CHAPTER 3

レイヤ 3 アウトオブバンド（L3 OOB）の設定

この章では、レイヤ 3 アウトオブバンド配置モデルに必要な設定について概説します。

アウトオブバンド配置モデルの Cisco NAC アプライアンスの設定に関する一般的な説明は、『*Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.9.*』の「Switch Management and Configuring Out-of-Band (OOB) Deployment」および「Enable the Login Page for L3 OOB」を参照してください。

概要

インバンド（有線）配置モデルのマルチホップ L3 サポートでは、CAS をインバンド（IB）構成で中央（コアまたは分散レイヤ）に配置して、L3 スイッチの外側のユーザをサポートするとともに（ルーテッド アクセスなど）、VPN コンセントレータやリモート WAN ルータの外側のリモート ユーザをサポートできます。L3 IB を使用すると、CAS から L3 で複数ホップ離れているユーザがサポートされ、このようなユーザのトラフィックは常に Cisco NAC アプライアンスを通過します。

アウトオブバンド（有線）配置モデルのマルチホップ L3 サポートでは、CAS をアウトオブバンド（OOB）構成で中央（コアまたは分散レイヤ）に配置して、L3 スイッチの外側のユーザ（ルーテッド アクセスなど）のほか、場合に応じて WAN ルータの外側のリモート ユーザもサポートできます。L3 OOB を使用すると、CAS から L3 で複数ホップ離れているユーザがサポートされ、このようなユーザのトラフィックは、認証またはポスチャ評価時にだけ Cisco NAC アプライアンスを通過します。

リモート WAN ユーザ用にリモート CAS または L3 IB CAS を配置したり、場合によって L3 OOB を使用できます。

クライアント MAC アドレスの検出：Agent、ActiveX または Java アプレット

L3 OOB 配置では、クライアント MAC アドレスが Agent の MAC 検出メカニズムによって自動的に検出されます。

Web ログインを実行中のユーザは、ユーザ ログインの前に ActiveX コントロール（IE ブラウザの場合）または Java アプレット（IE ブラウザではない場合）をクライアント マシンにダウンロードして実行します。これによってユーザ マシンの MAC アドレスが判断されます。この情報が CAS と CAM に報告され、IP アドレスと MAC アドレスのマッピングが提供されます。

L3 OOB ユーザの Agent ログイン

Cisco NAC アプライアンスは、アウトオブバンド（有線）配置のマルチホップ L3 サポートを可能にし、管理者は CAS をアウトオブバンド（OOB）構成で中央（コアまたは分散レイヤ）に配置して、L3 スイッチの外側のユーザ（ルーテッド アクセスなど）のほか、場合に応じて WAN ルータの外側のリモート ユーザもサポートできます。L3 OOB を使用すると、CAS から L3 で複数ホップ離れているユーザがサポートされ、このようなユーザのトラフィックは、認証またはポスチャ評価時に Cisco NAC アプライアンスを通過します。

L3 OOB 配置では、クライアント MAC アドレスが Agent の MAC 検出メカニズムによって自動的に検出されます。

Web ログインを実行中のユーザは、ユーザ ログインの前に ActiveX コントロール（IE ブラウザの場合）または Java アプレット（IE ブラウザではない場合）をクライアント マシンにダウンロードして実行します。これによってユーザ マシンの MAC アドレスが判断されます。この情報が CAS と CAM に報告され、IP アドレスと MAC アドレスのマッピングが提供されます。

ActiveX/Java アプレットおよびブラウザの互換性

- ActiveX と Java アプレット、およびブラウザの互換性の詳細については、『*Support Information for Cisco NAC Appliance Agents, Release 4.5 and Later*』を参照してください。
- Java アプレットは、Windows XP、Mac OS X、Linux オペレーティング システムの Safari 1.2+、Mozilla（Camino、Opera）、Internet Explorer を含む主要なブラウザでサポートされています。
- Firefox での Java に関する問題のため、Mac OS X 上の Firefox では Java アプレットがサポートされていません。詳細は、Firefox のリリース ノート（http://www.mozilla.com/firefox/releases/1.5.0.3.html）を参照してください。

（注）　**MAC OS X クライアントの場合：**Apple の Mac OS X の場合、プロキシを迂回するようにブラウザを設定するには、クライアント マシンが Java アプレットを正常にロードしてログインできるように、CAS の完全な IP アドレス（10.201.217.93 など）が必要です。

（注）　**Linux OOB クライアントの場合：**

Linux マシンは Windows や Mac OS X のクライアントとは動作が異なるので（NIC 停止時の IP アドレスの解放や、NIC 起動時の IP アドレスの更新を行わないなど）、OOB Linux クライアントの場合は、次の手順を使用してください。

1. 認証 VLAN 上の DHCP サーバのリース時間を短く設定します（例：60 秒）。
2. [Port Profile] で、[Remove out-of-band online user when SNMP linkdown trap is received] オプションをディセーブルにします（チェックを外す）。

   これにより、Linux クライアントは、認証/証明後短時間で IP アドレスを更新します。

（注）　Linux は IP アドレス更新時に NIC のシャットダウン/再起動を実行するので、[Port Profile] でこのオプションがイネーブルになっていると（チェックを付けておくと）、更新によってポートは認証 VLAN に戻されます。

3. あるいは、[Port Profile] の設定を、[Change to [Access VLAN] if the device is certified but not in the out-of-band user list] にしてもかまいません。このようにすると、認証/証明済みの Linux クライアントが DHCP リースの更新後にポートに再接続した場合、そのポートはアクセス VLAN のままになります。

この新機能によって、次の Web 管理コンソール ページが変更されました。

- 次のユーザ ログイン設定ページの [Use ActiveX or Java Applet to detect client MAC address when Clean Access Server cannot detect the MAC address] に、新しいチェックボックスとドロップダウン メニューが追加されています。
  - CAM Web コンソール : [Administration] > [User Pages] > [Login Page] > [List [Edit]] | [General]
  - SAS 管理ページ : [Device Management] > [CCA Servers] > [Manage [CAS_IP]] > [Authentication] > [Login Page] > [List [Edit]] > [General]
- [Device Management] > [Clean Access] > [Updates]（L3 Java アプレット Web クライアントおよび L3 ActiveX Web クライアントへの更新に関するバージョン情報）

さらに、L3 OOB ユーザのログイン ページに、Active X コントロールまたは Java アプレットのロードおよびクライアント IP アドレスの更新に関連したステータス情報が反映されます。

レイヤ 3 アウトオブバンド（OOB）配置を利用する場合

- OOB を使用できるのは有線の場合だけです。
- L3 OOB はルーテッド アクセスに最適です。
- L3 OOB は、リモート WAN サイトにも使用できますが、次のような他の導入への変更を検討してください。
  - WAN サイトへのリモート CAS
  - 中央サイトの L3 IB CAS による WAN サイトのサポート

レイヤ 2 とレイヤ 3 のアウトオブバンド実装

L2 OOB

- ユーザは CAS に L2 で隣接しています。
- ユーザ デバイスはスイッチに接続し、スイッチは CAM に SNMP トラップを送信します。
- CAM はスイッチからデバイス MAC とポート情報を取得します。
- CAS はパケットを受信し、ソース IP/MAC を CAM に送信します。
- これで CAM は IP/MAC/ ポートのマッピングを完了します。
- デバイスの準拠性が証明されると、CAM は VLAN を変更するポートを認識します。

L3 OOB

- ユーザは、CAS から 1 つまたは複数ホップ以上離れています。
- CAM はデバイス MAC とポート情報をスイッチから取得します。
- CAS はユーザ IP が含まれたパケットを受信します。
- CAS は Agent から MAC 情報を取得するか、または、ActiveX または Java アプレットによるデバイス MAC アドレスの判断と CAS への報告がイネーブルになっている場合には Web ログインページから MAC 情報を取得します。
- CAS はデバイスの IP と MAC を CAM に伝えます。
- CAM は IP、MAC、ポートのマッピングを完了します。

レイヤ 3 アウトオブバンド L3 OOB の詳細情報

Agent の使用

Agent は CAS にデバイスの MAC アドレスを伝えます。

Agent を使用しない場合（Web ログインを使用）

- Web ログイン ページに Active X コントロールまたは Java アプレットがダウンロードされ、これによって取得されたデバイス MAC アドレスが CAS に報告されます。
- CAS はデバイスの IP と MAC を CAM に伝えます。
- CAM は IP、MAC、ポートのマッピングを完了します。

レイヤ 3 OOB：設定

Agent を使用する場合

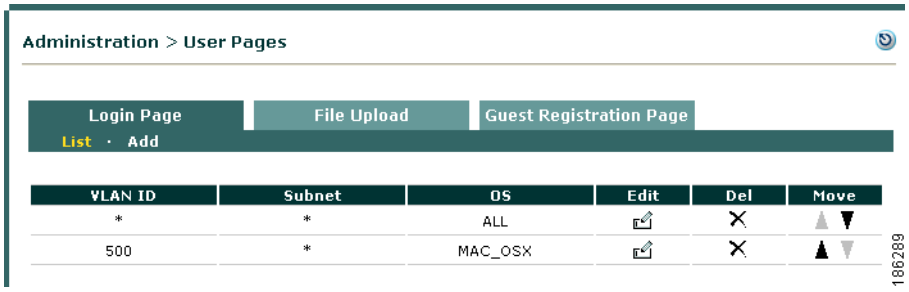
- Agent が CAS に MAC アドレスを通知します。
- 追加設定は必要ありません。

Agent を使用しない場合（Web ログインを使用）

ログイン ページの設定を行います。

- CAM：[Administration] > [User Pages] > [Login Page] > [Add/Edit]
- CAS：[Device Management] > [CCA Servers] > [Manage [CAS_IP]] > [Authentication] > [Login Page] | [Override Global Settings]

図 3-1　　管理ユーザ ページ



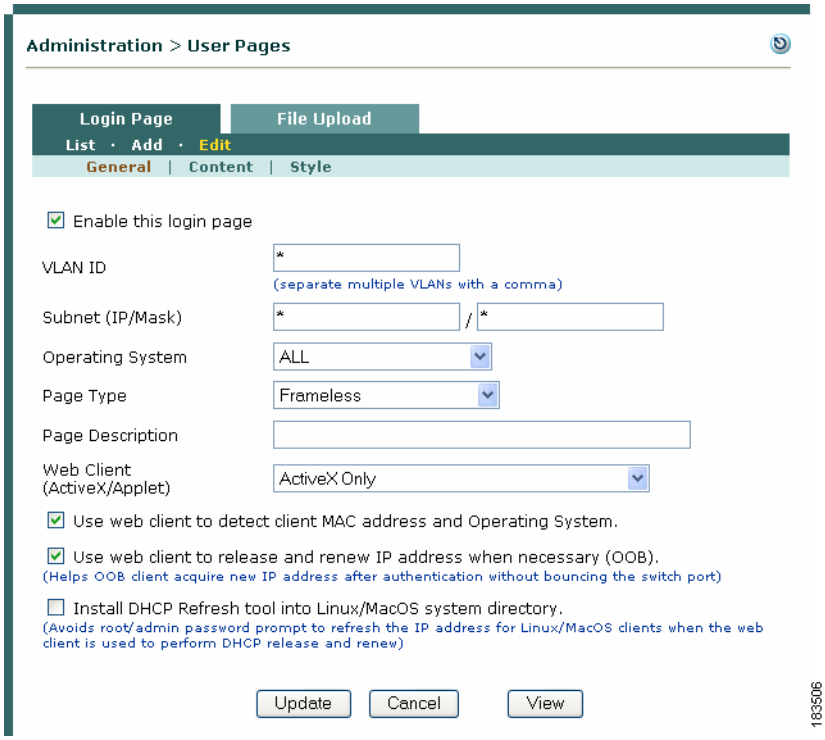
レイヤ 3 OOB：設定

- Login Page には、チェックボックスと [Use ActiveX or Java Applet to detect client MAC address when Clean Access Server cannot detect the MAC address] というドロップダウン メニューがあり、次のオプションを選択できます。
  - ActiveX Only（Active X のみ）
  - Java Applet Only（Java アプレットのみ）
  - ActiveX Preferred（Active X を優先）
  - Java Applet Preferred（Java アプレットを優先）
  - ActiveX on IE, Java Applet on non-IE Browser（ブラウザが IE の場合は Active X、IE ではない場合は Java アプレット）
- [Preferred] オプションでは、優先されるオプションがまずロードされ、そのロードが失敗した場合に別のオプションがロードされます。
  - Active X は IE 上で最も高速で動作します。
  - Active X はアプレットよりも優先され、高速に動作します。
- ActiveX は Windows XP の IE 6.0 でサポートされています。
- Java アプレットはほとんどのブラウザでサポートされています。

（注）　クライアント マシンの DHCP IP アドレスは、Agent または ActiveX コントロール、または Java アプレットを使用してリフレッシュされ、認証およびポスチャ評価後のポート バウンスは必要ありません。詳細については、『*Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.9*』の「Enable Web Client for Login Page」を参照してください。

認証 VLAN の変更検出の詳細については、『*Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.9*』の「Configuring Access to Authentication VLAN Change Detection」を参照してください。

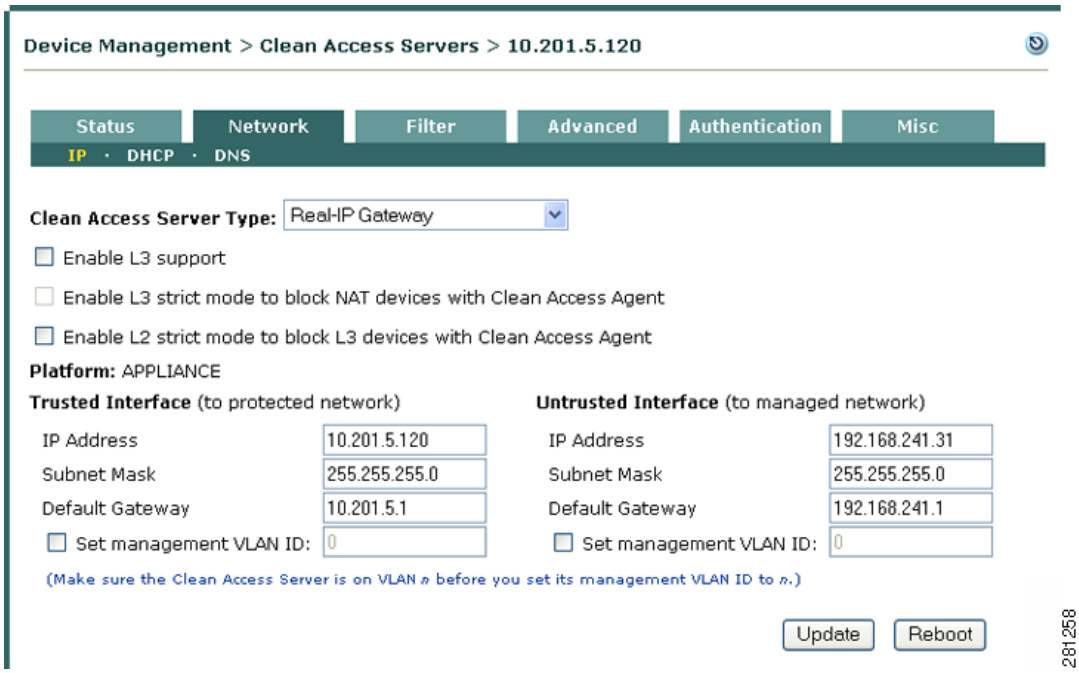
図 3-2　　管理ユーザ ページの編集



レイヤ 3 OOB：設定上の重要な注意事項

- 管理対象のサブネットを設定している場合、Cisco NAC アプライアンスはそれらのサブネットに L3 OOB を使用しません。
- 管理対象サブネットは L2 ユーザ専用です。
- [Device Management] > [CCA Servers] > [Manage [CAS_IP]] > [Network] > [IP] の [Enable L3 support] チェックボックスをオンにする必要があります。

図 3-3　L3 サポートのイネーブル化



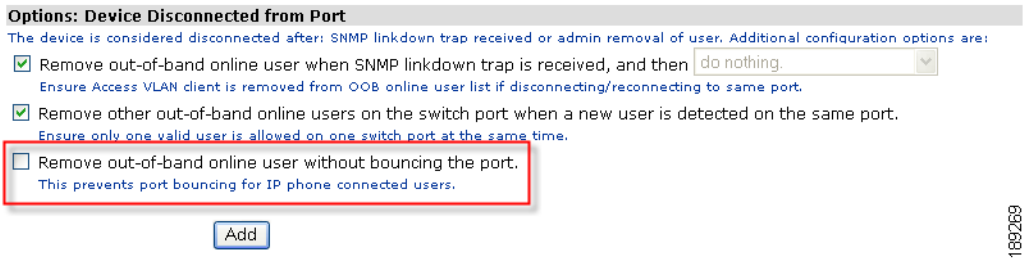
- クライアント マシンで Active X または Java アプレットを実行できるようにする必要があります。
- CAM でスイッチ ポートに対し、認証 VLAN からアクセス VLAN またはユーザ ロール VLAN へと VLAN が変更された場合には、ポート バウンスが必要になります。
  - [Port Profile]（[Switch Management] > [Profiles] > [Port] > [New/Edit]）で、[Bounce the port after VLAN is changed] がオンになっていることを確認してください。

    または
  - バージョン 4.1.2.0 以降の Agent、ActiveX コントロール、Java アプレットを使用してクライアントの DHCP IP アドレスを更新する場合は、ポートのプロファイルの [Bounce the switch port after VLAN is changed] オプションはディセーブルのままでもかまいません。この方法を使用する場合、『*Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.9*』の「DHCP Release/Renew with Agent/ActiveX/Java Applet」、「Configuring Access to Authentication VLAN Change Detection」、「Advanced Settings」に記載されているガイドラインと警告に従ってください。

図 3-4　ポート バウンスへの VLAN 設定の変更

– [Port Profile] で、[Remove out-of-band online user without bouncing the port] にチェックが入っていないことを確認します。

図 3-5　OOB 選択にチェックが入っていない状態



レイヤ 3 OOB：ネットワーキング

- SWISS パケットがアクセス VLAN を通過しないように、ネットワーク アクセス スイッチに ACL を追加することを推奨します。このようにすると、アクセス ネットワークの不要なパケットを減らすのと同時に、SWISS パケットが CAS に戻るとき、クライアント マシンで認証のループが生じないようにすることができます。

（注）　レイヤ 3 OOB Real-IP の配置で ACL を使用すると、Web ログインのリダイレクトが失敗したり、Agent のポップアップが表示されないことがあります。クライアント マシンの検出パケットの許可、またはブロックにアクセス コントロール リスト（IP 番号なしを含む）を使用するレイヤ 3 OOB の配置の場合、CAS 証明書と Discovery Host は同一の信頼できないインターフェイス IP アドレスかホスト名にする必要があります。また、レイヤ 3 OOB の SWISS 検出メカニズムでは、ネットワーク認証スイッチに設定された ACL で認証 VLAN から CAS の信頼できないインターフェイスへの TCP/UDP ポート 8905 のトラフィックを許可し、アクセス VLAN から CAS の信頼できないインターフェイスへの TCP/UDP ポート 8905 トラフィックをブロックすることが要求されます（レイヤ 3 OOB の配置でポリシー ベースのルーティングを使用する場合、これらの ACL は不要です）。

- L3 OOB は、通常ルーテッド アクセス環境で使用されます。
- OOB の目的は、認証、ポスチャ評価、および修復の場合にだけユーザ トラフィックが CAS を通過するようにすることです。
  - Unauthenticated、Quarantine、Temporary のロールでは、CAS はユーザのクレデンシャルを調べるとともに、ポリシー強制デバイスとしても機能します。
- 準拠性が証明されたユーザは CAS を迂回します。
- この機能は、ネットワーキング テクノロジー（PBR や VRF など）を使用して実現されます。
- 次の障害が発生することにより、クライアント マシンがレイヤ 3（インバンドおよびアウトオブバンドの両方）とレイヤ 2/ レイヤ 3 アウトオブバンド環境との間でローミングしたときに、Cisco NAC Agent が正常なユーザ認証を続けて表示する場合があります。また、ユーザがレイヤ 3 モードの Cisco NAC アプライアンス ネットワークから非 NAC ネットワークにローミングした場合、誤った Agent のログイン ダイアログが表示される場合があります。
  - ARP ポイズニング
  - クライアント マシンと CAS 間での一時的なネットワーク接続の切断
  - NAC 対応のクライアント マシンの非 NAC ネットワーク セグメントからの、CAS 上の非信頼インターフェイスの IP アドレスへのアクセス

  このような状況を防ぐため、次の項目を実行することをお勧めします。
  - すべての信頼ネットワーク（認証後）が、CAS の信頼インターフェイスのみを経由して CAS の非信頼インターフェイスの IP アドレスに到達できるようにする
  - すべての非 NAC ネットワークから CAS の非信頼インターフェイスの IP アドレスへの検出パケットをブロックする（CAS の信頼インターフェイスに到達した検出パケットはデフォルトでブロックされる）

（注） このような状況は、OOB ログオフ機能に固有のものではなく、一部のアウトオブバンドのトポロジに対する一般的な Cisco NAC Agent の動作にも発生します。