CHAPTER 1

導入の計画

この章では、ソフトウェアの導入を計画する場合の考慮事項について説明します。この章の内容は、次のとおりです。

概要

Clean Access Server（CAS）をインストールする前に、既存ネットワークに CAS を適合させる方法を検討する必要があります。

- CAS の動作モードの選択：動作モードにより、CAS が提供するサービスが決まります。たとえば、非信頼ネットワークと信頼ネットワークの間で、CAS はブリッジとして機能できます。また、非信頼ネットワークのゲートウェイとして機能することもできます。
- CAS を中央またはネットワーク エッジに配置します。

この章では、CAS の動作モードおよび導入オプションについて説明します。また、導入オプションが CAS やルータなどのネットワークの外部要素の設定に与える影響の概要を示します。

CAS の動作モード

CAS は、次に示すインバンド（IB）モードまたはアウトオブバンド（OOB）モードで動作します。

- **IB バーチャル ゲートウェイ**（L2 トランスペアレント ブリッジ モード）：非信頼ネットワークと既存ゲートウェイ間のブリッジとして機能し、ポスチャ評価、フィルタリング、その他のサービスを提供します。
- **IB Real-IP ゲートウェイ**：非信頼ネットワークのデフォルト ゲートウェイとして機能します。
- **IB NAT ゲートウェイ（テスト時のみ）**：IP ルータまたはデフォルト ゲートウェイとして機能し、非信頼ネットワークの Network Address Translation（NAT; ネットワーク アドレス変換）サービスを実行します。
- **OOB バーチャル ゲートウェイ**（L2 トランスペアレント ブリッジ モード）：認証および証明中には、バーチャル ゲートウェイとして動作します。その後、そのユーザは OOB に切り替わります（つまり、アクセス ネットワークに直接接続されます）。

- **OOB Real-IP ゲートウェイ**：認証および証明の処理中は Real-IP ゲートウェイ として動作します。その後、そのユーザは OOB に切り替わります（つまり、アクセス ネットワークに直接接続されます）。
- **OOB NAT ゲートウェイ（テスト時のみ）**：認証および証明中には、NAT ゲートウェイ として動作します。その後、そのユーザは OOB に切り替わります（つまり、アクセス ネットワークに直接接続されます）。

（注） NAT ゲートウェイ モードは、テストの簡易化を主目的としているため、最低限のネットワーク設定だけで、簡単に初期セットアップが可能です。ただし、NAT ゲートウェイは、処理できる接続数が限られているので、NAT ゲートウェイ モード（インバンドでもアウトオブバンドでも）の実働環境への導入はサポートされていません。NAT ゲートウェイ モードの場合、Cisco NAC アプライアンスはポート 20000 ～ 65535（45536 接続）を使用します。

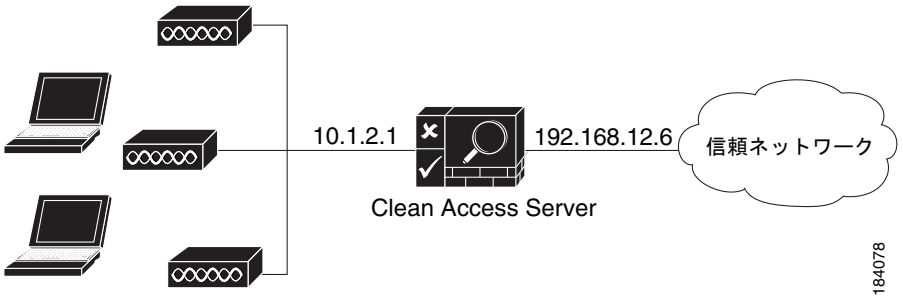
Clean Access Manager（CAM）は、そのドメイン内のインバンド CAS とアウトオブバンド CAS のどちらも制御できます。ただし、CAS 自体は、インバンドと OOB の*いずれか一方*に設定しなければなりません。

CAM の OOB 設定については、『*Cisco NAC Appliance - Clean Access Manager Installation and Configuration Guide, Release 4.5(1)*』を参照してください。次に、CAS の各動作モードについて説明します。

Real-IP ゲートウェイ

Real-IP ゲートウェイ 設定の場合、CAS は非信頼ネットワーク（管理対象）クライアントのデフォルト ゲートウェイとして機能します。非信頼ネットワークと信頼ネットワーク間のすべてのトラフィックは、CAS を通過します。CAS は IP フィルタリング規則、アクセス ポリシー、および設定されたその他のトラフィック処理メカニズムを適用します。

図 1-1　Real-IP ゲートウェイの構成



Real-IP ゲートウェイとして CAS を使用する場合は、2 つのインターフェイス（信頼側と非信頼側に 1 つずつ）の IP アドレスを指定する必要があります。2 つのアドレスは異なるサブネット上になければなりません。CAS は管理対象サブネットのゲートウェイとして機能する信頼できないインターフェイスを使用して、1 つまたは複数のサブネットを管理できます。管理対象サブネットの設定方法については、「管理対象サブネットまたはスタティック ルートの設定」（P.5-26）を参照してください。

CAS は、ルートのアドバタイズは行いません。そのため、管理対象のサブネットへのトラフィックが CAS の信頼できるインターフェイスにリレーされるように、ネクスト ホップ ルータにスタティック ルートを追加する必要があります。

（注）　Real-IP ゲートウェイ モードで CAS がトラフィックを送信できるのは 1 つの VLAN の信頼ポートからだけです。CAS の信頼ポートに接続しているスイッチ ポートをトランク ポートとして設定することはできません。

Real-IP ゲートウェイ モードの CAS は DHCP サーバまたは DHCP リレーとしても機能できます。DHCP サーバ機能がイネーブルの場合、CAS はクライアントに適切なゲートウェイ情報（つまり、特定の管理対象サブネットのために CAS が保持する適切なゲートウェイ IP）を提供します。CAS が DHCP リレーとして機能している場合は、DHCP サーバが管理対象のクライアントに該当するゲートウェイ情報（つまり、特定の管理対象サブネットのために CAS が保持する適切なゲートウェイ IP）を提供するように設定しなければなりません。詳細については、「管理対象サブネットまたはスタティック ルートの設定」（P.5-26）および第 6 章「DHCP の設定」を参照してください。

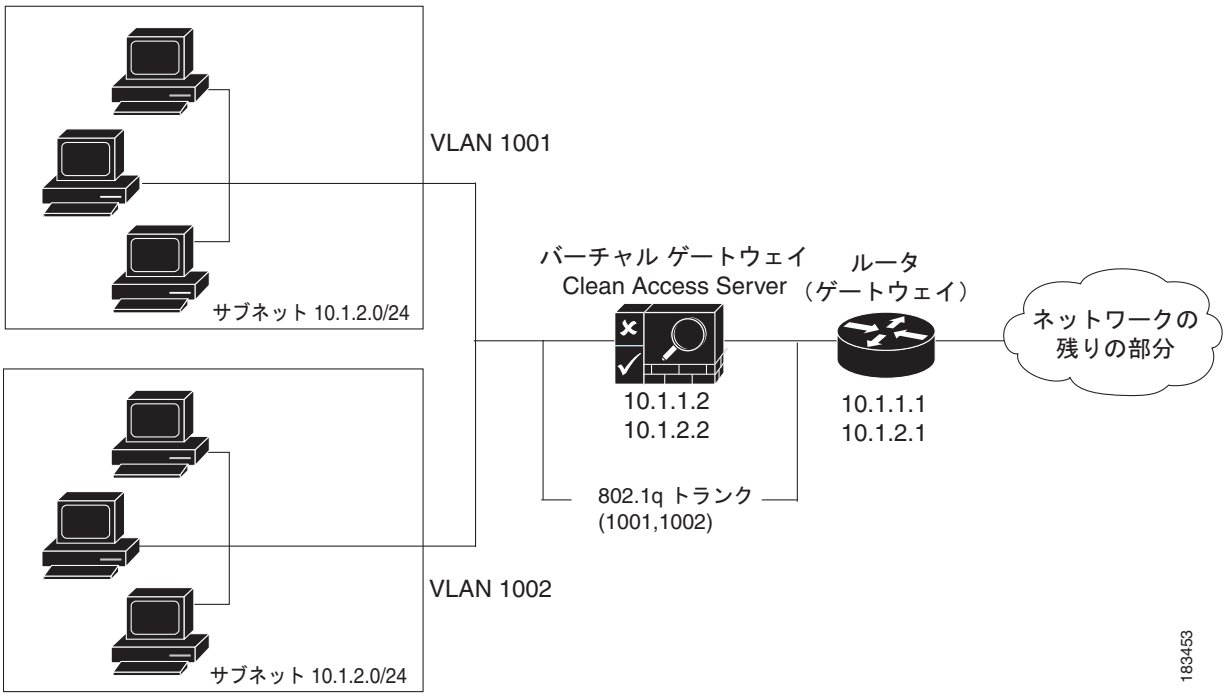
バーチャル ゲートウェイ

バーチャル ゲートウェイで導入の場合、CAS は標準イーサネット ブリッジとして機能しますが、IP フィルタおよび IPSec モジュールが提供する機能が追加されます。通常、この設定は、非信頼ネットワーク内にゲートウェイがすでに配置されていて、既存の設定を変更したくない場合に使用します。

たとえば、信頼できない 2 つのサブネット（10.1.1.0/24 および 10.1.2.0/24）があり、それぞれゲートウェイ 10.1.1.1 および 10.1.2.1 が配置されている場合、仮想ゲートウェイ モードの CAS は信頼できないサブネットとゲートウェイの間に配置されます（図 1-2）。信頼できないサブネットは、CAS の「管理対象サブネット」として設定されます。特に、次の点に注意してください。

- CAS は管理対象サブネットごとに IP アドレスを設定する必要があります。
- クライアントからのトラフィックは、ゲートウェイに到達する前に CAS を通過する**必要があります**。

図 1-2　　バーチャル ゲートウェイの構成



CAS がバーチャル ゲートウェイの場合は、次のようにします。

- CAS および CAM は異なるサブネット上に配置する**必要があります**。
- CAS の eth0 および eth1 には同じ IP アドレスを設定できます。
- ブリッジングされたサブネット内のすべてのエンド デバイスは、CAS の信頼できない側になければなりません。
- CAS で DHCP フォワーディングを使用するように設定しなければなりません。
- CAS の管理対象サブネットを設定します。図 1-2 の例では、2 つの管理対象サブネットを設定します。
  - 10.1.1.2 / 255.255.255.0 1001
  - 10.1.2.2 / 255.255.255.0 1002

CAS が OOB バーチャル ゲートウェイの場合、次の事項も適用されます。

- CAS および CAM は異なる VLAN（仮想 LAN）上に配置しなければなりません。
- CAS は、ユーザ VLAN やアクセス VLAN とは異なる VLAN に配置しなければなりません。

（注）

- バーチャル ゲートウェイ（インバンドまたは OOB）の場合は、CAS の信頼できないインターフェイス（eth1）をスイッチに接続する**前に**、Web コンソールを介して CAM に CAS を追加しておくことを推奨します。
- VLAN がマッピングされたバーチャル ゲートウェイの場合（インバンドまたは OOB）、[Device Management] > [CCA Servers] > [Manage [CAS_IP]] > [Advanced] > [VLAN Mapping] で VLAN マッピングが正しく設定されるまで、CAS の信頼できないインターフェイス（eth1）をスイッチに接続しないでください。「VLAN マッピングの設定」（P.5-39）を参照してください。

NAT ゲートウェイ

NAT ゲートウェイ設定の CAS は、Real-IP ゲートウェイ設定と同様に機能しますが、NAT サービスが追加されます。NAT が有効な場合、クライアントにはプライベート アドレス プールから動的に IP アドレスが割り当てられます。トラフィックは信頼できない（管理対象）ネットワークと外部ネットワーク間をルーティングされるため、CAS はプライベート アドレスとパブリック アドレス間の変換を実行します。CAS は標準のダイナミック NAT および 1:1 NAT をサポートします。1:1 NAT の場合、パブリック アドレスとプライベート アドレスは 1 対 1 で対応します。1:1 NAT を使用すると、IP アドレスだけでなく、ポート番号も対応付けて、変換することができます。

（注） NAT ゲートウェイ モードは、テストの簡易化を主目的としているため、最低限のネットワーク設定だけで、簡単に初期セットアップが可能です。ただし、処理できる接続数が限られているので、NAT ゲートウェイ モード（インバンドでもアウトオブバンドでも）の実働環境への導入はサポートされていません。詳細については、「ファイアウォールを通じた CAM/CAS の接続」（P.4-24）を参照してください。

中央配置とエッジ配置

CAS はネットワークの中央またはエッジに配置できます。中央配置の場合は、導入しなければならない CAS 数が削減されるため、管理および拡張が容易です。また、中央配置の場合は、非信頼ネットワークに対してルーティングまたはブリッジングを実行するように CAS を設定できます。

Cisco NAC アプライアンス を使用すると、CAS をユーザから複数ホップ分遠くに移動する必要がある場合に、マルチホップ L3 配置を実現できます。

ルーテッド中央配置（L2）

ルーテッド中央配置の場合は、管理するサブネットごとに Real-IP ゲートウェイとして機能するように CAS を設定します。

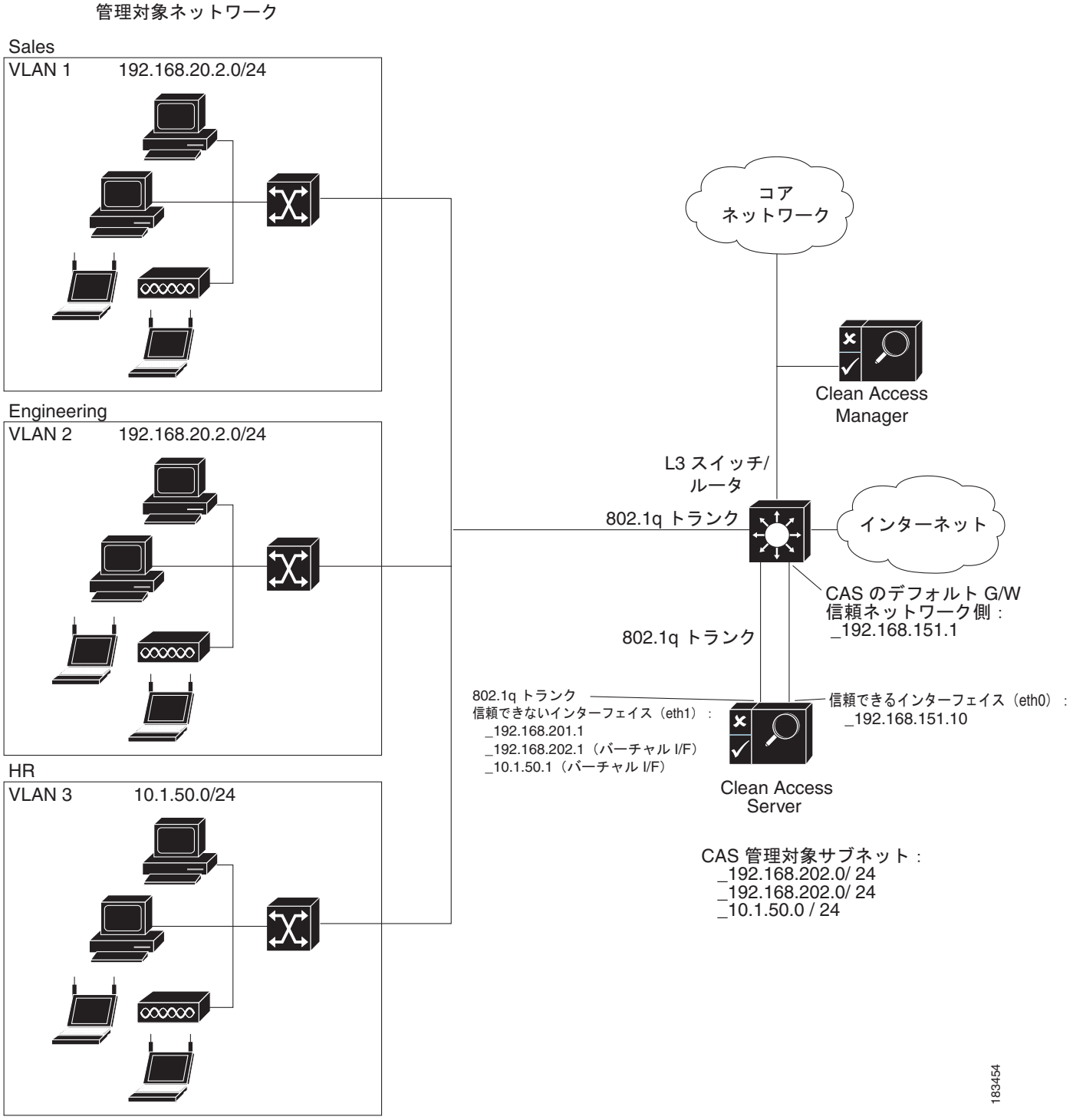
導入手順

一般的なネットワークに中央でルーティングされる CAS を導入する具体的な手順は、次のとおりです。

1. CAS を介して管理するサブネットに対して、既存の L3 スイッチまたはルータでのルーティングをオフにします。
2. CAS の信頼できないインターフェイスを、管理対象サブネットのゲートウェイとなるように設定します。
3. CAS の信頼できるインターフェイスのデフォルト ゲートウェイを、L3 スイッチまたはルータとなるように設定します。
4. L3 スイッチまたはルータでスタティック ルートを追加して、管理対象サブネットのトラフィックを CAS の信頼できるインターフェイスにルーティングします。
5. 独自の DHCP サーバを使用している場合は、DHCP リースを通してクライアントに送信するデフォルト ゲートウェイ アドレスが CAS の信頼できないインターフェイスのアドレスとなるように、設定を変更します。

VLAN 対応環境の場合は、複数の VLAN が単一 CAS を介して トランキングされます。単一の CAS を介して（VLAN トランキングによって）複数の VLAN を集約すると（ユーザの場所、配線、共通のニーズに基づいて編成すると）、配置を簡潔にすることができます。図 1-3 に、ルーテッド中央配置を示します。

図 1-3　VLAN 対応ネットワークのルーテッド中央配置



マルチホップ L3 配置

CAS はネットワークのエッジ付近、またはネットワークから複数ホップ離れた位置に配置できます。L3 中央配置の場合、CAS はユーザから複数ホップ離れた位置に配置できます。マルチホップ L3 配置には、次の利点があります。

- 導入が簡単です。CAS はルータ間に配置されます。スパニング VLAN は不要であり、必要な CAS 数は少なくて済みます。
- CAS を通過する必要があるパケットは一部に限定されます。信頼ネットワークにアクセスする場合だけ、ユーザ トラフィックは CAS を通過する必要があります。

ただし、Cisco NAC アプライアンス ポリシーは CAS でだけ適用されることに注意してください。CAS に到達しないトラフィックには、ポリシーが適用されません。

導入手順

一般的なネットワークに中央でルーティングされる CAS を導入する具体的な手順は、次のとおりです。

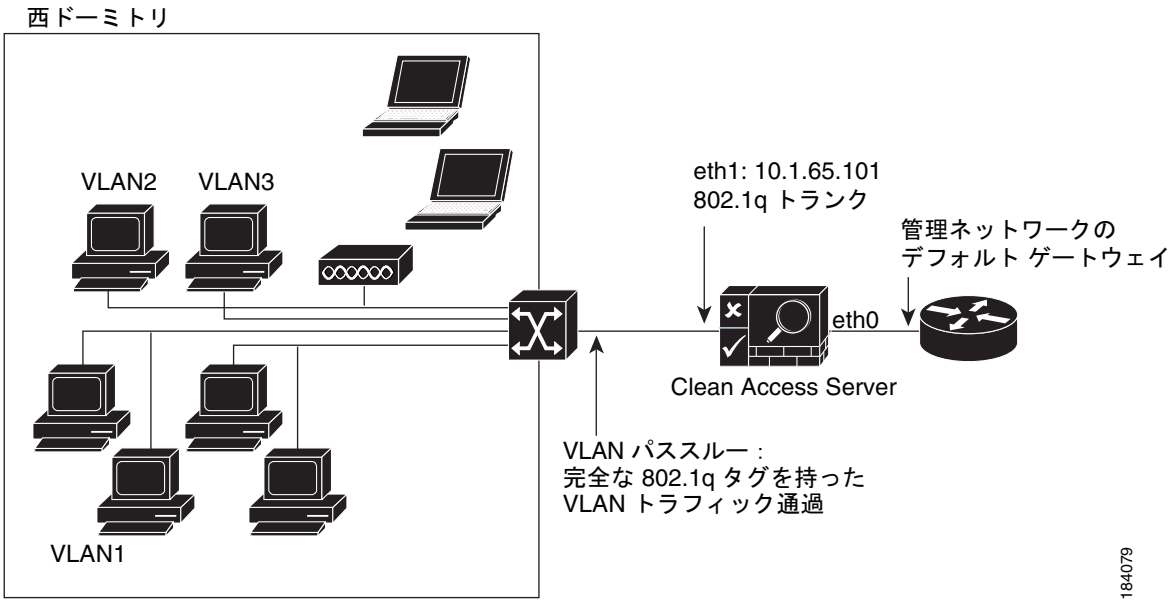
1. [Device Management] > [CCA Servers] > [Manage [CAS_IP]] > [Network] の順番に進み、[Enable L3 support for Clean Access Agent] のチェックボックスをクリックして、CAS 上で L3 をイネーブルにします。
2. レイヤ 2 で CAS に近接するユーザ サブネットの場合は、管理対象のサブネットを設定する必要があります。CAS から 1 つまたは複数ホップ以上離れているユーザ サブネットの場合は、スタティック ルートを設定する必要があります。したがって、CAS で L3 サポートをイネーブルにしている場合、L3 ユーザは [Device Management] > [CCA Servers] > [Manage [CAS_IP]] > [Advanced] > [Static Routes] でサブネットを設定しなければなりません。[Device Management] > [CCA Servers] > [Manage [CAS_IP]] > [Advanced] > [Managed Subnets] は使用しないでください。
3. [Device Management] > [Clean Access] > [Clean Access Agent] > [Distribution] の [Discovery Host] フィールドを設定します。
4. VPN（仮想私設網）コンセントレータ統合のための L3 マルチホップ機能をイネーブルにする場合は、第 7 章「Cisco VPN コンセントレータとの統合」に記載されたすべての設定を実行します。

ブリッジング中央配置

CAS がブリッジ（バーチャル ゲートウェイ）として設定された中央配置の場合は、VLAN トランクを使用して管理対象サブネットから CAS に送信されるトラフィックを集約してから、これらのトラフィックを L3 スイッチまたはルータの各ゲートウェイに転送する必要があります。

クライアントからゲートウェイへのパスが存在しないようにするには、CAS の信頼できないインターフェイスに接続されたすべての VLAN を集約するスイッチを配置し、CAS の信頼できるインターフェイスを L3 スイッチまたはルータに直接接続する必要があります（図 1-4 を参照）。CAS インターフェイスをトランキング ポートに接続し、VLAN パススルーを実現する必要があります。

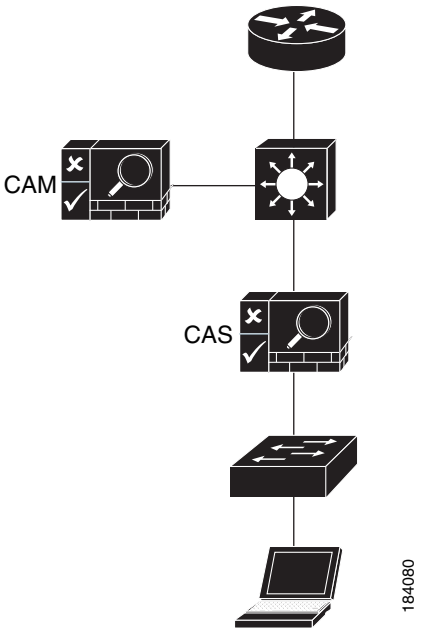
図 1-4　VLAN 対応ネットワーク内のブリッジング中央配置



エッジ配置

中央配置には必要な CAS 数が削減されるという利点がありますが、常にこの方法を使用できるわけではありません。たとえば、ネットワーク エッジでギガビット スループットを使用している場合は、エッジ配置が必要です。エッジ配置の場合、CAS はネットワーク内の各管理対象サブネットとルータの間に配置されます（図 1-5 を参照）。このようにすると、CAS は管理対象デバイスの MAC（メディア アクセス制御）アドレスを継続的にキャプチャします。エッジ配置の CAS は、バーチャル ゲートウェイまたは Real-IP ゲートウェイとして機能できます。

図 1-5　エッジ配置



CAS 動作モードの概要

表 1-1 に、各動作モードの機能および利点の概要を示します。

表 1-1　CAS 動作モードの概要

CAS のタイプ	機能	利点
バーチャル ゲートウェイ	• CAS は管理対象ネットワークのブリッジと同様に機能します。 • CAS は DHCP パススルーとして機能します。	• CAS は控えめに機能します。 • 既存ネットワークを変更しない場合に適しています。 • メイン ルータにスタティック ルートを定義する必要はありません。
Real-IP ゲートウェイ	• CAS は管理対象サブネットのゲートウェイとして機能します。 • CAS は管理対象サブネットのスタティック ルートとして指定されます。 • CAS は DHCP サービスを実行したり、DHCP リレーとして機能したりできます。	• 新しいサブネットを管理対象ネットワークに使用できる状況で有効です。 • クライアントには実際の IP アドレスが割り当てられます。 • CAS の高度な DHCP サービスを利用します。

表 1-1　CAS 動作モードの概要 （続き）

CAS のタイプ	機能	利点
NAT ゲートウェイ	• CAS は NAT または Port Address Translation（PAT; ポート アドレス変換）サービスを実行して、クライアントがプライベート アドレスを使用できるようにします。 • 管理対象クライアントに DHCP アドレス割り当てを実行します。 • 信頼できる側では、管理対象クライアントから送信されたすべてのトラフィックは CAS から送信されたと認識されます。	• 管理対象クライアントのプライベート アドレス範囲を使用できます。 • セットアップは簡単です。ルータの設定やサブネットの作成は作業に含まれません。 • 必要なのは 2 つの IP アドレスだけです。
OOB バーチャル ゲートウェイ	• CAS が管理対象ネットワークのブリッジと同様に機能するのは、認証、ポスチャ評価、および修復プロセス中だけです。 • CAS は認証 VLAN の DHCP パススルーとして機能します。	• 正常にログオンしたあと、ユーザ トラフィックは CAS を迂回し、スイッチ ポートを直接通過します。 • ユーザはロールベース セッション タイマーを介してログアウトしたり、SNMP（簡易ネットワーク管理プロトコル）トラップをリンクダウンしたりできます。 • エッジまたはコア（中央）スイッチに配置できます。 • クライアント ポートをバウンスする必要はありません。 • IP 電話 および PC 間でポートを共有する場合の推奨設定です。

表 1-1　CAS 動作モードの概要 （続き）

CAS のタイプ	機能	利点
OOB Real-IP ゲートウェイ	• CAS が管理対象ネットワークのインライン L3 ルータとして機能するのは、認証、ポスチャ評価、および修復プロセス中だけです。 • CAS は DHCP サービスを実行したり、DHCP リレーとして機能したりできます。 • ユーザは認証 VLAN から DHCP アドレスを取得します。 • L3 スイッチ/ルータの設定 : CAS を管理対象サブネットのデフォルト ゲートウェイとして設定します。	• クライアントには実際の IP アドレスが割り当てられます。 • 正常にログオンしたあと、ユーザ トラフィックは CAS を迂回し、スイッチ ポートを直接通過します。 • ポート バウンスは必要ありません。Web ログイン ページからダウンロードされた 4.1.1.0+ Agent または ActiveX や Java アプレットによって DHCP の解放と更新がトリガーされます。
OOB NAT ゲートウェイ	• CAS が管理対象ネットワークのインライン L3 ルータとして機能するのは、認証、ポスチャ評価、および修復プロセス中だけです。 • CAS は DHCP サービスを実行したり、DHCP リレーとして機能したりできます。 • ユーザは認証 VLAN から DHCP アドレスを取得します。 • NAT 設定を介してプライベート アドレス範囲を使用できます。 • L3 スイッチまたはルータの設定 : L3 スイッチまたはルータでの管理対象ネットワークのルーティングをオフにします。	• 認証 VLAN 上のクライアントには、NAT IP アドレスが割り当てられます。 • 正常にログオンしたあと、ユーザ トラフィックは CAS を迂回し、スイッチ ポートを直接通過します。 • クライアントがアクセス VLAN から新しい DHCP アドレスを取得するには、インターフェイスをバウンスする必要があります。