edit] ページが表示されます。
c) [Advanced] タブを選択して、[WLANs > Edit]（[Advanced]）ページを開きます。
d) この WLAN またはゲスト LAN に対して NAC アウトオブバンドのサポートを設定するには、[NAC State] チェックボックスをオンにします。 NAC アウトオブバンドのサポートを無効にするには、チェックボックスをオフ（デフォルト値）のままとします。
e) [Apply] をクリックして、変更を確定します。

**ステップ 3** 次の手順で、特定のアクセス ポイント グループに対して NAC アウトオブバンドのサポートを設定します。

a) [WLANs] > [Advanced] > [AP Groups] の順に選択して、[AP Groups] ページを開きます。
b) 目的のアクセス ポイント グループの名前をクリックします。
c) [WLANs] タブを選択して、[AP Groups > Edit]（[WLANs]）ページを開きます。
d) [Add New] をクリックして、このアクセス ポイント グループに WLAN を割り当てます。 [Add New] のセクションがページ上部に表示されます。
e) [WLAN SSID] ドロップダウン リストから、この WLAN の SSID を選択します。
f) [Interface Name] ドロップダウン リストから、アクセス ポイント グループをマップするインターフェイスを選択します。 NAC アウトオブバンドのサポートを有効にする場合は、隔離 VLAN を選択します。
g) このアクセス ポイント グループに対して NAC アウトオブバンドのサポートを有効にするには、[NAC State] チェックボックスをオンにします。 NAC アウトオブバンドのサポートを無効にするには、チェックボックスをオフ（デフォルト値）のままとします。
h) [Add] をクリックして、この WLAN をアクセス ポイント グループに追加します。 この WLAN が、このアクセス ポイント グループに割り当てられている WLAN のリストに表示されます。

（注） この WLAN をアクセス ポイント グループから削除する場合は、カーソルをこの WLAN の青のドロップダウン矢印の上に置いて、[Remove] を選択します。

**ステップ 4** [Save Configuration] をクリックして、変更を保存します。

**ステップ 5** 次の手順で、クライアントの現在の状態（Quarantine または Access）を表示します。

a) [Monitor] > [Clients] の順に選択して、[Clients] ページを開きます。
b) 目的のクライアントの MAC アドレスをクリックして、[Clients > Detail] ページを開きます。 NAC 状態が、[Security Information] のセクションに表示されます。

（注） クライアントがプロービングを行っている場合、クライアントが WLAN にまだアソシエートされていない場合、またはクライアントがレイヤ 2 認証を完了できない場合、クライアントの状態は「Invalid」として表示されます。

# NAC アウトオブバンド統合の設定（CLI）

**ステップ 1** 動的インターフェイスに対して隔離 VLAN を設定するには、次のコマンドを入力します。

**config interface quarantine vlan** *interface_name vlan_id*

（注） コントローラ上のインターフェイスごとに一意の隔離 VLAN を設定する必要があります。

インターフェイスで隔離 VLAN を無効にするには、VLAN ID に *0* を入力します。

**ステップ 2** WLAN またはゲスト LAN に対して NAC アウトオブバンド サポートを有効または無効にするには、次のコマンドを入力します。
**config** {**wlan** | **guest-lan**} **nac** {**enable** | **disable**} {*wlan_id* | *guest_lan_id*}

**ステップ 3** 特定のアクセス ポイント グループに対して NAC アウトオブバンド サポートを有効または無効にするには、次のコマンドを入力します。
**config wlan apgroup nac** {**enable** | **disable**} *group_name wlan_id*

**ステップ 4** 次のコマンドを入力して、変更を保存します。
**save config**

**ステップ 5** NAC 状態など、WLAN またはゲスト LAN の構成を表示するには、次のコマンドを入力します。
**show** {**wlan** *wlan_ id* | **guest-lan** *guest_lan_id*}

以下に類似した情報が表示されます。

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

  NAC-State.................................. Enabled
  Quarantine VLAN............................ 110
...
```

**ステップ 6** クライアントの現在の状態（Quarantine または Access）を表示するには、次のコマンドを入力します。
**show client detailed** *client_mac*

以下に類似した情報が表示されます。

```
Client’s NAC state.............................. QUARANTINE
```

（注） クライアントがプロービングを行っている場合、クライアントが WLAN にまだアソシエートされていない場合、またはクライアントがレイヤ 2 認証を完了できない場合、クライアントの状態は「Invalid」として表示されます。