CHAPTER 4

トラフィック代行受信の設定

この章では、IP および TCP ヘッダー情報に基づいて IP ベース ネットワークのすべての TCP トラフィックを代行受信し、Wide Area Application Engine（WAE）へリダイレクトする Wide Area Application Service（WAAS）ソフトウェア サポートについて説明します。この章では、トラフィックを WAE へ透過的にリダイレクトするための Web Cache Communication Protocol（WCCP; Web キャッシュ通信プロトコル）、Policy-Based Routing（PBR; ポリシーベース ルーティング）、およびインライン モードの使用方法について説明します。

（注） この章では、ネットワークに存在する WAAS Central Manager と WAE を総称する用語として「WAAS デバイス」を使用します。「WAE」は、WAE アプライアンスおよび WAE ネットワーク モジュール（NME-WAE デバイス ファミリ）を示します。

この章の手順を実行する前に、『*Cisco Wide Area Application Services Quick Configuration Guide*』の説明に従って WAAS ネットワークの基本的な初期インストールと設定を完了する必要があります。この章に現れる CLI コマンドの詳細なコマンド構文情報については、『*Cisco Wide Area Application Services Command Reference*』を参照してください。WCCP の詳細については、『*Cisco IOS Configuration Fundamentals Configuration Guide*』と『*Cisco IOS Configuration Fundamentals Command Reference*』を参照してください。

この章の構成は、次のとおりです。

要求リダイレクション方式

WAAS ネットワークでは、最適化、冗長性の除去、および圧縮のために、ブランチ オフィスのクライアントとデータセンターのサーバ間のトラフィックを WAE へリダイレクトできます。トラフィックは、ルータに設定されているポリシーに基づいて代行受信され、WAE へリダイレクトされます。要求を透過的にローカル WAE へリダイレクトするネットワーク要素は、WCCP バージョン 2 または PBR を使用してトラフィックを透過的にローカル WAE へリダイレクトするルータまたはレイヤ 4 ～ 7 のスイッチ（たとえば、Catalyst 6500 シリーズ Content Switching Module [CSM] や Application Control Engine [ACE]）です。代わりに、Cisco WAE Inline Network Adapter のある WAE でインライン モードを使用して、トラフィックを直接代行受信できます。

WAAS ネットワークでは、次の 2 つのモードでトラフィックを代行受信できます。

- 透過モード（WCCP または PBR）
  - アプリケーション トラフィックの場合、クライアント アプリケーションやクライアント / サーバ アプリケーションの設定を変更する必要はありません。無差別 WCCP モードでは、ネットワーク要素が、アプリケーション トラフィックを透過的にローカル WAE へリダイレクトします。

  （注） TCP 無差別モード サービス（WCCP サービス 61 と 62）には、CIFS プロトコルなどの、転送として TCP を使用するすべてのプロトコルが含まれています。ルータと Edge WAE および Core WAE で TCP 無差別モードを有効にした場合、CIFS が TCP 上で実行されているために、CIFS トラフィックは Cisco WAE にリダイレクトされます。

  - CIFS トラフィックに対して、Edge WAE は、システム設定とポリシーに基づいてトラフィックを高速化します。WAE は、ファイル サーバが切断モードで設定され、ネットワークが切断されなければ、透過モードで動作中は、ファイル サーバ名をアドバタイズしません。クライアントとファイル サーバ間の CIFS トラフィックは、クライアント本来のサーバへの到達機能に依存します（直接 IP トラフィック経由または名前解決）。TCP 無差別モードで、ルータは CIFS トラフィック（TCP ポート 139 または 445）をローカルの WAE へリダイレクトし、そこで、その WAE のローカル ポリシーに基づいて最適化されます。ローカル プリント サービスが設定されている場合、このモードで EdgeWAE が提供している唯一のネーム サービスが、ローカル プリント サービスのためのものです。

  （注） Edge WAE は透過（前述）または非透過（後述）の 2 つのモードのうちの 1 つでのみ動作します。このモードは、WAE で設定され、その WAE で高速化されるすべてのファイル サーバに適用されます。設定されたモードは Central Manager と WAE で保存されます。

- 非透過（明示）モード（WCCP バージョン 2 では無効、CIFS トラフィックのみ適用可能）
  - CIFS トラフィックでは、Edge WAE は、ブランチ オフィスのネットワークにファイル サーバ名を公開します。この公開された名前は、NetBIOS 名との競合のために、元のファイル サーバ名と同じではない場合があります。クライアント コンピュータは、Edge WAE によって公開された名前を使用して、高速化されたファイル サーバからドライブをマップする必要があります。これは、デフォルトのモードです。
  - アプリケーション トラフィック（CIFS ではない）に対して、トラフィックを最適化するために代行受信のあるフォームが必要です。WCCP、PBR、インライン モード、または CSM/ACE リダイレクションを設定する必要があります。そうでない場合は、CIFS ではないトラフィックは Cisco WAAS で最適化できません。

- インライン モード

  WAE は物理的にも透過的にもクライアントとルータ間のトラフィックを代行受信します。このモードを使用するには、Cisco WAE Inline Network Adapter が搭載された WAE を使用する必要があります。

表 4-1 に、WAAS でサポートされる透過トラフィック代行受信方式を示します。

表 4-1　サポートされる透過トラフィック代行受信方式

方式	説明
WCCP Version 2	アプリケーション トラフィックと Wide Area File Services（WAFS）トラフィックの透過的な代行受信に使用します。ブランチ オフィスとデータセンターで、トラフィックをローカル WAE へ透過的にリダイレクトするために使用します。WCCP 対応ルータまたはレイヤ 3 スイッチが、透過的にトラフィックを代行受信し、ローカル WAE へリダイレクトします。 ブランチ オフィスのルータと Edge WAE およびデータセンターのルータと Core WAE で、WCCP を設定する必要があります。詳細については、次のセクションを参照してください。 • WCCP を使用した WAE への透過的な TCP トラフィックのリダイレクション（p.4-4） • WCCP を使用した CIFS クライアント要求の透過的なリダイレクション（p.4-49）
Microsoft DFS	CIFS クライアント用の WAFS トラフィックの透過的または非透過的な代行受信だけに使用します。「Microsoft DFS を使用した CIFS クライアント要求の代行受信」（p.4-51）を参照してください。
NETBIOS	WAE がオリジン サーバ名を公開しない場合、CIFS クライアント用の WAFS トラフィックの非透過的な代行受信に使用します。WAE がオリジン サーバ名を公開する場合は、CIFS クライアント用の WAFS トラフィックの透過的な代行受信のために NetBIOS が使用されます。「明示的な共有命名を使用した明示的な CIFS クライアント要求の代行受信」（p.4-50）を参照してください。
PBR	ブランチ オフィスで、広域アプリケーションの最適化に使用します。ブランチ オフィスのルータは、PBR を使用してクライアントとサーバ両方のトラフィックを透過的に代行受信し、同じブランチ オフィスに存在する Edge WAE へルーティングするように設定されます。 データセンターでは、データセンター アプリケーションの最適化に使用します。データセンター ルータや L3 スイッチは、透過的に代行受信したり、クライアントとサーバをデータセンター内で Core WAE にルーティングするために、PBR を使用するように設定されている場合があります。ただし、PBR は、複数の WAE 間の負荷分散（WCCP が行うような）をサポートしません。Cisco CSM や ACE などのロード バランサを使用した場合でも負荷分散をサポートしません。「PBR を使用した WAE へのすべての TCP トラフィックの透過的なリダイレクション」（p.4-32）を参照してください。
インライン	アプリケーション トラフィックと WAFS トラフィックの透過的な代行受信に使用します。「TCP トラフィックの透過的な代行受信へのインライン モードの使用」（p.4-43）を参照してください。
CSM または ACE	データセンターの最適化のために、Cisco Catalyst 6500 Content Switching Module（CSM）または Application Control Engine（ACE）がデータセンターにインストールされています。CSM と ACE は、データセンター内の複数の WAE 間のトラフィックの代行受信と負荷分散の両方を行うことができます。

すべての TCP トラフィックの要求リダイレクション

この項では、TCP トラフィックの要求リダイレクションをサポートする方式について説明します。この項の内容は、次のとおりです。

WCCP を使用した WAE への透過的な TCP トラフィックのリダイレクション

WAFS ソフトウェアは、WCCP 標準バージョン 2 を使用して、リダイレクションを実行します。WCCP バージョン 2 の主な機能は、次のとおりです。

- WCCP サービスあたり最大 32 の WAE
- 複数のルータをサポート
- WAE と WCCP 対応ルータとの間のプロトコル メッセージのマルチキャスト
- プロトコル パケットの認証
- 非 HTTP トラフィックのリダイレクション
- パケット リターン（GRE を含む。WAE は、リダイレクトされたパケットを拒否し、転送するルータへ戻すことができる）
- L2 キャッシング（ルータと GRE を使用）およびマスキング（負荷分散を改善するため）
- 複数の転送方式
- サービス グループ内でのパケット分散方式のネゴシエーション
- WAE とサービス グループ間のコマンドとステータスの交換

（注）　WCCP は、IPv4 ネットワークでのみ動作します。

WAAS ソフトウェアは、WCCP TCP 無差別モードサービス（サービス 61 および 62）をサポートしています。この WCCP サービスでは、ルータと WAE で WCCP バージョン 2 が動作している必要があります。

TCP 無差別モード サービスとは、すべての TCP トラフィックを代行受信し、ローカル WAE へリダイレクトする WCCP サービスです。

また、WAAS ソフトウェアは、サービス パスワード、WAE フェールオーバー、フローの保護、および固定的バイパスもサポートしています。

Cisco 2600、Cisco 2800、Cisco 3600、Cisco 3700、Cisco 3800、および Cisco 7600 シリーズ ルータがサポートされ、Cisco WAE で使用するために WCCP バージョン 2 サポートを手動で設定し、有効にすることができます。Catalyst 6000 および Catalyst 6500 シリーズ スイッチも、WCCP バージョン 2 をサポートしています。

（注）

Cisco 2500、2600、および 3600 ルータを含む多くの従来型ルータは、Integrated Services Router（ISR）モデル 2800 や 3800 のような新しいルーティング プラットフォームに比べ、処理能力とメモリが大幅に劣っています。そのため、WCCPv2 や PBR の使用によってルータの CPU 使用率が高くなり、動作が不安定になることがあります。これらのルータで動作するように WAAS を設定できますが、新しいルーティング プラットフォームと同じレベルのパフォーマンスや拡張性は実現できません。Cisco ISR は、ブランチ オフィス用のルーティング プラットフォームとして最適です。

WAE がサービス グループから除外されるなど動作が不安定になる場合は、ユーザ、サーバ、WAE、および WAN と接続するルータのすべての物理インターフェイスで、公平キュー方式、重み付き公平キュー方式、または速度制限を有効にしてください。公平キュー方式はサブインターフェイスでは設定できず、入力と出力の両方の物理インターフェイスで設定する必要があります。LAN や WAN インターフェイスでは、同様の公平さを提供する公平キュー方式以外のキュー方式がすでに設定されており、それで十分です。

さらに、ルータの LAN 側インターフェイスで受信できる帯域幅を制限すると、ルータのインターフェイス キューの混雑が軽減され、パフォーマンスが向上し、CPU 利用率が低下します。ルータの最大インターフェイス帯域幅を WAN 帯域幅容量の 10 倍未満に設定します。たとえば、WAN リンクが T1 である場合、LAN インターフェイスと WAE の LAN インターフェイス帯域幅を 10 × T1 = 10 × 1.544 Mbps（約 15 Mbps）に制限する必要があります。詳細については、Cisco IOS マニュアルを参照してください。

ここでは、次の内容について説明します。

WCCP を設定するためのガイドライン

WCCP バージョン 2 を使用して WAE で透過的なリダイレクションを設定するときは、次の一般的なガイドラインに従ってください。

- 可能な場合は常に、着信インターフェイスでパケットを代行受信し、リダイレクトします。
- WAE をクライアントおよびサーバとして同一の VLAN またはサブネットに配置する場合は、WCCP GRE を WCCP 出力方式として使用します。IP 転送出力方式を使用する場合は、このトポロジは利用できません。
- Edge WAE は、パケットを暗号化したり圧縮したりせずに、内部 Network Address Translation（NAT; ネットワーク アドレス変換）ファイアウォール（存在する場合）の一部として動作する必要があります。
- Catalyst 6500 シリーズ スイッチまたは Cisco 7600 シリーズ ルータを使用している場合は、パケット転送方式としてレイヤ 2 リダイレクションを使用します。他の Cisco シリーズ ルータを使用している場合は、レイヤ 3 GRE パケットリダイレクションを使用します。
- Hot Standby Router Protocol（HSRP; ホットスタンバイ ルータ プロトコル）と WCCP を使用する場合、WAE のデフォルト ゲートウェイとして HSRP または Virtual Router Redundancy Protocol（VRRP; 仮想ルータ冗長プロトコル）を設定し、HSRP グループのルータのプライマリ アドレスに WAE WCCP ルータリストを設定します。
- 可能な場合は、ハードウェアがサポートする方式（Cisco Express Forwarding [CEF、dCEF]）を使用します。CEF は不要ですが、パフォーマンスを改善するために推奨します。ルータで CEF が有効になっている場合、WCCP は IP CEF を使用できます。
- ネットワークのクライアント側に Edge WAE を配置し、ルータを経由するクライアント側のパケット数を最小限に抑えます。

- DoS 攻撃（サービス拒絶攻撃）を避けるため、WCCP パスワードを使用します。詳細については、「ルータ上のサービス グループ パスワードの設定」（p.4-11）を参照してください。
- 新たに実装した場合は、WCCP リダイレクト リストを使用して、クライアントまたはサーバの読み込みを制限します。詳細については、「ルータ上の IP アクセス リストの設定」（p.4-9）を参照してください。
- WAE は、複数の WCCP 対応ルータからリダイレクトされたパケットを受け入れるように設定する必要があります。
- WAAS CLI または WAAS Central Manager GUI から、WAE で設定できる WCCP 設定とサービスのリストを迅速に表示できます。WAAS CLI から、**wccp** EXEC コマンドと疑問符（?）を入力します。WCCP バージョン 2 が有効になっている WAE の出力例は、次のとおりです。

```
WAE(config)# wccp ?
   access-list      Configure an IP access-list for inbound WCCP encapsulated
traffic
   flow-redirect    Redirect moved flows
   router-list      Router List for use in WCCP services
   shutdown         Wccp Shutdown parameters
   tcp-promiscuous  TCP promiscuous mode service
   version          WCCP Version Number
```

- 基本 WCCP を設定するには、ネットワーク内の少なくとも 1 台のルータとトラフィックをリダイレクトしたい WAE、WCCP サービスを有効にする必要があります。WAE を起動し稼働させるために、使用可能な WCCP 機能またはサービスをすべて設定する必要はありません。ブランチ オフィスとデータセンターのルータと WAE で基本的な WCCP 設定を完了する方法の例については、『*Cisco Wide Area Application Services Quick Configuration Guide*』を参照してください。
- WCCP バージョン 1 は Web トラフィック（ポート 80）しかサポートしていないため、ルータと WAE が WCCP バージョン 1 の代わりに WCCP バージョン 2 を使用するように設定する必要があります。
- ルータで WCCP を有効にしたら、『*Cisco Wide Area Application Services Quick Configuration Guide*』の説明に従って、ルータと WAE で TCP 無差別モード サービス（WCCP サービス 61 および 62）を設定する必要があります。
- WAE は、TCP 無差別モードで動作するために、WCCP バージョン 2 サービス 61 および 62 使用します。この 2 つの WCCP サービスは、WAE の標準名 tcp-promiscuous で表現されます。
- ルータと WAE の両方で CLI コマンドを使用して基本的な WCCP を設定できます。また、CLI コマンドを使用して WCCP 用にルータを設定し、WAAS Central Manager GUI を使用して WAE 上の基本的な WCCP を設定できます。『*Cisco Wide Area Application Services Quick Configuration Guide*』に記載されている設定例では、CLI を使用して WAE 上の基本的な WCCP を設定しています。

  最初の Edge WAE と Core WAE では、『*Cisco Wide Area Application Services Quick Configuration Guide*』の説明に従って、WAAS CLI を使用して WCCP の基本的な初期設定を完了することを推奨します。

  WCCP 透過リダイレクションが正常に動作していることを確認したら、WAAS Central Manager GUI を使用して集中的にこの基本的な WCCP 設定を変更したり、WAE（または WAE のグループ）用に追加の WCCP 設定（負荷分散など）を構成することができます。詳細については、「WAE 用の WCCP 設定の集中管理」（p.4-12）を参照してください。
- ルータ上の基本的な WCCP を構成したら、「WCCP 対応ルータでの高度な WCCP 機能の設定」（p.4-7）の説明に従って、ルータ上の高度な WCCP 機能を構成できます。

ファイル サーバ アクセス方式に関するガイドライン

一部のファイル サーバには複数のネットワーク インターフェイスがあり、複数の IP アドレスを通じて到達できます。このようなサーバの場合は、Edge WAE の WCCP 受容リストに、使用できるすべての IP アドレスを追加する必要があります。このようにすると、クライアントは、登録されていない IP アドレスを使用して Edge WAE をバイパスすることがなくなります。WAE Device Manager GUI は、すべての IP アドレスを表示します。

一部のファイル サーバには、複数の NetBIOS 名と、ただ 1 つの IP アドレスがあります。このようなサーバの場合は、クライアントが UNC パス内の IP アドレス（すなわち、\\server\share でなく \\IP_address\share）を使用して接続すると、WAAS は、WAE Device Manager GUI でサーバ リストからこの IP アドレスと一致する最初の NetBIOS 名を選択します。WAAS は、その名前を使用して、Core WAE とファイル サーバ間の NetBIOS ネゴシエーションを実行し、キャッシュにリソースを作成します。ファイル サーバが複数の NetBIOS 名を使用して（設定が異なる場合がある）仮想サーバを表し、プライマリ サーバ名として識別される 1 つの NetBIOS 名を持つ場合は、サーバ リストの先頭にその名前を置きます。

WCCP 対応ルータでの高度な WCCP 機能の設定

この項では、WAAS ネットワークで要求を WAE へ透過的にリダイレクトする WCCP 対応ルータで、高度な WCCP バージョン 2 機能を設定する方法について説明します。

- WCCP サービス グループをサポートするためのルータの設定（p.4-7）
- ルータ上の IP アクセス リストの設定（p.4-9）
- ルータ上のサービス グループ パスワードの設定（p.4-11）
- ルータ上のループバック インターフェイスの設定（p.4-11）

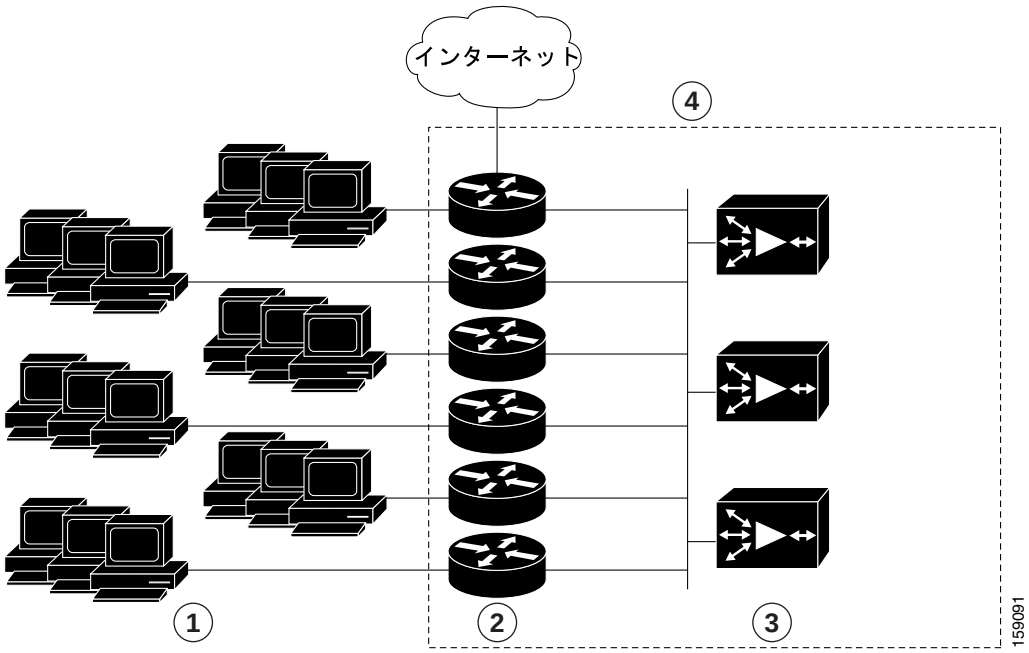
（注）　このセクションの手順を実行する前に、『*Cisco Wide Area Application Services Quick Configuration Guide*』の説明に従ってルータに基本 WCCP を設定しておく必要があります。

WCCP サービス グループをサポートするためのルータの設定

WCCP バージョン 2 では、WAE グループ内の 1 組の Edge WAE が、複数のルータに接続することができます。グループ内の WAE、および同じ WCCP サービスを稼働している WAE グループに接続されている WCCP バージョン 2 対応ルータのことを「*サービス グループ*」と呼びます。

WCCP バージョン 2 対応ルータは、Edge WAE との通信を通じて、使用できる Edge WAE を識別します。ルータと Edge WAE は相互に識別し、WCCP バージョン 2 を使用してサービス グループを形成します。図 4-1 を参照してください。

図 4-1　WCCP バージョン 2 でのサービス グループ



1	ファイル サービスを要求するクライアント	3	Edge WAE として機能する WAE
2	Cisco ルータ	4	WAE サービス グループ

Edge WAE のグループが存在する場合は、すべての WCCP バージョン 2 対応ルータが Edge WAE のグループを認識し、最も小さい IP アドレスを持つ Edge WAE がリード Edge WAE になります。

次の手順で、サービス グループ内の 1 つの Edge WAE をリードとして指定する方法を説明します。

1. 各 Edge WAE に、WCCP 対応ルータのリストが設定されます。

   複数の WCCP 対応ルータがグループにサービスを提供できます（最大 32 台のルータを指定できます）。サービス グループ内の使用可能なルータはどれも、グループ内の各 Edge WAE にパケットをリダイレクトできます。

2. 各 Edge WAE は、自身が存在することを、ルータ リストの各ルータに通知します。ルータは、サービス グループ内の Edge WAE のビューとともに応答を返します。

3. グループ内のすべての Edge WAE の間でビューの一貫性が確保されると、1 台の Edge WAE がリード Edge WAE として指定され、パケットをリダイレクトするために WCCP 対応ルータを配置する必要があるという内容のポリシーが設定されます。

リード Edge WAE は、グループの Edge WAE にトラフィックを割り当てる方法を指定します。グループの WCCP 対応ルータがパケットをリダイレクトし、グループ内の Edge WAE がそれぞれの負荷をより適切に管理できるように、割り当て情報は指定されたリード Edge WAE からサービス グループ全体に渡されます。

WCCP は、サービス グループを使用して、グループ内の WCCP バージョン 2 対応ルータと Edge WAE 用の WAAS サービスを定義します。また、WCCP は、リアルタイムでこれらのグループへクライアント要求をリダイレクトします。

同じ WCCP サービス グループのメンバーとして設定され、リダイレクトされたトラフィックを受信するポートはすべて、次の特性を共有します。

- ポートはすべて、WAAS Central Manager GUI（「WAE 用の WCCP サービス マスクの変更」[p.4-25]）または **wccp service-number mask** グローバル設定コマンドで設定されているとおり、同じハッシュまたはマスク パラメータを持ちます。
- 個々のポートの WCCP バージョン 2 サービスを、個別に停止または開始することはできません（WCCP バージョン 2 の制限）。

WCCP バージョン 2 対応ルータで、WCCP サービス グループのサポートを有効または無効にするには、**ip wccp** グローバル設定コマンドを使用します。WCCP サービス グループのサポートを制御するためのルータの機能を削除するには、このコマンドの **no** 形式を使用します。

ip wccp {**web-cache** | *service-number*} [**group-address** *groupaddress*]

次の例は、100.10.10.1 というグループ アドレスを持つ WAE のグループ用の TCP 無差別モード サービス（WCCP バージョン 2 サービス 61 および 62）を有効にする方法を示しています。

```
Router# ip wccp 61 group-address 100.10.10.1
Router# ip wccp 62 group-address 100.10.10.1
```

オンラインになった WAE は WCCP サービス グループに加入します。新しい WAE がサービス グループに参加すると、負荷を分散するためのハッシュ テーブルが更新され、以前は WAE1 へ転送されていたトラフィックを WAE2 へ転送できます。WAE2 に、すでに接続されているクライアントのパケットを WAE1 へ転送させるには、フローの保護を有効にする必要があります。その最終結果として、単一のセッションに属する要求はすべて、同じ WAE によって処理されます。管理者がフローの保護を無効にしている場合は、WAE をサービス グループに追加したときに、一部の既存のクライアントが切断されてしまうことがあります。

WAE をサービス グループから削除すると、そのクライアントは切断されます（そのクライアントを再接続すると、別の WAE に到達するか、使用可能な場合は元のファイル サーバに到達します）。

WAAS は、Edge WAE が故障した場合にクライアントを他の Edge WAE に再接続して、WAE フェールオーバーをサポートしています。Edge WAE は、故障すると、WCCP キープアライブの発行を停止します（高い CPU 負荷が続く場合も、その結果、キープアライブが失われ、フェールオーバーを実行するケースとして見なされる場合があります）。ルータは、キープアライブの消失を検出し、サービス グループから Edge WAE を削除します。指定した Edge WAE は、Edge WAE の削除を反映して WCCP 設定ハッシュ テーブルを更新し、残っている Edge WAE の間でそのバケットを分割します。リード Edge WAE が故障すると、指定した新しいリード Edge WAE が選択されます。クライアントは切断されますが、別の Edge WAE が以後の接続を処理します。

一旦、TCP のフローが Edge WAE によって代行受信されると、障害時の動作は、非透過モードで発生する障害時の動作と同じになります。たとえば、Core WAE の障害およびファイル サーバの障害のシナリオは、WCCP 代行受信を使用した場合の障害と異なる方法で処理されるわけではありません。

ルータ上の IP アクセス リストの設定

オプションで、ルータに定義されたアクセス リストに基づいて、トラフィックを WAE からリダイレクトするようにルータを設定できます。これらのアクセス リストのことを「リダイレクト リスト」と呼びます。

（注）　また、「WAE 用の固定バイパス リストの設定」（p.4-30）の説明に従って、WAE に固定バイパス リストを設定することもできます。アクセス リストの方が効率的であるため、固定バイパス機能を使用するより、WCCP 対応ルータ上の IP アクセス リストを使用することを推奨します。また、第 8 章「WAAS デバイス用の IP アクセス コントロール リストの作成および管理」の説明に従って、WAE へのアクセスを制御するために、WAE 上でアクセス コントロール リストを設定することもできます。

ルータ上の IP アクセス リストは、最高の優先順位を持ち、WAE に定義された IP ACL や、WAE の固定バイパス リストより優先します。WAE に設定されている IP ACL は、WAE で定義されているアプリケーション定義ポリシーより優先します。この項目の詳細については、「WAE 上の IP ACL とアプリケーション定義ポリシーの優先順位について」（p.8-3）を参照してください。

WCCP バージョン 2 対応ルータには、WAE への TCP トラフィックのリダイレクションを許可または拒否するためのアクセス リストを設定できます。次の例では、ルータは、次の条件に一致するトラフィックを WAE へリダイレクトしません。

- ホスト 10.1.1.1 から発信され、任意のその他のホスト宛てである
- 任意のホストから発信され、ホスト 10.255.1.1 宛てである

```
Router(config)# ip wccp 61 redirect-list 120
Router(config)# ip wccp 62 redirect-list 120
Router(config)# access-list 120 deny ip host 10.1.1.1 any
Router(config)# access-list 120 deny ip any host 10.1.1.1
Router(config)# access-list 120 deny ip any host 10.255.1.1
Router(config)# access-list 120 deny ip host 10.255.1.1 any
Router(config)# access-list 120 permit ip any
```

明示的に許可されないトラフィックは、暗黙的にリダイレクションが拒否されます。**access-list 120 permit ip any** コマンドは、明示的にすべてのトラフィック（任意の送信元から任意の宛先宛て）の WAE へのリダイレクションを許可しています。コマンドが入力された順番で条件に照合されるため、グローバル **permit** コマンドが最後に入力するコマンドとなります。

パケットのリダイレクションをアクセス リストに一致したパケットだけに制限するには、**ip wccp redirect-list** グローバル設定コマンドを使用します。このコマンドを使用して、どのパケットを WAE へリダイレクトする必要があるかを指定します。

WCCP が有効になっていても、**ip wccp redirect-list** コマンドを使用しない場合は、WCCP サービスの条件に一致するすべてのパケットが WAE へリダイレクトされます。**ip wccp redirect-list** コマンドを指定すると、アクセス リストに一致するパケットだけがリダイレクトされます。

WCCP を使用して WAE への要求のリダイレクションを開始するために必要なコマンドは、**ip wccp** グローバル設定コマンドと **ip wccp redirect** インターフェイス設定コマンドだけです。WCCP 対応ルータのインターフェイスが、該当する発信パケットかどうかをチェックし、パケットを WAE へリダイレクトするように指定するには、**ip wccp redirect** インターフェイス設定コマンドを使用します。**ip wccp** コマンドが有効でも、**ip wccp redirect** コマンドが無効の場合、WCCP 対応ルータは WAE を認識しますが、この WAE を使用しません。

名前または番号でアクセス リストを指定するには、グループ メンバシップの基準を定義する **ip wccp group-list** グローバル設定コマンドを使用します。次の例では、**access-list 1 permit 10.10.10.1** コマンドを使用して、WCCP サービス グループへの参加を許可する WAE の IP アドレスを定義しています。

```
Router(config)# ip wccp 61 group-list 1
Router(config)# ip wccp 62 group-list 1
Router(config)# access-list 1 permit 10.10.10.1
```

アクセス リストの詳細については、Cisco IOS IP アドレッシングおよびサービス ソフトウェアのマニュアルを参照してください。

ルータ上のサービス グループ パスワードの設定

セキュリティ を目的として、WCCP バージョン 2 対応ルータとそれにアクセスする WAE に、サービス パスワードを設定できます。正しいパスワードが設定されたデバイスだけに、WCCP サービス グループへの参加が許可されます。

ルータで、WCCP 対応ルータのグローバル設定モードから次のコマンドを入力して、TCP 無差別モードサービス（WCCP バージョン 2 サービス 61 および 62）用のサービス グループ パスワードを指定します。

```
Router(config)# ip wccp 61 password [0-7] password
Router(config)# ip wccp 62 password [0-7] password
```

必須の *password* 引数は、指定したサービス グループから受信したメッセージに MD5 認証を適用するために、WCCP バージョン 2 対応ルータに転送されるストリングです。認証によって受け入れられなかったメッセージは、廃棄されます。*0* ～ *7* は、パスワードの暗号化に使用される HMAC MD5 アルゴリズムを示すオプションの値です。この値は、WAE の暗号化パスワードが作成されたときに生成されます。7 の値を推奨します。オプションの *password* 引数は、ルータと WAE 間の接続のセキュリティを確立するために、HMAC MD5 値と組み合わされるオプションのパスワード名です。

WAAS Central Manager GUI を使用して WAE（またはデバイス グループ）上のサービス グループ パスワードを指定する方法については、「WAE 用の WCCP サービスの現在の設定の変更」（p.4-20）を参照してください。

ルータ上のループバック インターフェイスの設定

WAE へのルートは、常にルータのループバック インターフェイスの IP アドレスを使用して識別されます。ループバック アドレスが存在しない場合は、ルータ上の最も使用可能な IP アドレスが使用されます。ループバック アドレスを使用しているときにインターフェイスの状態が変化すると、別の IP アドレスが使用され、再接続で問題が発生する場合があります。

次の例では、ループバック インターフェイスを設定し、設定モードを終了し、実行中の設定を起動時設定として保存しています。

```
Router(config)# interface Loopback0
Router(config-if)# ip address 111.111.111.111 255.255.255.0
Router(config-if)# no shutdown
Router(config-if)# end
Router# copy running-config startup-config
```

WAE 用の WCCP 設定の集中管理

ここでは、次の内容について説明します。

（注）　このセクションの手順を実行する前に、『*Cisco Wide Area Application Services Quick Configuration Guide*』の説明に従って、ルータと WAE 上の WCCP バージョン 2 と TCP 無差別モード サービスの基本的な設定を含む WAAS ネットワークの初期設定が完了していることを仮定しています。

負荷分散と WAE

ブランチ オフィスで WCCP 対応の複数の Edge WAE を展開して、動的なロードバランシングを実装することで、サービス グループ内の個々の Edge WAE に転送される負荷の調整を行うことができます。WCCP 対応ルータが受信した IP パケットは、Edge WAE へ転送する必要のある要求であるかどうかがチェックされて判別されます。パケット検査には、要求と定義されたサービス基準との照合が含まれます。これらのパケットは、どの Edge WAE（ある場合）がリダイレクトされたパケットを受信する必要があるかを判断するために、ルータ上の処理ルーチンへ渡されます。

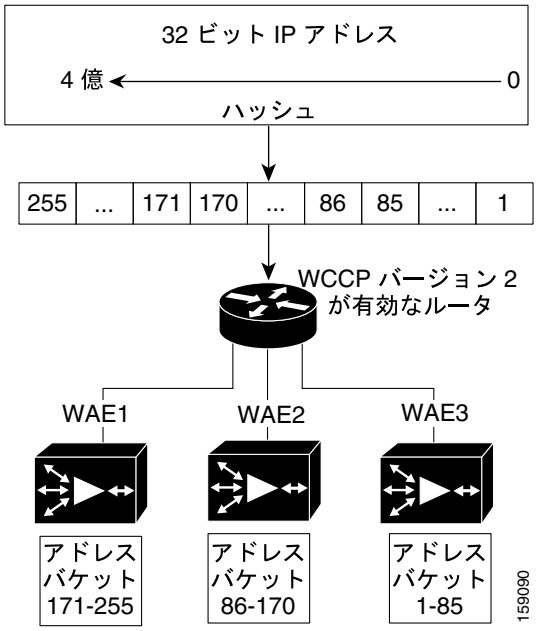
負荷分散を使用すると、複数の Edge WAE 間でトラフィックの負荷バランスを取ることができます。負荷分散を使用すると、過負荷の Edge WAE から、使用可能な容量を持つその他の Edge WAE へ負荷を移動して、Edge WAE に割り当てられている一連のハッシュ アドレス バケットを調整することができます。この技術では、2 つの割り当て方式が使用されます。それは、ハッシュとマスキングです。

「*割り当て方式*」とは、WCCP が Edge WAE 間に負荷を分散するために使用する方式を示します。2 つの負荷分散割り当て方式は、ハッシュとマスキングです。マスク負荷分散方式が指定されていない場合は、ハッシュ負荷分散方式が使用されます。これは、デフォルトの方式です。

WCCP は、ハッシュ関数に基づくリダイレクションをサポートします。ハッシュ キーは、パケットの送信元または送信先 IP アドレスをベースにすることができます。WAFS の場合、負荷分散ハッシュは、送信元 IP アドレス（デフォルト）、送信先 IP アドレス、またはその両方に基づいています。

ハッシュ関数は、送信元 IP アドレスを使用して、パケットの割り当て先となるアドレス バケットを取得します。その後、この送信元アドレス バケットは、存在する Edge WAE の数と Edge WAE の使用状況に応じて、特定の Edge WAE にマッピングされます（図 4-2 を参照）。

図 4-2　IP アドレスのハッシュによる負荷分散



（注） Edge WAE が処理しないパケットは、送信元の同じルータへ返信されます。ルータは、正式にリダイレクトされたパケットを受信した場合に、それを再度リダイレクトする必要がないことを認識します。

送信先 IP アドレス ハッシュは、1 つの Edge WAE が 1 つの特定のファイル サーバだけをキャッシュするように保証します。この方式により、ローカル一貫性ディレクティブをファイル サーバの内容に安全に適用できるため（内容に他の共同作業が行われていない場合）、パフォーマンス、WAN リンク、およびディスクの使用率が向上します。ただし、ファイル サーバ上のアクティビティは一様でないため、この方式では、負荷が不均等に分散されることがあります。

送信元 IP アドレスのハッシュの方が、Edge WAE 上のキャッシュ間のセッション分散に適しています。この方式は、パフォーマンス、WAN リンク、およびディスク利用率に影響する場合があります（負荷分散を適用するときに考慮する必要がある要因については、前の説明を参照してください）。また、クライアントの IP アドレスが変更されると（DHCP 環境で動作中に発生する場合がある）、クライアントが別の Edge WAE に切り替えることがあります。これにより、クライアントのワーキング セットが新しいキャッシュに取り込まれるまで、クライアントのパフォーマンスが低下することがあります。

クライアント IP アドレスに基づくハッシュは、ハッシュ キーの局所性を一切保証しません。たとえば、同じサブネットのクライアント（同じ内容を共有し、同じ内容に対して共同作業している可能性がある）に、2 つの異なるハッシュ番号が割り当てられ、それによってそれぞれ異なる Edge WAE にリダイレクトされる場合もあれば、異なるサブネットのクライアントに同じハッシュ番号が割り当てられ、同じ Edge WAE にリダイレクトされる場合もあります。クライアント IP アドレスに基づくハッシュは、一貫性を保証します。たとえば、同じ IP アドレスを使用しているクライアントは、同じ Edge WAE にリダイレクトされます。

サービス集合の中で、使用できる Edge WAE の間で負荷を分散するハッシュ テーブルを作成するために、リード Edge WAE が選択されます。リード Edge WAE は、均等にバケットを分散します。送信元 IP アドレスがハッシュされ、その結果割り当てられたバケットにしたがい、パケットを処理する Edge WAE が決定されます（フローの保護が、セッション全体を通じて同じ Edge WAE が使用されるように保証します）。

WCCP は、マスク値割り当てによるリダイレクションをサポートします。この方式は、マスキングに依存して、リダイレクションに関する決定を下します。決定は、WCCP 対応ルータの特殊なハードウェア サポート機能を使用して実行されます。この方式は、ハードウェアがパケットを交換するため、非常に効率的です。

（注）　マスキング方式は、Catalyst 6500 シリーズ スイッチや Cisco 7600 シリーズ ルータとの負荷分散だけに使用できます。

マスキングは、明示的に指定する必要があります。パケットの送信先または送信元の IP アドレスに基づいた 2 つのマスキングの値を指定できます。WAAS の場合、デフォルトのマスク値は、送信先 IP アドレスに基づいています。デフォルト値を使用するか、特定のマスク値を指定することで、マスクを有効にすることができます。デフォルトのマスク値（16 進数表記）は、次のとおりです。

- dst-ip-mask= 0x0
- src-ip-mask= 0x1741

最大 7 ビットのマスク値が指定できます。Edge WAE は、2^7（128）通りの組み合わせのテーブルを作成し、Edge WAE の IP アドレスをその組み合わせに割り当て、このテーブルを WCCP 対応ルータに送信します。ルータは、このテーブルを使用して、サービス グループ内のすべての Edge WAE にトラフィックを分散します。WCCP サービス パラメータと一致する各パケットがこのテーブルと比較され、対応する Edge WAE へ送信されます。

パケット転送方式

WCCP 対応ルータは、次の 2 つのパケット転送方式のいずれかを使用して、代行受信した TCP セグメントを WAE へリダイレクションします。

- Generic Routing Encapsulation（GRE; 総称ルーティング カプセル化）— WAE へのパスに多数のルータが存在する場合でも、パケットはその WAE に到達できます。
- レイヤ 2 リダイレクション — パケットは、レイヤ 2（MAC 層）で交換され、WAE に到達できます。

表 4-2 で、パケット転送方式について説明します。

表 4-2　パケット転送方式

パケット転送方式	負荷分散方式：ハッシュ	負荷分散方式：マスキング
GRE（レイヤ 3）	パケット リダイレクションは、ルータ ソフトウェアによって完全に処理されます。	パケット リダイレクションは、ルータ ソフトウェアによって完全に処理されます。パケット転送方式として GRE が使用されている場合に、マスク割り当てを使用することは推奨しません。
レイヤ 2 リダイレクション	最初にリダイレクトされたパケットは、ルータ ソフトウェアによって処理されます。それ以降にリダイレクトされたパケットはすべて、ルータ ハードウェアによって処理されます。	すべてのパケットが、ルータ ハードウェアによって処理されます（特殊なハードウェアが必要となるため、現時点では、Catalyst 6500 シリーズ スイッチまたは Cisco 7600 シリーズ ルータでのみサポートされています）。

リダイレクション モードは、Edge WAE によって制御されます。WCCP サービス グループに最初に加入した Edge WAE が、転送方式（GRE またはレイヤ 2 リダイレクション）と割り当て方式（ハッシュまたはマスキング）を決定します。「*マスク割り当て*」という用語は、WCCP レイヤ 2 Policy Feature Card 2（PFC2; ポリシー フィーチャ カード 2）入力リダイレクションを指しています。

WCCP 出力リダイレクションにおいてマスキングを選択すると、Edge WAE は、Multilayer Switch Feature Card（MSFC; マルチレイヤ スイッチ フィーチャ カード）および Policy Feature Card（PFC; ポリシー フィーチャ カード）で使用されているオリジナルのハードウェア アクセラレーションに戻ります。

たとえば、WCCP はパケットをフィルタして、リダイレクトされたパケットのうち、どれが Edge WAE から戻されたパケットか、どれが戻されたパケットではないかを判別します。Edge WAE がパケットを処理する必要がないと判断したため、WCCP は戻されたパケットをリダイレクトしません。WCCP バージョン 2 は、Edge WAE が処理しないパケットを、送信元のルータへ返信します。

ここでは、次の内容について説明します。

- パケットの拒否と返信の理由（p.4-15）
- パケット転送方式としてのレイヤ 3 GRE（p.4-16）
- パケット転送方式としてのレイヤ 2 リダイレクション（p.4-17）

パケットの拒否と返信の理由

Edge WAE は次の理由により、パケットを拒否して返信します。

- パケット処理が逆効果となるような特定の状況、たとえば、IP 認証がオンになっている場合などを、Edge WAE が除外しているため。
- Edge WAE によってキャッシュするように設定されていないサーバ宛ての CIFS パケットを、Edge WAE が受信したため。
- Edge WAE に固定バイパス リストが設定されているため。

（注）　パケットは、WCCP 対応ルータと Edge WAE との間の接続の送信元にリダイレクトされます。使用されている Cisco IOS ソフトウェアのバージョンによって、この送信元は発信インターフェイスの場合もあれば、ルータ IP アドレスの場合もあります。後者の場合は、Edge WAE のルータ リストに WCCP 対応ルータの IP アドレスが格納されていなければなりません。ルータ リストの詳細につ

いては、「WAE 用の WCCP ルータ リストの設定の変更」（p.4-26）を参照してください。

Cisco Express Forwarding（CEF）は不要ですが、パフォーマンスを改善するために推奨します。ルータで CEF が有効になっている場合、WCCP は IP CEF を使用できます。また、WCCP を使用して、複数のルータ（ルータ リスト）が特定の WCCP サービス（たとえば、CIFS リダイレクション）をサポートするように設定することができます。

パケット転送方式としてのレイヤ 3 GRE

WCCP 対応ルータは、代行受信した要求を GRE を使用してパケットをカプセル化することができます。このパケット転送方式では、WAE へのパスに複数のルータが存在する場合でも、パケットはその WAE に到達できます。パケット リダイレクションは、ルータ ソフトウェアによって完全に処理されます。

GRE は、WCCP 対応ルータでデータグラムを IP パケットにカプセル化し、その後 WAE にリダイレクトします（トランスペアレント プロキシ サーバ）。この中間の宛先で、データグラムはカプセル化が解除され、その後、WAAS ソフトウェアによって処理されます。要求をローカルに処理できない場合は、関連する WAE が元のサーバに接触して要求を完了できます。その場合、内部データグラムから見て、元のサーバへのトリップ分は 1 ホップと見なされます。通常、GRE を使用してリダイレクトされたトラフィックは、GRE トンネル トラフィックと呼ばれます。GRE を使用した場合、リダイレクションはすべて、ルータ ソフトウェアによって処理されます。

WCCP リダイレクションを使用する場合、ルータの接続の宛先ポート上の WCCP は有効になっているため、Cisco ルータは TCP SYN パケットを宛先へ転送しません。その代わり、WCCP 対応ルータが GRE トンネリングを使用してパケットをカプセル化し、この WCCP 対応ルータからリダイレクトされたパケットを受け入れるように設定された WAE へそのパケットを送信します。

リダイレクトされたパケットを受信すると、WAE は次のように処理します。

1. パケットから GRE レイヤを取り除きます。
2. 次のように、リダイレクトされたこのパケットを受け付けて内容の要求を処理するか、リダイレクトされたパケットを拒否するかを決定します。
   a. WAE は、要求を受け入れる必要があると判断した場合は、TCP SYN ACK パケットをクライアントへ送信します。WAE は、WAE がクライアントに見えない（透過的）ように、この応答パケットの中で送信元アドレスとして指定された元の送信先（元のサーバ）の IP アドレスを使用します。WAE は、クライアントからの TCP SYN パケットの送信先であるかのように動作します。
   b. WAE は、要求を受け入れる必要がないと判断した場合は、GRE を使用して TCP SYN パケットを再度カプセル化し、WCCP 対応ルータへ返します。ルータは、WAE がこの接続に関与していないことを認識し、パケットを元の送信先（つまり、元のサーバ）へ転送します。

パケット転送方式としてのレイヤ 2 リダイレクション

レイヤ 2 リダイレクションは、WCCP 対応ルータまたはスイッチが、WCCP トラフィック代行受信およびリダイレクション機能をレイヤ 2 で部分的または完全に実装している内部スイッチング ハードウェアを利用している場合に実現されます。現在このタイプのリダイレクションがサポートされているのは、Catalyst 6500 シリーズ スイッチおよび Cisco 7200 および 7600 シリーズ ルータのみです。レイヤ 2 リダイレクションでは、最初にリダイレクトされたトラフィック パケットがルータ ソフトウェアによって処理されます。それ以降のトラフィックは、ルータ ハードウェアによって処理されます。Edge WAE は、ルータまたはスイッチに、特定のパケット フィールドにビット マスクを適用し、その後、マスク インデックス アドレス テーブルの形式で、マスクの結果またはインデックスをサービス グループ内の Edge WAE にマッピングするように指示します。リダイレクション プロセスは、スイッチング ハードウェアによって加速化されるため、レイヤ 2 リダイレクションの方がレイヤ 3 GRE に比べ効率的です。

（注）　WCCP は、WAE 上でのみ使用が許可されており、リダイレクト ルータでの使用は許可されていません。WCCP が、ルータやスイッチの正常な動作を妨げることはありません。

WAE での WCCP フロー リダイレクション

フローの保護は、Edge WAE がサービス グループに対して追加および削除されたときに、既存のクライアント TCP 接続に及ぼす影響を削減します。デフォルトでは、WCCP フロー リダイレクションは WAE で有効になっています。フローの保護は、Edge WAE がサービス グループに対して追加および削除されたときに、既存のクライアント TCP 接続に及ぼす影響を削減します。フローの保護によってクライアントへの影響を削減できるのは、次のような状況の場合です。

- WAAS ネットワークの拡張 — Edge WAE がサービス グループに追加されると、以前に別の Edge WAE が処理していたトラフィックを、新たに起動した Edge WAE が受信します。さらに、そのトラフィックは、継続して処理するために、関連する Edge WAE へ転送されます。新しい接続は、新しい Edge WAE によって処理されます。
- Edge WAE の交換後の障害 — Edge WAE で障害が発生すると、以前はその Edge WAE または元のファイル サーバが処理していたトラフィックを、別の Edge WAE が受信できます。受信側の Edge WAE は、それ以前の 2 通りの使用例にしたがって動作します。

フローの保護を使用していない場合、上記の状況では、確立済みのクライアント接続は TCP RESET によって切断されます。フローの保護は、サポートされる WCCP サービスすべてに適用され、サービス単位で設定することはできません。

WAE 上の一般的な WCCP 設定の表示と変更

WAAS ネットワークでは、WAE 用の設定パラメータのことを「WCCP 一般設定」と総称します。

- WCCP version
- Flow redirection
- Shutdown delay

表 4-3 に、WAE 上の WCCP 一般設定のデフォルト値を示します。

表 4-3　WAE 上の WCCP 一般設定のデフォルト値

機能	デフォルト値	説明
WCCP Version 2	Disabled	WAAS でサポートされるのは WCCP バージョン 2 のみです。
Flow redirection	Enabled	TCP フローを維持し、WAE が起動し、新しいトラフィックを割り当てられたときに過剰な負荷がかかることを防止します。
Shutdown delay	120 秒	TCP 接続の切断を防止するために、WAE は、WAE でリロードまたは WCCP が停止した（無効になった）あとで、WCCP の正常なシャットダウンを実行します。

一貫性を保証するため、個々のデバイスでなく、デバイス グループ単位で WCCP 一般設定を変更することを推奨します。

（注） このセクションの手順を実行する前に、『*Cisco Wide Area Application Services Quick Configuration Guide*』の説明に従って、TCP 無差別モード サービス（WCCP バージョン 2 サービス 61 および 62）の設定を含む WAAS ネットワーク用の基本的な WCCP 設定はすでに完了しているものとします。

WAE（または WAE のグループ）用の一般的な WCCP 設定を集中的に表示または変更するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI から、**[Devices] > [Devices]**（または **[Devices] > [Device Groups]**）を選択します。

ステップ 2　WCCP 一般設定の値を変更したいデバイス（またはデバイス グループ）の名前の横にある **[Edit]** アイコンをクリックします。

ステップ 3　[Contents] ペインで、**[Interception] > [WCCP] > [General Settings]** を選択します。[WCCP General Configuration Settings] ウィンドウが表示されます。

ステップ 4　選択したデバイス（またはデバイス グループ）の現在の設定を確認します。

- 現在の設定を保持し、ウィンドウを閉じるには、**[Cancel]** をクリックします。
- 現在の設定を変更するには、この手順の残りの説明に従って現在の設定を変更します。

デフォルトで、WAE 上の WCCP は無効になっています。ただし、WAAS ネットワークでの WCCP の初期設定の一環として、WAE（Edge WAE と Core WAE）とこれらの要求を透過的に WAE へリダイレクトするデータセンターとブランチ オフィスのルータで、WCCP バージョン 2 が有効になっている必要があります。WAAS ネットワークで基本的な WCCP 設定を実行する手順については、『*Cisco Wide Area Application Services Quick Configuration Guide*』を参照してください。

ステップ 5　[WCCP Version] ドロップダウン リストから **[2]** を選択して、選択したデバイス（またはデバイス グループ）の WCCP バージョン 2 を有効にします。あるいは、**[Disabled]** を選択して、選択したデバイス（またはデバイス グループ）の WCCP を無効にします。

（注）　WCCP バージョン 1 は Web トラフィック（ポート 80）しかサポートしていないため、選択したデバイス（またはデバイス グループ）が WCCP バージョン 1 の代わりに WCCP バージョン 2 を使用するように設定する必要があります。

WCCP 環境で使用しているルータで、WCCP バージョン 2 をサポートするバージョンの Cisco IOS ソフトウェアが稼働していることを確認します。

ステップ 6　TCP フローを維持し、デバイス（またはデバイス グループ）が起動したときや新しいトラフィックが再割り当てされる際に過剰な負荷がかかるのを防止するには、**[Enable Flow Redirection]** チェック ボックスを選択します。詳細については、「WAE での WCCP フロー リダイレクション」（p.4-17）を参照してください。

ステップ 7　[Shutdown Delay] フィールドで、選択したデバイス（またはデバイス グループ）が WCCP の正常なシャットダウンを実行するのを待つ最大時間（秒）を指定します。デフォルトは 120 秒です。

WAE は、すべての接続が処理されるか、（この [Shutdown Delay] フィールドで指定した）WCCP バージョン 2 用の最大待ち時間が経過するまで再起動しません。

ステップ 8　**「Submit」**をクリックして、変更を保存します。

CLI から WCCP 設定を構成するには、**wccp version**、**wccp flow-redirect**、および **wccp shutdown** グローバル設定コマンド使用できます。

WAE 上の WCCP バージョン 2 の正常なシャットダウンの詳細については、「WCCP の正常なシャットダウンのための WAE の設定」（p.4-29）を参照してください。

WAE 用に現在設定されている WCCP サービスのリストの表示

WAE（または WAE のグループ）用に現在設定されている WCCP サービスのリストを集中的に表示するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI から、**[Devices] > [Devices]**（または **[Devices] > [Device Groups]**）を選択します。

WAAS ネットワークに設定されているすべてのデバイス タイプを表示する [Devices] ウィンドウが表示されます。

ステップ 2　現在設定されている WCCP サービスのリストを表示したいデバイス（またはデバイス グループ）の横にある **[Edit]** アイコンをクリックします。

ステップ 3　[Contents] ペインで、**[Interception] > [WCCP] > [Services]** を選択します。

選択したデバイス（またはデバイス グループ）用に現在設定されている WCCP サービスのリストを表示する [WCCP Service Settings for WAE] ウィンドウが表示されます。

ステップ 4　既存の WCCP サービスを変更するために変更したいサービスの横にある **[Edit WCCP Service Setting]** アイコンをクリックします。

サービスを変更する詳細については、「WAE 用の WCCP サービスの現在の設定の変更」（p.4-20）を参照してください。

ステップ 5　タスクバーの **[Create New WCCP Service Setting]** アイコンをクリックして、選択したデバイス（またはデバイス グループ）用の新しい WCCP サービスを作成します。

CLI から現在設定されている WCCP サービスを表示するには、**show wccp services** EXEC コマンドを使用できます。

WAE 用の WCCP サービスの現在の設定の変更

WAE（または WAE のグループ）用の WCCP サービスの現在の設定を集中的に変更するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI から、**[Devices] > [Devices]**（または **[Devices] > [Device Groups]**）を選択します。

ステップ 2　WCCP 設定またはサービスを変更したいデバイス（またはデバイス グループ）の名前の横にある **[Edit]** アイコンをクリックします。

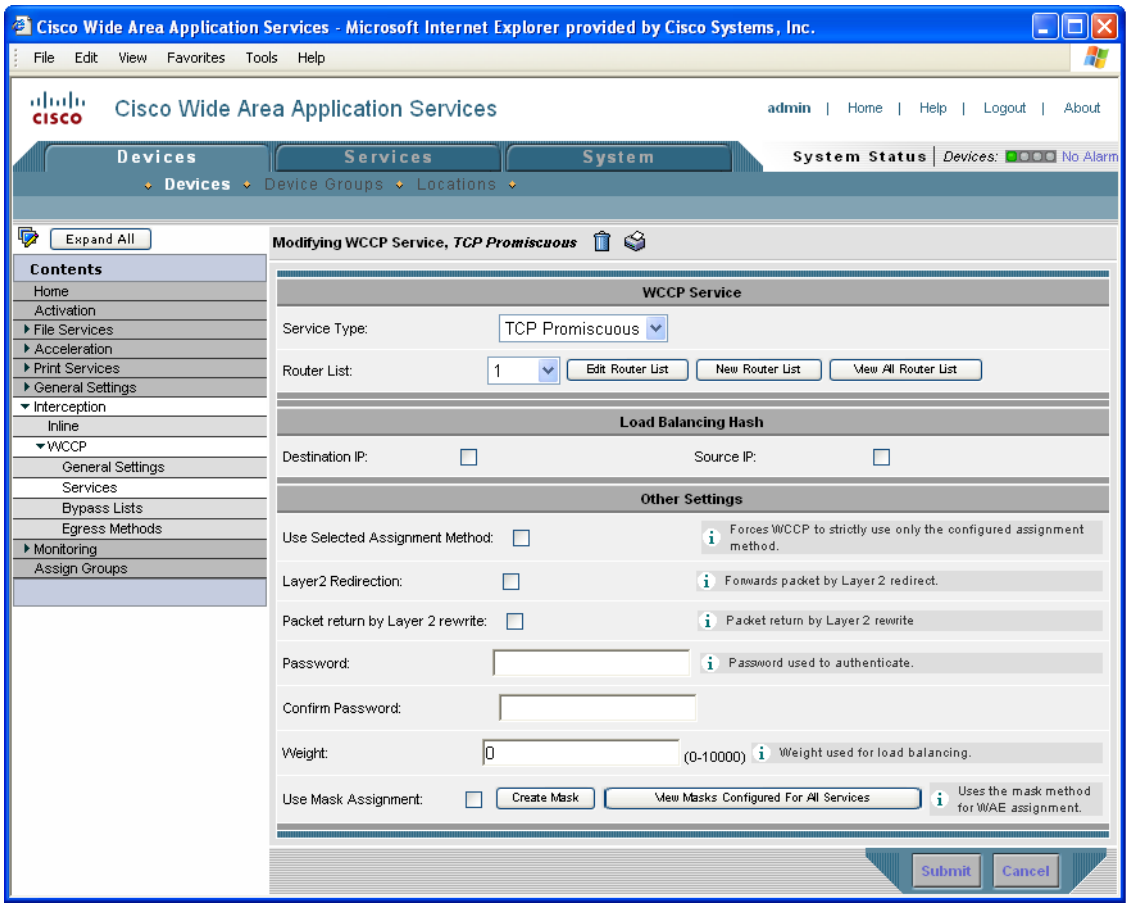
ステップ 3　[Contents] ペインで、**[Interception] > [WCCP] > [Services]** を選択します。

選択したデバイス（またはデバイス グループ）用に現在設定されている WCCP サービスのリストを表示する [WCCP Service Settings] ウィンドウが表示されます。

ステップ 4　変更したいサービスの横にある **[Edit WCCP Service Setting]** アイコンをクリックします。

[Modifying WCCP Service] ウィンドウが表示されます（図 4-3 を参照してください）。

図 4-3　WCCP サービスの設定の変更



（注）　サービスがルータ リストと関連付けられたあとのみ、WCCP シリーズに対するすべての設定を行うことができます。

ステップ 5　[Router List] ドロップダウン リストから適切な WCCP ルータ リスト番号を選択して、TCP 無差別モード サービスにルータ リストを関連付けます。

ドロップダウン リストには、設定済みの WCCP ルータ リストだけが表示されます。WAAS ネットワークの初期設定の一環として、『*Cisco Wide Area Application Services Quick Configuration Guide*』の説明に従って、Edge WAE 用の少なくとも 1 つの WCCP ルータ リストと Core WAE 用の 2 番めのルータ リストがすでに作成されている場合があります。WCCP ルータの詳細については、次の項を参照してください。

- WAE 用の WCCP ルータ リストの設定の変更（p.4-26）
- WAE からの WCCP ルータ リストの削除（p.4-27）
- WAE での追加 WCCP ルータ リストの定義（p.4-27）

ステップ 6　（任意）次のように、選択した WCCP サービス用の現在の負荷分散設定を変更します。

a. 送信先 IP アドレスの負荷分散ハッシュを定義するには、**[Destination IP]** チェック ボックスを選択します。

b. 送信元 IP アドレスの負荷分散ハッシュを定義するには、**[Source IP]** チェック ボックスを選択します。

（注）　負荷分散の詳細については、「負荷分散と WAE」（p.4-12）を参照してください。

ステップ 7　（任意）次のように、選択した WCCP サービス用の現在の他の設定を変更します。

a. 設定した割り当て方式だけを使用するように WCCP に強制するには、**[Use Selected Assignment Method]** チェック ボックスを選択します。選択後は、次の 2 つの負荷分散方式のいずれかを使用します。

- ハッシュ割り当て — Catalyst 6500 シリーズ スイッチと Cisco 7600 シリーズ ルータの場合、この負荷分散方式は、WCCP レイヤ 2 PFC リダイレクションと呼ばれます。この方式は、Supervisor Engine 1A と MSFC 2 を使用して、最大 3 Gbps の転送パフォーマンスを実現することを目的としています。
- マスク割り当て — この負荷分散方式は、WCCP レイヤ 2 PFC2 リダイレクションと呼ばれます。Supervisor Engine 2 と MSFC2 の組み合わせを使用します。

Edge WAE グループ内の WCCP サービスごとにどちらか一方の負荷分散方式（ハッシュまたはマスキング）を指定できます。負荷分散割り当て方式の詳細については、「負荷分散と WAE」（p.4-12）を参照してください。

b. WAE がデバイスとのレイヤ 2 接続を確立し、デバイスがレイヤ 2 リダイレクション用に設定されている場合に、WAE（またはデバイス グループ）が WCCP バージョン 2 スイッチまたはルータから透過的にリダイレクションされたトラフィックを受信できるようにするには、**[Layer2 Redirection]** チェック ボックスを選択します。

ルータやスイッチ上の WCCP は、部分的または全体的に WCCP のトラフィック代行受信とリダイレクション機能をハードウェアのレイヤ 2 で実装するハードウェアのスイッチを利用できます。WAE が Cisco スイッチ互換機と正しく接続されていれば、レイヤ 2 または MAC アドレス リライト リダイレクションが実行されます。リダイレクション処理は、スイッチング ハードウェアによって加速化されるため、この方式の方が、GRE を使用したレイヤ 3 リダイレクションより効率的です。WAE は、ルータまたはスイッチとのレイヤ 2 接続を保持している必要があります。スイッチと WAE 間の GRE トンネルは必須ではないため、スイッチは **[Layer2 Redirection]** チェック ボックスを選択して、カプセル化されたパケットを転送するカットスルー方式を使用できます。詳細については、「パケット転送方式」（p.4-14）を参照してください。

c. パケット返信にレイヤ 2 更新を使用できるようにするには、**[Packet return by Layer 2 rewrite]** チェック ボックスを選択します。

d. [Password] フィールドで、クラスタ内の WAE と指定したサービス用のルータ間の安全なトラフィックに使用するパスワードを指定します。クラスタ内の他のすべての WAE とルータを同じパスワードで有効にします。パスワードの長さは、8 文字以内です。[Confirm Password] フィールドに、パスワードを再入力します。

（注）　CLI を使用してルータ上のサービス グループのパスワードを指定する方法については、「ルータ上のサービス グループ パスワードの設定」（p.4-11）を参照してください。

e. [Weight] フィールドで、負荷分散に使用される重み値を指定します。重み値の範囲は 0 ～ 10000 です。サービス グループの WAE のすべての重み値の合計が 100 以下の場合、重みの値は、合計の負荷分散の目的でデバイスにリダイレクトされた負荷のそのままのパーセントを表します。たとえば、10 の重みの WAE は、すべての重み値の合計が 50 のサービス グループですべての負荷の 10% を受け取ります。そのようなサービス グループで WAE に障害が発生した場合、別の WAE は障害前と同じ負荷パーセントを受信し続け、失敗した WAE に割り当てられた負荷を受信しません。

サービス グループで WAE のすべての重み値の合計が 101 ～ 10000 の間である場合、重み値は、サービス グループでのアクティブな WAE すべての合計の重み付けの割合として扱われます。たとえば、200 の重みの WAE は、すべての重み値の合計が 800 のサービス グループですべての負荷の 25 パーセントを受け取ります。そのようなサービス グループで WAE に障害が発生した場合、別の WAE は障害が発生した WAE に割り当てられていた負荷を受け取ります。障害の処理は、重みの合計が 100 以下の場合と異なります。

デフォルトで、重みは割り当てられず、トラフィックの負荷はサービス グループ内の WAE の間で均等に分散されます。

f. WAE 割り当て用のマスク方式を使用するには、**[Use Mask Assignment]** チェック ボックスを選択します。

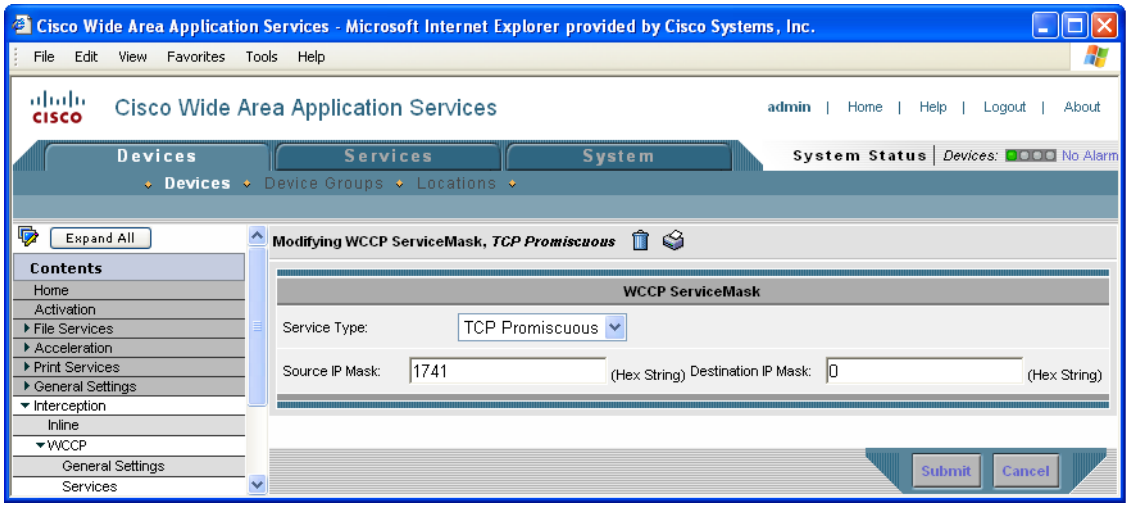
ステップ 8　（任意）選択した WCCP サービス用の既存のサービス マスクを変更するには、**[Edit Mask]** ボタンをクリックします。サービス マスクを変更する詳細については、「WAE 用の WCCP サービス マスクの変更」（p.4-25）を参照してください。

ステップ 9　（任意）選択したサービス用に設定されているすべての WCCP サービス マスクのリストを表示するには、**[View Masks Configured for All Services]** ボタンをクリックします。[WCCP Service Mask Settings] ウィンドウが表示されます

ステップ 10　[WCCP Service Mask Settings] ウィンドウから、次の作業を実行できます。

- WCCP サービス マスクを編集するには、変更したいサービス マスクの横にある **[Edit WCCP Service Mask]** アイコンをクリックします。[Modifying WCCP Service Mask] ウィンドウが表示されます（図 4-4 を参照）。

図 4-4　WCCP サービス マスクの変更



次のように、変更したい設定の値を変更し、**[Submit]** をクリックします。

- [Source IP Mask] フィールドで、パケットの送信元 IP アドレスと照合するために使用する IP アドレス マスク（16 進数）を指定します（たとえば、0xFE000000）。範囲は、0x00000000 ～ 0xFE000000 です。デフォルトは、0x00001741 です。
- [Destination IP Mask] フィールドで、パケットの送信先 IP アドレスと照合するために使用する IP アドレス マスク（16 進数）を指定します（たとえば、0xFE000000）。範囲は、0x0000000 ～ 0XFE000000 です。デフォルトは、0x00000000 です。

（注） [Modifying WCCP Service] ウィンドウの **[Edit Mask]** ボタンをクリックして、サービス マスクを編集することもできます（図 4-3 を参照）。

- 既存の WCCP サービス マスクを削除するには、削除したいサービス マスクの横にある **[Edit WCCP Service Mask]** アイコンをクリックします。[Modifying WCCP Service Mask] ウィンドウが表示されます（図 4-4 を参照）。タスクバーの **[Delete WCCP Service Mask]** アイコンをクリックし、**[Submit]** をクリックします。

CLI から WCCP service を設定するには、**wccp tcp-promiscuous** グローバル設定コマンドを使用します。

既存の WCCP サービス用の WCCP サービス マスクの作成

WAE（または WAE のグループ）用の既存の WCCP サービス用のサービス マスクを集中的に作成するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI から、**[Devices] > [Devices]**（または **[Devices] > [Device Groups]**）を選択します。

ステップ 2　WCCP サービス マスクを作成したいデバイス（またはデバイスのグループ）の横にある **[Edit]** アイコンをクリックします。

ステップ 3　[Contents] ペインで、**[Interception] > [WCCP] > [Services]** を選択します。

[WCCP Service Settings for WAE] ウィンドウが表示されます。

ステップ 4　タスクバーの **[Create New WCCP Service Setting]** アイコンをクリックします。

[Creating New WCCP Service] ウィンドウが表示されます。

ステップ 5　**[Create New Mask]** ボタンをクリックします。

[Creating New WCCP Service Mask] ウィンドウが表示されます。

最大 16 個の WCCP サービス マスクを設定できます。ビット マスクは、16 進数で指定します。指定するすべてのビット マスク合計で、セットできるビット数は 7 ビット以内です。たとえば、3 個のマスクを正しく使用するには、0xF（4 ビット）、0x1（1 ビット）、および 0x3（2 ビット）のように合計 7 ビットにします。この場合、0x0 以外の追加マスクは設定できません。0x0 以外の追加マスクを設定すると、エラー メッセージが表示されます。たとえば、4 個のマスクを使用するには、0xA（2 ビット）、0x7（3 ビット）、0x8（1 ビット）、0x1（1 ビット）のように、合計 7 ビットにします。

ステップ 6　**[Submit]** をクリックして、WCCP サービス マスク用の設定を保存します。

WAE 用の WCCP サービス マスクの変更

WAE（または WAE のグループ）用に設定されている WCCP サービス用のサービス マスクを集中的に変更するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI から、**[Devices] > [Devices]**（または **[Devices] > [Device Groups]**）を選択します。

ステップ 2　WCCP サービス マスクを変更したいデバイス（またはデバイスのグループ）の横にある **[Edit]** アイコンをクリックします。

ステップ 3　[Contents] ペインで、**[Interception] > [WCCP] > [Services]** を選択します。

[WCCP Service Settings for WAE] ウィンドウが表示されます。

ステップ 4　タスクバーの **[Create New WCCP Service Setting]** アイコンをクリックします。

[Creating New WCCP Service] ウィンドウが表示されます。

ステップ 5　**[Edit Mask]** ボタンをクリックします。

[Modifying WCCP Service Mask] ウィンドウが表示されます

ステップ 6　[Source IP Mask] フィールドで、パケットの送信元 IP アドレスと照合するために使用する IP アドレス マスク（16 進数）を指定します（たとえば、0xFE000000）。範囲は、0x00000000 ～ 0xFE000000 です。デフォルトは、0x00001741 です。

ステップ 7　[Destination IP Mask] フィールドで、パケットの送信先 IP アドレスと照合するために使用する IP アドレス マスク（16 進数）を指定します（たとえば、0xFE000000）。範囲は、0x0000000 ～ 0XFE000000 です。デフォルトは、0x00000000 です。

ステップ 8　**[Submit]** をクリックして、WCCP サービス マスク用の新しい設定を保存します。

WAE 用の WCCP ルータ リスト設定の表示

WAE（または WAE のグループ）用に現在定義されている WCCP ルータ リストのリストを集中的に表示するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI から、**[Devices] > [Devices]**（または **[Devices] > [Device Groups]**）を選択します。

ステップ 2　WCCP ルータ リストを表示したいデバイス（またはデバイス グループ）の名前の横にある **[Edit]** アイコンをクリックします。

ステップ 3　[Contents] ペインで、**[Interception] > [WCCP] > [Services]** を選択します。[WCCP Service Settings] ウィンドウが表示されます。

ステップ 4　表示される任意の WCCP サービスの横にある **[Edit]** アイコンをクリックします。[Modifying WCCP Service] ウィンドウが表示されます。

ステップ 5　**[View All Router List]** ボタンをクリックします。

選択したデバイス（またはデバイス グループ）用の [WCCP Router List Configurations] ウィンドウが表示されます。

WCCP ルータ リストの設定（各ルータ リストに入っている各ルータのルータ リストの番号と IP アドレス）が表示されます。

（注）　特定の WCCP ルータ リストの設定を変更するには、ルータ リストの横にある **[Edit]** アイコンをクリックし、表示される [Modifying Router List] を使用して、選択したルータ リストを変更します。ルータ リストを変更する詳細については、「WAE 用の WCCP ルータ リストの設定の変更」（p.4-26）を参照してください。WAE（または WAE のグループ）から WCCP ルータ リストを削除する方法については、「WAE からの WCCP ルータ リストの削除」（p.4-27）を参照してください。

CLI からルータ リストを表示するには、**show wccp routers** EXEC コマンドを使用できます。

WAE 用の WCCP ルータ リストの設定の変更

WAE（または WAE のグループ）用の WCCP ルータ リストの設定を集中的に変更する（たとえば、ルータ リストにルータを追加または削除する）には、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI から、**[Devices] > [Devices]**（または **[Devices] > [Device Groups]**）を選択します。

ステップ 2　ルータ リストの設定を変更したいデバイス（またはデバイス グループ）の名前の横にある **[Edit]** アイコンをクリックします。

ステップ 3　[Contents] ペインで、**[Interception] > [WCCP] > [Services]** を選択します。

[WCCP Service Settings] ウィンドウが表示されます。

ステップ 4　変更したいルータ リストを使用するように現在設定されている WCCP サービスの横にある **[Edit]** アイコンをクリックします。[Modifying WCCP Service] ウィンドウが表示されます。

ステップ 5　**[Edit Router List]** ボタンをクリックします。[Modifying WCCP Router List] ウィンドウが表示されます。

ステップ 6　選択したルータ リストにルータを追加するには、[Add Router] フィールドにルータの IP アドレスを入力し、**[Add Router]** ボタンをクリックします。

ステップ 7　選択したルータ リストからルータを削除するには、削除するルータの IP アドレスの横にあるチェックボックスを選択し、**[Remove Router]** ボタンをクリックします。

ステップ 8　**[Submit]** をクリックして、設定を保存します。

WAE からの WCCP ルータ リストの削除

ルータ リストを削除すると、このルータ リストを使用するように設定されていた WCCP バージョン 2 サービスも削除されます。設定されているルータ リストを削除する前に、WCCP サービスが別のルータ リストに関連付けられていることを確認してください。

WAE（または WAE のグループ）用の WCCP ルータ リストを集中的に削除する（たとえば、ルータ リストにルータを追加または削除する）には、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI から、**[Devices] > [Devices]**（または **[Devices] > [Device Groups]**）を選択します。

ステップ 2　WCCP ルータ リストを削除したいデバイス（またはデバイス グループ）の名前の横にある **[Edit]** アイコンをクリックします。

ステップ 3　[Contents] ペインで、**[Interception] > [WCCP] > [Services]** を選択します。[WCCP Service Settings] ウィンドウが表示されます。

ステップ 4　**[Edit Router List]** ボタンをクリックします。[Modifying WCCP Router List] ウィンドウが表示されます。

ステップ 5　ルータの IP アドレスの横にあるチェック ボックスを選択し、**[Remove Router]** ボタンをクリックして、選択したルータ リストから表示されているすべてのルータを削除します。

ステップ 6　選択したルータ リスト（たとえば、ルータ リスト 2）からすべてのルータを削除したら、タスクバーの **[Delete Router List]** アイコンをクリックします

ルータ リスト設定を永久に削除するかどうかを確認するダイアログボックスが表示されます。操作を確認するには、**[OK]** をクリックします。選択したデバイス（またはデバイス グループ）から、選択したルータ リストとそれに関連する WCCP サービスが削除されます。

WAE での追加 WCCP ルータ リストの定義

WAE の WCCP サービスの設定の一部として、WAE に対して TCP 無差別サービスをサポートする WCCP バージョン 2 が有効なルータのリストを作成する必要があります。WAAS CLI（**wccp router-list** グローバル設定コマンド）または WAAS Central Manager GUI を使用して、WCCP ルータ リストを定義できます。

一般に、WAAS 管理者は、『*Cisco Wide Area Application Services Quick Configuration Guide*』の説明に従って、WAAS CLI を使用して WCCP ルータ リストの初期集合を定義します。WAAS CLI を使用して WCCP ルータ リストの初期設定を完了したら、WAAS Central Manager GUI を使用して、WAE 用の WCCP ルータ リスト設定を集中的に管理し、変更することを推奨します。

（注）　このセクションの手順を実行する前に、『*Cisco Wide Area Application Services Quick Configuration Guide*』の説明に従って、TCP 無差別モード サービス（WCCP バージョン 2 サービス 61 および 62）の設定を含む WAAS ネットワーク用の基本的な WCCP の設定はすでに完了しているものとします。

WAE（または WAE のグループ）用の追加 WCCP ルータ リストを集中的に定義するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI から、**[Devices] > [Devices]**（または **[Devices] > [Device Groups]**）を選択します。

ステップ 2　WCCP ルータ リストを作成したいデバイス（またはデバイス グループ）の名前の横にある **[Edit]** アイコンをクリックします。

ステップ 3　[Contents] ペインで、**[Interception] > [WCCP] > [Services]** を選択します。

[WCCP Service Settings] ウィンドウが表示されます。

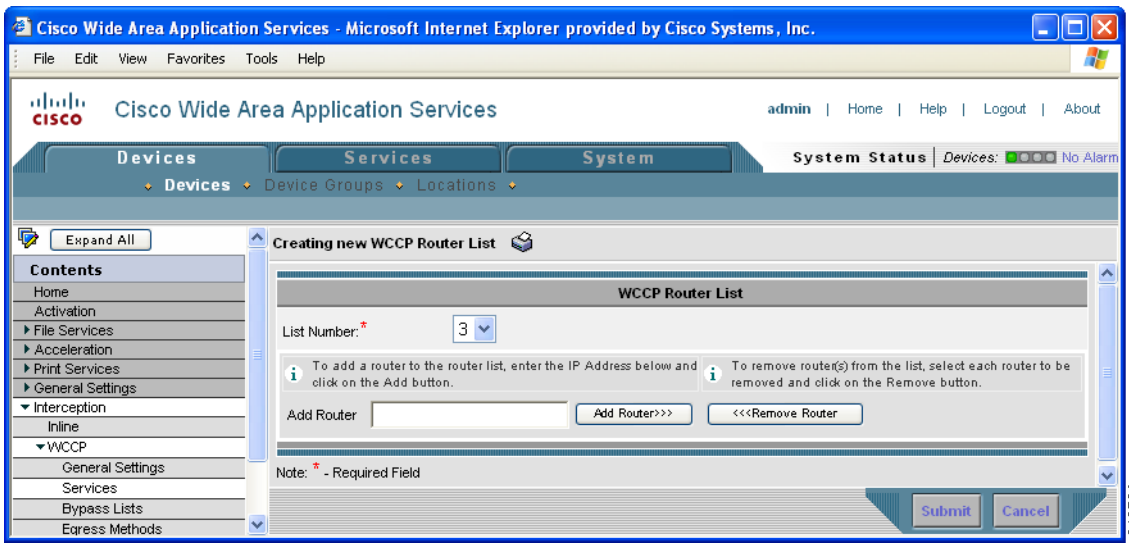
ステップ 4　**[Create New WCCP Service Settings]** アイコンをクリックして、WCCP バージョン 2 サービス用の新しいルータ リストを作成します。

[Creating New WCCP Service] ウィンドウが表示されます。

ステップ 5　**[New Router List]** ボタンをクリックします。

[Creating New WCCP Router List] ウィンドウが表示されます（図 4-5 を参照）。

図 4-5　新しい WCCP ルータ リストのサンプル画面の作成



この例では、選択したデバイス（またはデバイス グループ）用にすでに 2 つの WCCP ルータ リストが定義されているため、[List Number] ドロップダウン リストであらかじめ **[3]** が選択されています。データセンターでは、トラフィックを透過的に Core WAE へリダイレクトするルータ リスト 1 が WCCP ルータ用にすでに定義されています。また、ブランチ オフィスでは、透過的にトラフィックを同じブランチ オフィスに存在する Edge WAE へリダイレクトするルータ リスト 2 が WCCP ルータ用に定義されています。

ステップ 6　[Add Router] フィールドで、ルータ リスト 3 に追加するルータの IP アドレスを指定します。

少なくとも 1 つの IP アドレスを入力する必要があります。追加するすべての IP アドレスが、ルータ リストの中で固有である必要があります。そうでない場合は、適用時にエラー メッセージが表示されます。

ステップ 7　ルータ リスト 3 に IP アドレスを追加するには、**[Add]** をクリックします。

このリストは、TCP 無差別モード サービス用に選択した WAE（または WAE のグループ）へ透過的にトラフィックをリダイレクトするすべての WCCP ルータの IP アドレスを表します。

ウィンドウが更新され、アドレスが番号順に表示されます。順序は、IP アドレスを入力した順序と一致しない場合があります。

ステップ 8　**[Submit]** をクリックして、ルータ リストを保存するか、ルータ IP アドレスに行った編集を保存します。

CLI からルータ リストを定義するには、**wccp router-list** グローバル設定コマンドを使用できます。

WAE または WAE のグループで WCCP ルータ リストを作成したら、WAE または WAE のグループでルータ リストを特定の WCCP サービス（TCP 無差別モード サービス）に関連付ける必要があります。詳細については、「WAE 用の WCCP サービスの現在の設定の変更」（p.4-20）の ステップ 5 を参照してください。また、『*Cisco Wide Area Application Services Quick Configuration Guide*』の説明に従って、この新しいルータ リストに入っている WCCP ルータで、WCCP バージョン 2 と WCCP TCP 無差別サービスが有効になり、設定されていることを確認してください。

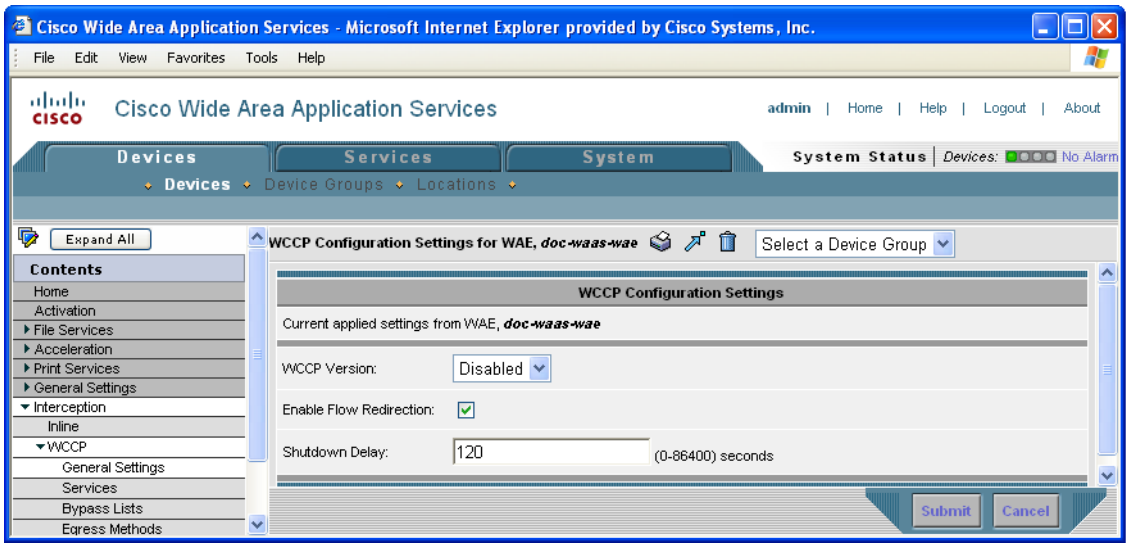
WCCP の正常なシャットダウンのための WAE の設定

TCP 接続の切断を防止するために、WAE は、WAE で WCCP バージョン 2 を無効にしたり、WAE をリロードしたあとで、WCCP の正常なシャットダウンを実行します。

WAAS Central Manager GUI を使用すると、WAE で WCCP バージョン 2 を集中的に無効にすることができます。また、CLI を使用して（WAE で **no wccp version** CLI コマンドを入力して）、この作業をローカルに実行することもできます。

選択したデバイスまたはデバイス グループ用の WCCP を集中的に無効にするには、WAAS Central Manager の [WCCP Configuration Settings] ウィンドウの **[WCCP Version]** ドロップダウン リストから **[Disabled]** を選択します（図 4-6 を参照）。

図 4-6　[WCCP Configuration Settings] ウィンドウ



WAE は、次のいずれかの状況になるまで起動しません。

- すべての接続がサービスを受けている。
- （[WCCP Configuration Settings] ウィンドウの [Shutdown Delay] フィールドまたは **wccp shutdown max-wait** コマンドで指定した）WCCP バージョン 2 の最大待ち時間が経過した（デフォルトは 120 秒）。

WCCP の正常なシャットダウンの間、WAE は継続して処理中のフローにサービスを提供しますが、新しいフローのバイパスを開始します。フローの数がゼロになると、リード WAE は、そのバケットを他の WAE に再割り当てグループから脱退します。WCCP を正常にシャットダウンすることなく WAE が機能停止またはリブートした場合は、TCP 接続が切断される可能性が残ります。

WAE の特定のポートで個々の WCCP サービスをシャットダウンできません。WAE の WCCP をシャットダウンする必要があります。WAE 上の WCCP がシャットダウンされると、WAE は自分の WCCP 構成の設定値を保存します。

WAE 用の固定バイパス リストの設定

固定バイパスを使用すると、設定可能な 1 組のクライアントとファイル サーバ間のトラフィックのフローを WAE によってバイパス処理することができます。Edge WAE に固定バイパス項目を設定すると、ルータの設定を変更することなく、トラフィックの代行受信を制御できます。ルータで、最初にトラフィックを Edge WAE へリダイレクションせず、トラフィックをバイパスするように、IP アクセス リストを個別に設定できます。通常、WCCP 受け入れリストは、キャッシュされるファイル サーバのグループを定義します（暗黙的に、キャッシュされないファイル サーバが定義されることとなります）。特定のクライアントから特定のファイル サーバ（または特定のクライアントからすべてのファイル サーバ）への接続を WAAS がキャッシングしないようにしたい場合、固定バイパスを使用することができます。

（注）　アクセス リストの方が効率的であるため、固定バイパス機能を使用するより、WCCP 対応ルータ上の IP アクセス リストを使用することを推奨します。ルータでバイパス リストを設定する方法については、「ルータ上の IP アクセス リストの設定」（p.4-9）を参照してください。

WAE（または WAE のグループ）用の固定バイパス リストを集中的に設定するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI から、**[Devices] > [Device]**（または **[Devices] > [Device Groups]**）を選択します。

ステップ 2　固定バイパス リストを作成したいデバイス（またはデバイス グループ）の名前の横にある **[Edit]** アイコンをクリックします。

ステップ 3　[Contents] ペインで、**[Interception] > [WCCP] > [Services]** を選択します。

ステップ 4　タスクバーで、**[Create New WCCP Bypass List]** アイコンをクリックします。[Creating new WCCP Bypass List] ウィンドウが表示されます

ステップ 5　[Client Address] フィールドに、クライアントの IP アドレスを入力します。

ステップ 6　[Server Address] フィールドに、サーバの IP アドレスを入力します。

ステップ 7　**[Submit]** をクリックして、設定を保存します。

CLI から固定バイパス リストを設定するには、**bypass static** グローバル設定コマンドを使用できます。

代行受信接続の出力方式の設定

WAAS 4.0.13 ソフトウェアでは、2 つの出力方式 IP 転送と WCCP GRE 返信による WCCP 代行受信接続をサポートします。

デフォルトの出力方式は IP 転送です。WCCP GRE 出力方式を設定しない場合、WAE では IP 転送を使用します。IP 転送出力方式では、WAE をクライアントおよびサーバとして同一の VLAN またはサブネットに配置することはできません。また、パケットが代行受信ルータに返信されるとは限りません。

WCC GRE 返信出力方式では、WAE をクライアントおよびサーバとして同一の VLAN またはサブネットに配置することができます。また最適化フローでは、WCCP GRE 返信により、冗長ルータおよびルータ負荷分散に「ベストエフォート」型サポートが提供されます。つまり、WCCP GRE を出力方式として設定すると、ネットワークでルータ負荷分散を使用した場合に WAAS は最初に選択したルータをベストエフォートで保持します。

WAAS は、次の論理に基づいて WCCP GRE のルータを選択します。

- WAAS ソフトウェアが DRE（データ冗長性除去）を実行して TCP フローを圧縮すると、出力されるパケット数は減少します。最適化されたデータを送信する単一パケットが、複数のルータからリダイレクトされた複数のパケットで受信されたオリジナル データを表す場合もあります。この最適化されたデータを送信するパケットは WAE から出力され、パケットを最後に WAE にリダイレクトしたルータに元のフロー方向で送信されます。
- WAE で受信された最適化データは、さまざまなルータから複数のパケットに入って送信される場合があります。WAAS は最適化されたデータをオリジナル データに戻し、複数のパケットとして送信します。オリジナル データを送信するパケットは WAE から出力され、パケットを最後に WAE にリダイレクトしたルータに元のフロー方向で送信されます。

WCCP バージョン 2 には、リダイレクト方式および返信方式をネゴシエートして代行受信接続を行う機能があります。ただし、WAAS は現在、WCCP がネゴシエートする唯一の返信方式として WCCP GRE をサポートしています。WCCP が WCCP L2 返信をネゴシエートすると、WAE はデフォルトの出力方式として IP 転送を使用します。WAE がデフォルトの IP 転送を有効にすると、通知は送信されなくなります。ただし、その場合は Syslog メッセージが生成されます。

CLI の設定に関係なく、WCCP バイパス トラフィックは WCCP GRE を返信方式として使用し IP 転送は使用しません。

WCCP によるネゴシエートの返信設定は、インライン モードの動作には適用されません。

WCCP 代行受信接続の出力方式を Central Manager GUI から設定する場合は、次の手順に従います。

ステップ 1　WAAS Central Manager GUI から、**[Devices] > [Devices]**（または **[Devices] > [Device Groups]**）を選択します。

ステップ 2　出力方式を設定するデバイス（またはデバイス グループ）の横にある **[Edit]** アイコンをクリックします。

ステップ 3　[Contents] ペインで、**[Interception] > [WCCP] > [Egress Methods]** を選択します。[Egress Methods for WAE]（または [Device Group]）ウィンドウが表示されます。

ステップ 4　[Interception Method] ドロップダウン リストで、代行受信の方式を選択します。現在は **[WCCP TCP Promiscuous]** だけを選択できます。

ステップ 5　[Egress Method Configured] ドロップダウン リストから、**[IP Forwarding]** または **[WCCP Negotiated Return]** を選択します。

ステップ 6　**[Submit]** をクリックします。

CLI で代行受信と WCCP GRE パケット返信による出力方式を設定するには、**egress-method** グローバル設定コマンドを使用します。

```
WAE(config)# egress-method negotiated-return intercept-method wccp
```

CLI で代行受信と IP 転送による出力方式を設定するには、**egress-method** グローバル設定コマンドを使用します。

```
WAE(config)# egress-method ip-forwarding intercept-method wccp
```

特定の WAE に設定した出力方式を表示するには、**show egress-methods** EXEC コマンドまたは **show tfo egress-methods connection** EXEC コマンドを使用します。

PBR を使用した WAE へのすべての TCP トラフィックの透過的なリダイレクション

Cisco IOS Software Release 11.0 で導入された PBR により、選択したパケットをネットワークの特定のパスで送信するポリシーが実装できるようになりました。

また、PBR は、Cisco IOS ソフトウェアを通じて可能になるキューイング手法と組み合わせて使用すると、特定の種類のトラフィックが差別化された優先サービスを受信するようにパケットにマークに付ける方法も提供します。これらのキューイング手法は、ネットワークにルーティング ポリシーを実装するネットワーク管理者に、非常に強力で単純で柔軟なツールを提供します。

PBR を使用すると、パケットをルーティングする前に、ルート マップを通過させることができます。PBR を設定するとき、一致基準とすべての一致節に適合する場合の処理を指定するルート マップを作成する必要があります。特定のインターフェイス上のそのルート マップ用に PBR を有効にする必要があります。指定したインターフェイスに到達し、一致節と一致するすべてのパケットが、PBR に支配されます。

1 つのインタフェースにはただ 1 つのルート マップ タグしか指定できませんが、シーケンス番号を持つ複数のルート マップ項目を作成できます。項目は、最初の一致が現れるまで、シーケンス番号の順に評価されます。一致する項目がない場合、パケットは通常のようにルーティングされます。

```
Router(config-if)# ip policy route--tag
```

ルート マップは、ルーティングするパケットの順序を決定します。

PBR を有効にして、一部またはすべてのパケットが WAAS を通過するルートを確立できます。WAAS プロキシ アプリケーションは、次のように、PBR がリダイレクションしたトラフィックと同じ方法で、PBR がリダイレクションしたトラフィックを受信します。

1. 次のように、ブランチ オフィスのルータ（Edge-Router1）で、関係するトラフィックを定義します。
   a. Edge-Router1 で、LAN インターフェイス（入力インターフェイス）に関係するトラフィックを指定します。

      拡張 IP アクセス リストを使用して、関係するトラフィック（すべてまたは選別されたローカル送信元アドレスから任意または選別された送信先アドレスへのトラフィック）を定義します。

   b. Edge-Router1 で、WAN インターフェイス（出力インターフェイス）に関係するトラフィックを指定します。

      拡張 IP アクセス リストを使用して、関係するトラフィック（すべてまたは選別されたローカル送信元アドレスから任意または選別されたリモート アドレスへのトラフィック）を定義します。
2. データセンターのルータ（Core-Router1）で、関係するトラフィックを指定します。
   a. Core-Router1 で、LAN インターフェイス（入力インターフェイス）に関係するトラフィックを指定します。

      拡張 IP アクセス リストを使用して、関係するトラフィック（すべてまたは選別されたローカル送信元アドレスから任意または選別された送信先アドレスへのトラフィック）を定義します。

   b. Core-Router1 で、WAN インターフェイス（出力インターフェイス）に関係するトラフィックを指定します。

      拡張 IP アクセス リストを使用して、関係するトラフィック（すべてまたは選別されたローカル送信元アドレスから任意または選別されたリモート アドレスへのトラフィック）を定義します。
3. 次のように、ブランチ オフィスの Edge-Router1 にルート マップを作成します。
   a. Edge-Router1 の LAN インターフェイスに PBR ルート マップを作成します。
   b. Edge-Router1 の WAN インターフェイスに PBR ルート マップを作成します。
4. 次のように、データセンターの Core-Router1 にルート マップを作成します。
   a. Core-Router1 の LAN インターフェイスに PBR ルート マップを作成します。
   b. Core-Router1 の WAN インターフェイスに PBR ルート マップを作成します。
5. ブランチ オフィスの Edge-Router1 に PBR ルート マップを適用します。
6. データセンターの Core-Router1 に PBR ルート マップを適用します。

7. WAE のネクストホップが使用できるかどうかを検査するために使用する PBR 方式を決定します。詳細については、「PBR のネクストホップが使用できるかどうかを確認する方法」（p.4-39）を参照してください。

（注）　このセクションで参照する PBR コマンドの完全な説明については、『*Cisco Quality of Service Solutions Command Reference*』を参照してください。

図 4-7 に示すように、WAE（Edge-WAE1 と Core-WAE1）は、トラフィックの送信先と送信元から分離された帯域外ネットワークに存在する必要があります。たとえば、Edge-WAE1 は、クライアント（トラフィックの送信元）とは別のサブネットに存在し、Core-WAE は、ファイル サーバとアプリケーション サーバ（トラフィックの送信先）とは別のサブネットに存在します。さらに、ルーティング ループを防止するために第 3 のインターフェイス（別の物理インターフェイス）またはサブインターフェイスを通じてトラフィックを WAE へリダイレクトするルータに、WAE を接続する必要があります。

図 4-7　PBR または WCCP バージョン 2 を使用してすべての TCP トラフィックを透過的に WAE へリダイレクトする例

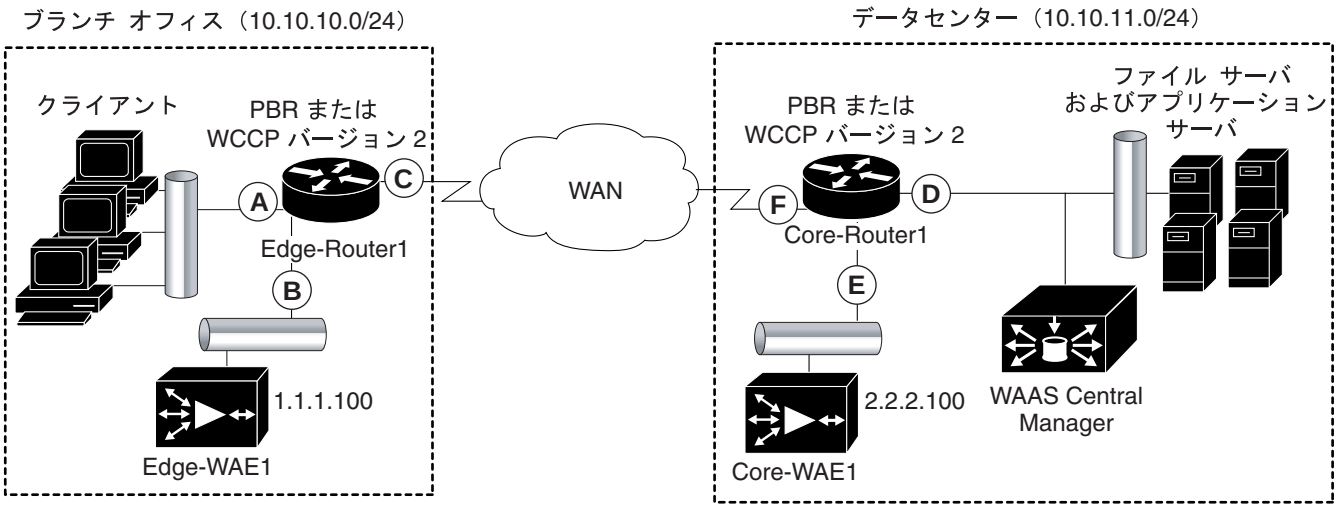


表 4-4 に、PBR または WCCP バージョン 2 を使用して、透過的にトラフィックを WAE へリダイレクトするために設定する必要があるルータ インターフェイスの概要を示します。

表 4-4　WCCP または PBR がトラフィックを WAE へリダイレクトするためのルータ インターフェイス

ルータ インターフェイス	説明
Edge-Router1	
A	発信トラフィックのリダイレクションを実行する Edge LAN インターフェイス（入力インターフェイス）。
B	Edge-Router1 の LAN ポートにない第 3 のインターフェイス（分離された物理インターフェイス）またはサブインターフェイス。ブランチ オフィスの Edge-Router1 に Edge-WAE1 を接続するために使用します。

表 4-4　WCCP または PBR がトラフィックを WAE へリダイレクトするためのルータ インターフェイス（続き）

ルータ インターフェイス	説明
C	着信トラフィックのリダイレクションを実行する Edge-Router1 の Edge WAN インターフェイス（出力インターフェイス）。
Core-Router1	
D	発信トラフィックのリダイレクションを実行する Core LAN インターフェイス（入力インターフェイス）。
E	Core-Router 上の LAN ポートにない第 3 のインターフェイスまたはサブインターフェイス。データセンターの Core-Router1 に Core-WAE1 を接続するために使用します。
F	着信トラフィックのリダイレクションを実行する Core-Router1 の Core WAN インターフェイス（出力インターフェイス）。

（注）　図 4-7 では、冗長性（たとえば、冗長なルータ、スイッチ、WAE、WAAS Central Manager、およびルータ）が省略されています。

次の例は、（図 4-7 に示すように）ブランチ オフィスに 1 台の Edge WAE 、データセンターに 1 台の Core WAE が存在する WAAS ネットワークで、トラフィック リダイレクション方式として PBR を設定する方法を示しています。

（注）　ルータで PBR を設定するために使用するコマンドは、ルータにインストールされている Cisco IOS リリースによって変化します。ルータで使用している Cisco IOS リリース用に PBR を設定するために使用するコマンドについては、該当する Cisco IOS 設定ガイドを参照してください。

TCP トラフィックを透過的に WAE へリダイレクトするように PBR を設定するには、次の手順に従ってください。

ステップ 1　ブランチ オフィスの Edge-Router で、拡張 IP アクセス リストを使用して、LAN インターフェイス（入力インターフェイス -A）に関係するトラフィックを指定します。

a. Edge-Router1 で、100 ～ 199 の範囲で拡張 IP アクセスを定義します。次の例では、Edge-Router1 にアクセス リスト 100 が作成されます。

```
Edge-Router1(config)# ip access-list extended 100
```

b. Edge-Router1 で、この特定のインターフェイスに関係するトラフィックを指定します。

- たとえば、任意の TCP ポート上の任意のローカル送信元アドレスから任意の送信先への任意の IP/TCP トラフィック（任意のブランチ オフィスクライアント用のトラフィック）に「関係がある」というマークを付けます。

```
Edge-Router1(config-ext-nac1)# permit tcp 10.10.10.0 0.0.0.255 any
```

- あるいは、送信元 IP サブネット、送信先 IP アドレス、および TCP ポート番号を定義して、選択的にトラフィックに「関係がある」というマークを付けることができます。たとえば、TCP ポート 135 と 80 上の任意のローカル送信元アドレスから任意の送信先への IP/TCP トラフィックに「関係がある」というマークを付けます。

```
Edge-Router1(config-ext-nac1)# permit tcp 10.10.10.0 0.0.0.255 any eq 135
Edge-Router1(config-ext-nac1)# permit tcp 10.10.10.0 0.0.0.255 any eq 80
```

ステップ 2　ブランチ オフィスの Edge-Router1 で、拡張 IP アクセス リストを使用して、WAN インターフェイス（出力インターフェイス -C）に関係するトラフィックを指定します。

a. Edge-Router1 で、100 ～ 199 の範囲で拡張 IP アクセスを定義します。次の例では、Edge-Router1 にアクセス リスト 101 が作成されます。

```
Edge-Router1(config)# ip access-list extended 101
```

b. Edge-Router1 で、WAN インターフェイスに関係するトラフィックを指定します。

- たとえば、ローカル デバイスへの任意の IP/TCP トラフィックに「関係がある」というマークを付けます。

```
Edge-Router1(config-ext-nac1)# permit tcp any 10.10.10.0 0.0.0.255
```

- あるいは、送信元 IP サブネット、送信先 IP アドレス、および TCP ポート番号を定義して、選択的にトラフィックに「関係がある」というマークを付けることができます。たとえば、TCP ポート 135 と 80 上の任意のローカル送信元アドレスから任意の送信先への IP/TCP トラフィックに「関係がある」というマークを付けます。

```
Edge-Router1(config-ext-nac1)# permit tcp any 10.10.10.0 0.0.0.255 eq 135
Edge-Router1(config-ext-nac1)# permit tcp any 10.10.10.0 0.0.0.255 eq 80
```

ステップ 3　データセンターの Core-Router1 で、拡張 IP アクセス リストを使用して、LAN インターフェイス（入力インターフェイス -D）に関係するトラフィックを指定します。

a. Core-Router1 で、100 ～ 199 の範囲で拡張 IP アクセスを定義します。次の例では、Core-Router1 にアクセス リスト 102 が作成されます。

```
Core-Router1(config)# ip access-list extended 102
```

b. Core-Router1 で、LAN インターフェイスに関係するトラフィックを指定します。

- たとえば、任意の TCP ポート上の任意のローカル デバイスから任意の送信先へ送信される 任意の IP/TCP トラフィック（たとえば、データセンターの任意のファイル サーバまたはアプリケーション サーバから送信されるトラフィック）に「関係がある」というマークを付けます。

```
Core-Router1(config-ext-nac1)# permit tcp 10.10.11.0 0.0.0.255 any
```

- あるいは、送信元 IP サブネット、送信先 IP アドレス、および TCP ポート番号を定義して、選択的にトラフィックに「関係がある」というマークを付けることができます。たとえば、TCP ポート 135 上の任意のローカル デバイスから任意の送信先への IP/TCP トラフィックに選択的に「関係がある」というマークを付けます。

```
Core-Router1(config-ext-nac1)# permit tcp 10.10.11.0 0.0.0.255 any eq 135
Core-Router1(config-ext-nac1)# permit tcp 10.10.11.0 0.0.0.255 any eq 80
```

ステップ 4　データセンターの Core-Router1 で、拡張 IP アクセス リストを使用して、WAN インターフェイス（出力インターフェイス -F）に関係するトラフィックを指定します。

a. Core-Router1 で、100 ～ 199 の範囲で拡張 IP アクセスを定義します。次の例では、Core-Router1 にアクセス リスト 103 が作成されます。

```
Core-Router1(config)# ip access-list extended 103
```

b. Core-Router1 で、WAN インターフェイス用のトラフィックに「関係がある」というマークを付けます。

- たとえば、任意のローカル デバイスへ送信される任意の IP/TCP トラフィック（たとえば、データセンターの任意のファイル サーバまたはアプリケーション サーバへ送信されるトラフィック）に「関係がある」というマークを付けます。

```
Core-Router1(config-ext-nac1)# permit tcp any 10.10.11.0 0.0.0.255
```

- あるいは、送信元 IP サブネット、送信先 IP アドレス、および TCP ポート番号を定義して、選択的にトラフィックに「関係がある」というマークを付けることができます。たとえば、TCP ポート 135 と 80 上の任意のローカル送信元アドレスへの IP/TCP トラフィックに「関係がある」というマークを付けます。

```
Core-Router1(config-ext-nac1)# permit tcp any 10.10.11.0 0.0.0.255 eq 135
Core-Router1(config-ext-nac1)# permit tcp any 10.10.11.0 0.0.0.255 eq 80
```

ステップ 5　ブランチ オフィスの Edge-Router1 に PBR ルート マップを定義します。

a. LAN インターフェイス（入力インターフェイス）用のルート マップを定義します。次の例で、WAAS-EDGE-LAN ルート マップが作成されます。

```
Edge-Router1(config)# route-map WAAS-EDGE-LAN permit
```

b. WAN インターフェイス（出力インターフェイス）用のルート マップを定義します。

次の例で、WAAS-EDGE-WAN ルート マップが作成されます。

```
Edge-Router1(config)# route-map WAAS-EDGE-WAN permit
```

c. 一致基準を指定します。

match コマンドを使用して、Edge-Router1 が、どのトラフィックが WAN インターフェイスに関係があるかを決定するために使用する拡張 IP アクセス リストを指定します。**match** コマンドを指定しない場合、ルート マップはすべてのパケットに適用されます。

次の例で、Edge-Router1 は、WAN インターフェイスに関係があるトラフィックを決定するための基準として、アクセス リスト 101 を使用するように設定されます。

```
Edge-Router1(config-route-map)# match ip address 101
```

（注）　**ip address** コマンド オプションは、1 つまたは複数の標準または拡張アクセス リストで許可される送信元または送信先 IP アドレスを照合します。

d. 一致したトラフィックを処理する方法を指定します。

次の例で、Edge-Router1 は、指定した基準と一致するパケットをネクストホップ（IP アドレスが 1.1.1.100 の Edge-WAE1）へ送信するように設定されます。

```
Edge-Router1(config-route-map)# set ip next-hop 1.1.1.100
```

（注）　複数の Edge WAE がある場合、フェールオーバーの目的で 2 番めの Edge WAE の IP アドレスを指定して（たとえば、Edge-Router1 で **set ip next-hop 1.1.1.101** コマンドを入力して）、フェールオーバーの目的でネクストホップ アドレス 1.1.1.101（Edge-WAE2 の IP アドレス）を指定できます。**next-hop** コマンドは、負荷分散の目的でなく、フェールオーバーの目的で使用されます。

ステップ 6　データセンターの Core-Router1 にルート マップを作成します。

a. LAN インターフェイス（入力インターフェイス）でルート マップを定義します。

次の例で、WAAS-CORE-LAN ルート マップが作成されます。

```
Core-Router1(config)# route-map WAAS-CORE-LAN permit
```

b. WAN インターフェイス（出力インターフェイス）でルート マップを定義します。

次の例では、WAAS-CORE-WAN ルート マップが作成されます。

```
Core-Router1(config)# route-map WAAS-CORE-WAN permit
```

c. 一致基準を指定します。

match コマンドを使用して、Core-Router1 がどのトラフィックが WAN インターフェイスに関係があるかを決定するために使用する拡張 IP アクセス リストを指定します。**match** コマンドを入力しない場合、ルート マップはすべてのパケットに適用されます。次の例で、Core-Router1 は、WAN インターフェイスに関係があるトラフィックを決定するための基準として、アクセス リスト 103 を使用するように設定されます。

```
Core-Router1(config-route-map)# match ip address 103
```

d. 一致したトラフィックを処理する方法を指定します。

次の例で、Core-Router1 は、指定した基準と一致するパケットをネクストホップ（IP アドレスが 2.2.2.100 の Core-WAE1）へ送信するように設定されます。

```
Core-Router1(config-route-map)# set ip next-hop 2.2.2.100
```

（注）　複数の Core WAE がある場合、フェールオーバーの目的で 2 番めの Core WAE の IP アドレスを指定して（たとえば、Core-Router1 で **set ip next-hop 2.2.2.101** コマンドを入力して）、フェールオーバーの目的でネクストホップ アドレス 2.2.2.101（Core-WAE2 の IP アドレス）を指定できます。**next-hop** コマンドは、負荷分散の目的でなく、フェールオーバーの目的で使用されます。

ステップ 7　ブランチ オフィスの Edge-Router1 の LAN インターフェイス（入力インターフェイス）と WAN インターフェイス（出力インターフェイス）にルート マップを適用します。

a. Edge-Router1 で、インターフェイス設定モードに入ります。

```
Edge-Router1(config)# interface FastEthernet0/0.10
```

b. LAN ルータ インターフェイスが PBR 用の WAAS-EDGE-LAN ルート マップを使用するように指定します。

```
Edge-Router1(config-if)# ip policy route-map WAAS-EDGE-LAN
```

c. インターフェイス設定モードに入ります。

```
Edge-Router1(config-if)# interface Serial0
```

d. WAN ルータ インターフェイスが PBR 用の WAAS-EDGE-WAN ルート マップを使用するように指定します。

```
Edge-Router1(config-if)# ip policy route-map WAAS-EDGE-WAN
```

ステップ 8　データセンターの Core-Router1 の LAN インターフェイス（入力インターフェイス）と WAN インターフェイス（出力インターフェイス）にルート マップを適用します。

a. Core-Router1 で、インターフェイス設定モードに入ります。

```
Core-Router1(config)# interface FastEthernet0/0.10
```

b. LAN ルータ インターフェイスが PBR 用の WAAS-CORE-LAN ルート マップを使用するように指定します。

```
Core-Router1(config-if)# ip policy route-map WAAS-CORE-LAN
```

c. インターフェイス設定モードに入ります。

```
Core-Router1(config-if)# interface Serial0
```

d. WAN ルータ インターフェイスが PBR 用の WAAS-CORE-WAN ルート マップを使用するように指定します。

```
Core-Router1(config-if)# ip policy route-map WAAS-CORE-WAN
```

PBR のネクストホップが使用できるかどうかを確認する方法

PBR を使用してトラフィックを透過的に WAE へリダイレクトするときは、次のいずれかの方法を使用して、WAE の PBR のネクストホップが使用できるかどうかを確認することを推奨します。選択する方法は、ルータで使用している Cisco IOS ソフトウェアのバージョンと WAE の配置によって異なります。ただし、可能なかぎり、方法 2 を使用してください。

- 方法 1 — デバイスは、WAE を CDP 隣接（直接接続されている）とみなすと、CDP と ICMP を使用して WAE が動作していることを確認できます。詳細については、「方法 1 ：CDP を使用して WAE が動作していることを確認する。」（p.4-40）を参照してください。
- 方法 2（推奨方式）— Cisco IOS ソフトウェア リリース 12.4 以降が動作しているデバイスが WAE を CDP 隣接と見なさない場合は、IP サービス レベル契約（SLA）を使用して、ICMP エコーを使用して WAE が動作していることを確認できます。詳細については、「方法 2 ：IP SLA を使用して、ICMP エコー検査を使用して WAE が動作していることを確認する（推奨方式）」（p.4-40）を参照してください。
- 方法 3 — Cisco IOS ソフトウェア リリース 12.4 以降が動作しているデバイスが WAE を CDP 隣接と見なさない場合は、IP サービス レベル契約（SLA）を使用して、TCP 接続試行 を使用して WAE が動作していることを確認できます。詳細については、「方法 3 ：IP SLA を使用して、TCP 接続試行を使用して WAE が動作可能していることを確認する。」（p.4-41）を参照してください。

（注）　この項で、「デバイス」という用語は、PBR を使用してトラフィックを透過的に WAE へリダイレクトするように設定されたルータまたはスイッチのことを指しています。

PBR を使用するように設定されたデバイスが WAE を CDP 隣接とみなすかどうかを確認するには、デバイスで **show cdp neighbors** コマンドを入力します。デバイスが WAE を CDP 隣接とみなす場合、WAE は **show cdp neighbors** コマンドの出力に表示されます。

方法 1 ：CDP を使用して WAE が動作していることを確認する。

PBR を使用するように設定されたデバイスが WAE を CDP 隣接（WAE がデバイスに直接接続されている）とみなす場合は、CDP と ICMP を使用して PBR のネクストホップとして WAE を使用できるかどうかを確認できます。

次の例は、この方法を使用して、PBR のネクストホップとして WAE を使用できるかどうかを確認する方法を示しています。CDP を使用する必要があるときに設定される LAN ルート マップと WAN ルート マップのそれぞれについて、次の設定プロセスを完了する必要があります。

CDP を使用して WAE が動作していることを確認するには、次の手順に従ってください。

ステップ 1　PBR が設定されているルータ（たとえば、ブランチ オフィスの Edge-Router1 ルータ）で、設定モードに入り、CDP を有効にします。

```
Edge-Router1(config)# cdp run
```

ステップ 2　すでにルータに作成されている WAAS-EGDE-LAN ルート マップ用のルート マップ設定モードを有効にします。

```
Edge-Router1(config)# route-map WAAS-EDGE-LAN permit
```

ステップ 3　CDP を使用して設定済みのネクストホップ アドレスが使用できるかどうかを確認するようにルータを設定します。

```
Edge-Router1(config-route-map)# set ip next-hop verify-availability
```

ステップ 4　ルータが PBR を使用してトラフィックをリダイレクトするようにしたい WAE（たとえば、ブランチ オフィスの Edge-WAE1）で、CDP を有効にします。

```
Edge-WAE1(config)# cdp enable
```

PBR を設定し、複数の WAE があり、方法 1 を使用して PBR のネクストホップとして WAE が使用できることを確認する場合、前のプロセスを完了したら、追加の設定は不要です。

方法 2 ：IP SLA を使用して、ICMP エコー検査を使用して WAE が動作していることを確認する（推奨方式）

IP SLA と ICMP を使用して（推奨方式）、PBR のネクストホップとして WAE が使用できることを確認するには、次の手順に従ってください。

ステップ 1　ブランチ オフィスの Edge-Router1 ルータで、このルータですでに設定されている WAAS-EDGE-LAN ルート マップ用のルート マップ設定モードに入ります。

```
Edge-Router1(config)# route-map WAAS-EDGE-LAN permit
```

ステップ 2　トラフィックの一致条件を指定します。次の例では、一致条件にアクセス リスト番号 105 が指定されます。

```
Edge-Router1(config)# match ip address 105
```

ステップ 3　IP SLA 追跡インスタンス番号 1 を使用してネクストホップ WAE（たとえば、IP アドレスが 1.1.1.100 の Edge-WAE1）が使用できることを確認するように、ルート マップを設定します。

```
Edge-Router1(config-route-map)# set ip next-hop verify-availability 1.1.1.100 track 1
```

（注）　ブランチ オフィスのエッジ ルータと PBR を使用してトラフィックを WAE へリダイレクトするように設定されているデータセンターのコア ルータに設定されている各ルート マップについて、**set ip next-hop verify-availability** コマンドを入力します。

ステップ 4　IP SLA 追跡インスタンス 1 を設定します。

```
Edge-Router1(config-route-map)# exit
Edge-Router1(config)# ip sla 1
Edge-Router1(config-ip-sla)#
```

ステップ 5　指定のソース インターフェイスを使用し、Edge-WAE1 をエコーするようにルータを設定します。

```
Edge-Router1(config-ip-sla)# icmp-echo 1.1.1.100 source-interface FastEthernet 0/0.20
```

ステップ 6　20 秒周期でエコーを実行するようにルータを設定します。

```
Edge-Router1(config-ip-sla)# frequency 20
Edge-Router1(config-ip-sla)# exit
```

ステップ 7　ただちに開始し、継続的に動作するように、IP SLA 追跡インスタンス 1 のスケジュールを設定します。

```
Edge-Router1(config)# ip sla schedule 1 life forever start-time now
```

ステップ 8　IP SLA 追跡インスタンス 1 で定義されているデバイスを追跡するように、IP SLA 追跡インスタンス 1 を設定します。

```
Edge-Router1(config)# track 1 rtr 1
```

PBR を設定し、複数の WAE があり、方法 2 を使用して PBR のネクストホップとして WAE が使用できることを確認している場合は、WAE ごとに別々の IP SLA を設定し、IP SLA ごとに **track** コマンドを実行する必要があります。

方法 3 ：IP SLA を使用して、TCP 接続試行を使用して WAE が動作可能していることを確認する。

PBR 用に設定され、Cisco IOS ソフトウェアリリース 12.4 以降が動作しているデバイスが WAE を CDP 隣接と見なさない場合は、IIP SLA を使用して、TCP 接続試行 を使用して WAE が動作していることを確認できます。IP SLA を使用して、60 秒の固定周期で TCP 接続試行を使用して、PBR のネクストホップとして WAE が使用できることを監視できます。

PBR のネクストホップとして WAE が使用できることを確認するには、次の手順に従ってください。

ステップ 1　ブランチ オフィスの Edge-Router1 ルータで、このルータですでに設定されている WAAS-EDGE-LAN ルート マップ用のルート マップ設定モードに入ります。

```
Edge-Router1(config)# route-map WAAS-EDGE-LAN permit
```

ステップ 2　IP SLA 追跡インスタンス番号 1 を使用してネクストホップ WAE（たとえば、IP アドレスが 1.1.1.100 の Edge-WAE）が使用できることを確認するように、ルート マップを設定します。

```
Edge-Router1(config-route-map)# set ip next-hop verify-availability 1.1.1.100 track 1
```

（注）　ブランチ オフィスのこのエッジ ルータと PBR を使用してトラフィックを透過的に WAE へリダイレクトするように設定されているデータセンターのコア ルータの各ルート マップについて、**set ip next-hop verify-availability** コマンドを入力します。

ステップ 3　IP SLA 追跡インスタンス 1 を設定します。

```
Edge-Router1(config-route-map)# exit
Edge-Router1(config)# ip sla 1
```

ステップ 4　指定した送信先ポートと送信元ポートを使用し、60 秒の固定周期で TCP 接続試行を使用して WAE が使用できることを監視するように、ルータを設定します。

```
Edge-Router1(config-ip-sla)# tcp-connect 1.1.1.100 80 source-port 51883 control
disable
Edge-Router1(config-ip-sla)# exit
```

ステップ 5　ただちに開始し、継続的に動作するように、IP SLA 追跡インスタンス 1 のスケジュールを設定します。

```
Edge-Router1(config)# ip sla schedule 1 life forever start-time now
```

ステップ 6　IP SLA 追跡インスタンス 1 で定義されているデバイスを追跡するように、IP SLA 追跡インスタンス 1 を設定します。

```
Edge-Router1(config)# track 1 rtr 1
```

PBR を設定し、複数の WAE があり、方法 3 を使用して PBR のネクストホップとして WAE が使用できることを確認している場合は、WAE ごとに別々の IP SLA を設定し、IP SLA ごとに **track** コマンドを実行する必要があります。

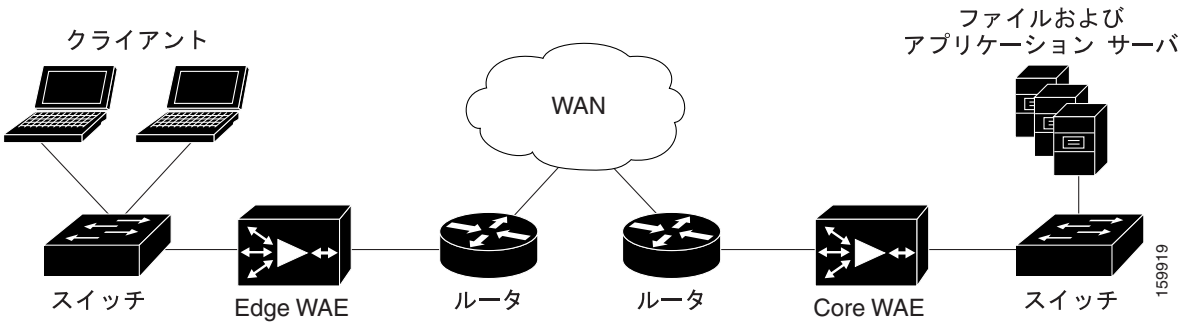
TCP トラフィックの透過的な代行受信へのインライン モードの使用

インライン モードを使用して、WAE は、物理的に透過的にトラフィックをクライアントとルータの間で代行受信できます。インライン モードを使用するには、Cisco WAE Inline Network Adapter がインストールされた WAE を使用する必要があります。このモードでは、WAE デバイスを最適化するトラフィックのパスに物理的に配置します。通常は、図 4-8 で表示したスイッチとルータの間です。トラフィックのリダイレクションは必要ありません。

（注）　インライン WAE デバイスをインストールするときは、Cisco.com にある『*Installing the Cisco WAE Inline Network Adapter*』の「Cabling」セクションのケーブルの要件に従う必要があります。

ピア WAE 上でのトラフィック代行受信メカニズムの任意の組み合わせがサポートされています。たとえば、インライン代行受信を Core WARE 上の Edge WAE と WCCP で使用できます。複雑なデータセンターの構成に対して、ハードウェアが加速化された WCCP 代行受信または Cisco Application Control Engine（ACE）での負荷分散の使用を推奨します。

図 4-8　インライン代行受信



（注）　インライン モードと WCCP リダイレクションは排他的です。WAE が WCCP 操作用に設定されている場合は、インライン モードを設定できません。インライン モードは、WAE デバイスに Cisco WAE Inline Network Adapter がインストールされたときのデフォルトのモードです。

（注）　Cisco WAE Inline Network Adapter のある WAE は、Central Manager として設定できますが、インライン代行受信機能は有効ではありません。

Cisco WAE Inline Network Adapter には、2 つの論理グループにグループ化されるイーサネット ポートが含まれます。各グループには LAN 対応ポート 1 つと WAN 対応ポート 1 つがあります。通常、1 つのグループのみを使用し、LAN 対応ポートをスイッチに接続し、WAN 対応ポートをルータに接続します。WAE を 2 つのルータに接続する必要があるネットワーク トポロジを使用する場合、インターフェイスの 2 番めのグループが提供されます。グループで 1 つのインターフェイスを入力するトラフィックは、同じグループの別のインターフェイス上のデバイスを終了させます。

（注）　Cisco WAE Inline Network Adapter とインライン モードを使用する場合でも、WAE アプライアンス上で組み込みイーサネット インターフェイスを設定する必要があります。組み込みインターフェイスは、CIF で加速化されたトラフィック、プリント サービス トラフィック、および WAAS Central Manager と交換された管理トラフィック、非透過的なトラフィック、Telnet などの特に WAE ダイレクトされるトラフィックに使用されます。

Cisco WAE Inline Network Adapter を通過するトラフィックは、最適化のために、透過的に代行受信されます。最適化の必要のないトラフィックは、LAN/WAN インターフェイス間でブリッジされます。電源、ハードウェア、回復不能なソフトウェアの障害が発生した場合、ネットワーク アダプタは、自動的にバイパス モードで動作し始めます。この場合、すべてのトラフィックは各グループで LAN と WAN のインターフェイス間で機械的にブリッジングされます。WAE の電源を切るか起動したときに、Cisco WAE Inline Network Adapter もバイパス モードで動作します。さらに、手動で Cisco WAE Inline Network Adapter をバイパス モードに追加することもできます。

インライン モードはデフォルトで、すべての TCP トラフィックを受けるように設定されます。WAE が挿入されるネットワーク セグメントが 802.1 のタグ付け（VLAN）トラフィックを実行中の場合、最初にすべての VLAN 上のトラフィックが受信されます。インライン代行受信は、各 VLAN に対して、有効または無効にできます。ただし、最適化のポリシーは、VLAN 上でカスタマイズできません。

Cisco WAE Inline Network Adapter が搭載された複数の WAE デバイスを連続的にクラスタ化して、スピルオーバー負荷分散やアクティブ / アクティブ フェールオーバーを提供できます。詳細については、「インライン WAE のクラスタリング」（p.4-48）を参照してください。

（注）　Cisco WAE Inline Network Adapter がインストールされた WAE がバイパス モードを入力するとき、接続されたスイッチとルータのポートは、再初期化される場合があり、これによって数秒間トラフィックの WAE の通過が中断される場合があります。

WAE がループの作成ができないような設定で展開される場合（つまり、スイッチとルータ間にスタンダードな形式で展開される場合）、スイッチ ポート上の PortFast を WAE が接続されるように設定します。PortFast によって、ポートは、Spanning Tree Algorithm（STA; スパニング ツリー アルゴリズム）の最初の数ステージをスキップでき、より早くパケット転送モードに移行できます。

ここでは、次の内容について説明します。

インライン インターフェイス設定

インライン インターフェイス設定を行うには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI から、**[Devices] > [Devices]** を選択します。（[Device Groups] からインライン インターフェイスを設定できません。）

WAAS ネットワークに設定されているすべてのデバイス タイプを表示する [Devices] ウィンドウが表示されます。

ステップ 2　インライン設定を変更したいデバイスの横にある **[Edit]** アイコンをクリックします。

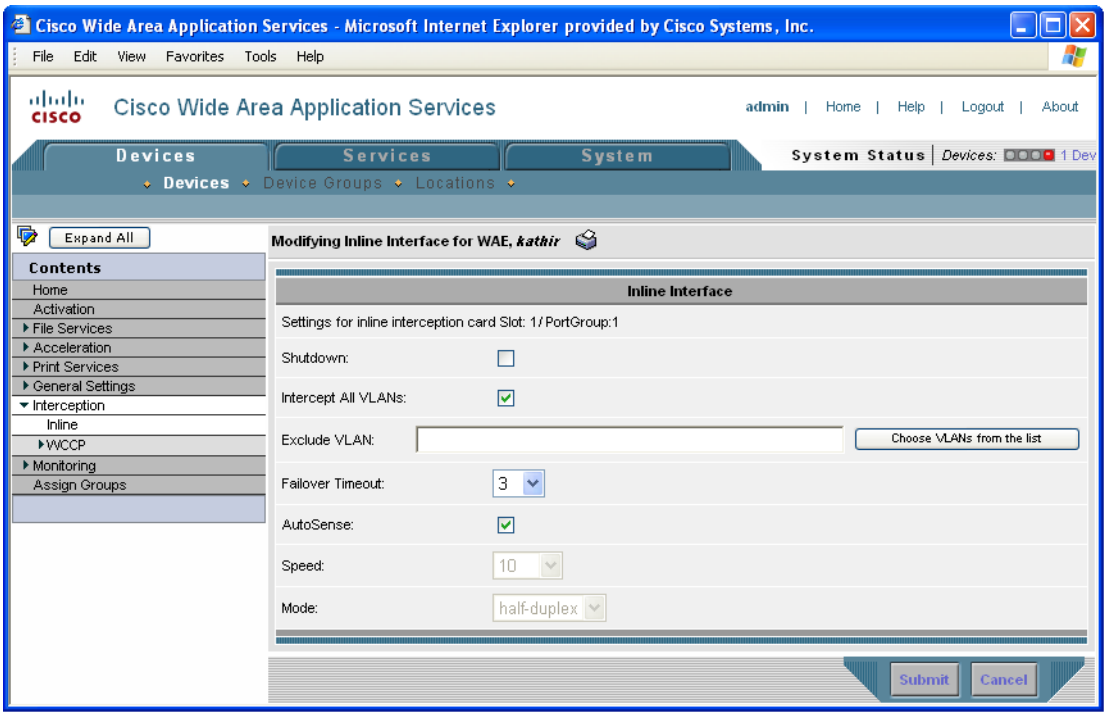
[Device Home] ウィンドウが表示され、左側に [Contents] ペインが表示されます。

ステップ 3　[Contents] ペインで、**[Interception] > [Inline]** を選択します。

[Inline Interfaces] ウィンドウが表示され、デバイス上のインライン インターフェイス グループをリストします。変更したいインライン インターフェイス グループの横にある **[Edit Inline Interface]** アイコンをクリックします。

[Modifying Inline Interface] ウィンドウが表示され、特定のスロットとグループ上のインライン インターフェイス設定が表示されます（図 4-9 を参照）。

図 4-9　[Modifying Inline Interfaces] ウィンドウ



ステップ 4　**[Shutdown]** チェック ボックスを選択して、インターフェイスを停止します。この設定は、処理なしでトラフィックを LAN/WAN インターフェイス間でブリッジングします。

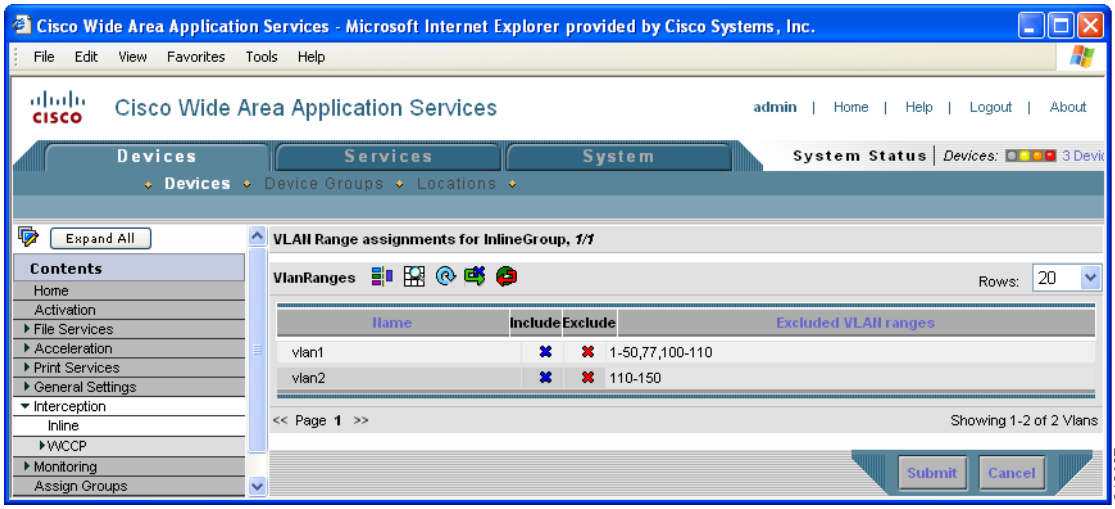
ステップ 5　**[Intercept all VLANs]** チェックボックスをチェックして、インターフェイス グループのインライン代行受信を有効にします。デフォルトでインライン代行受信が有効な場合、WAE は Cisco WAE Inline Network Adapter を含みます。

（注）　インライン モードと WCCP リダイレクションは排他的です。WAE が WCCP 操作用に設定されている場合は、インライン モードを設定できません。インライン モードは、WAE デバイスに Cisco WAE Inline Network Adapter がインストールされたときのデフォルトのモードです。

ステップ 6　[Exclude VLAN] フィールドで、最適化から除外する 1 つまたは複数の VLAN 範囲のリストを入力します。native VLAN を除外するには、「native」という言葉を入力できます。各 VLAN 範囲をカンマで分離します。代わりに、次に示す手順に従って、VLAN 範囲をリストから選択できます。

a. **[Choose VLANs from the list]** ボタンをクリックして、VLAN 範囲をピックします。[VLAN Range Assignments] ウィンドウが表示され、定義された VLAN 範囲を表示します（図 4-10 を参照）。VLAN 範囲の定義は、「インライン サポートの VLAN の設定」（p.4-47）で説明されます。

図 4-10　[VLAN Range Assignments] ウィンドウ



b. 含める、または除外する VLAN 範囲を次の手順で選択します。

- このインライン インターフェイス グループの最適化に含めるそれぞれの VLAN 範囲の横の ✖ をクリックします。アイコンは ✔ に変わります。最適化に含まれないすべての VLAN は、除外されます。
- このインライン インターフェイス グループの最適化から除外するそれぞれの VLAN 範囲の横の ✖ をクリックします。アイコンは ✔ に変わります。
- タスクバーの をクリックして最適化する有効な VLAN 範囲を選択するか、タスクバーの をクリックして、すべての VLAN 範囲を最適化から除外します。

c. **[Submit]** をクリックします。

ステップ 7　[Failover Timeout] ドロップダウン リストから、**1**、**3**、**5**、または **10** 秒を選択します。デフォルトは 1 秒です。この値は、バイパス モードで動作を開始する前に、WAE が待つ障害イベント後の秒数を設定します。バイパス モードでは、インターフェイス グループのいずれかのポートで受信されるすべてのトラフィックはグループの別のポートへ転送されます。

ステップ 8　ポートについて [Speed] と [Mode] を次のように設定します。

a. デフォルトで有効になっている **[AutoSense]** チェックボックスのチェックを外します。

b. [Speed] ドロップダウン リストから、伝送速度（**10**、**100**、または **1000** Mbps）を選択します。

c. [Mode] ドロップダウン リストから、送信モード（**[full-duplex]** または **[half-duplex]**）を選択します。

（注）　WAE、ルータ、スイッチ、またはその他のデバイスでは半二重接続を使用しないことを強く推奨します。半二重接続だとパフォーマンスが低下するので、使用は避けてください。各 Cisco WAE インターフェイスおよび隣接デバイス（ルータ、スイッチ、ファイアウォール、WAE）のポート設定を調べて、全二重接続が使用されていることを確認してください。

ステップ 9　**[Submit]** をクリックします。

CLI からインライン代行受信を設定するには、**interface InlineGroup** グローバル設定コマンドを使用できます。

インライン サポートの VLAN の設定

最初、WAE はトラフィックをすべての VLAN から受信します。ある VLAN からのトラフィックを含めるまたは排除するように WAE を設定できます。排除された VLAN に対してトラフィックはグループで LAN/WAN インターフェイス間でブリッジングされ、処理されません。

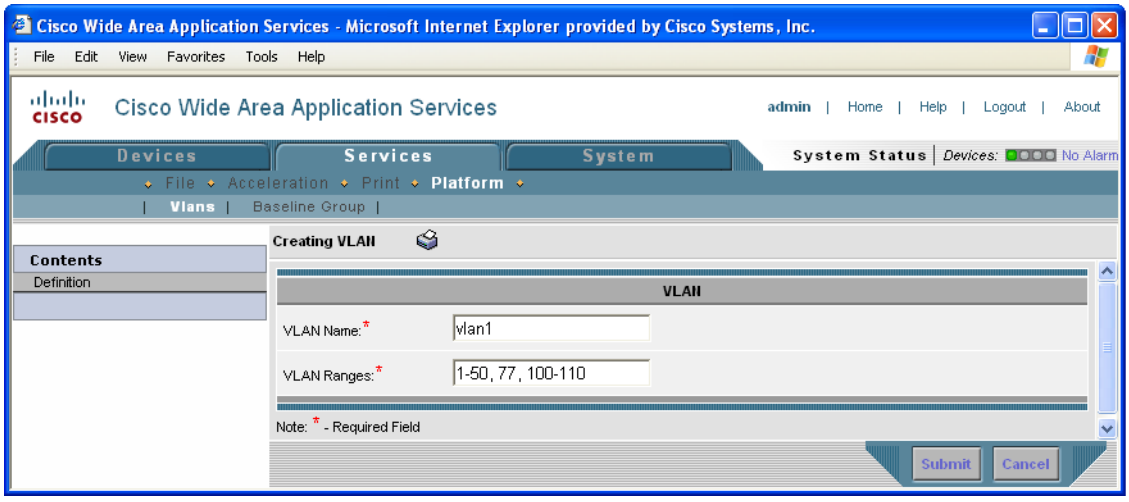
インラインをサポートするように VLAN を設定するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI から、**[Services] > [Platform] > [Vlans]** を選択します。

[Vlans] ウィンドウが表示され、定義された VLAN をリストします。修正する既存の VLAN の横の **[Edit Vlan]** アイコンをクリックできます。

ステップ 2　タスクバーで、**[Create New Vlan]** アイコンをクリックします。[Creating Vlan] ウィンドウが表示されます（図 4-11 を参照）。

図 4-11　[Creating New Vlan] ウィンドウの例



ステップ 3　[Vlan Name] フィールドで、VLAN リストの名前を入力します。

ステップ 4　[VLAN Ranges] フィールドで、1 つまたは複数の VLAN 範囲のリストを入力します。各 VLAN 範囲をカンマで分離します（スペースはなし）。「インライン インターフェイス設定」（p.4-44）の説明に従って、インライン インターフェイス グループを設定するときに、VLAN 範囲のこのリストは、最適化に含めたり除外することができます。このフィールドに「native」を指定できません。

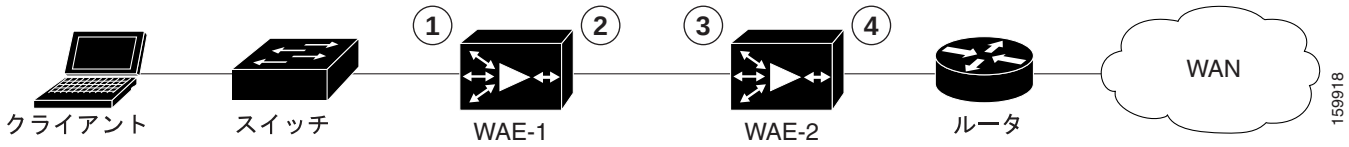
ステップ 5　**[Submit]** をクリックします。

VLAN リスト作成のこの機能が提供され、VLAN リストをグローバルに設定できます。インライン インターフェイス用に VLAN を設定するには、この機能を使用する必要はありません。「インライン インターフェイス設定」（p.4-44）の説明に従って、インライン インターフェイス設定ウィンドウで VLAN を直接設定できます。

インライン WAE のクラスタリング

Cisco WAE Inline Network Adapter が搭載された複数の WAE デバイスを連続的にクラスタ化して、スピルオーバー負荷分散や active-active フェールオーバーを提供できます。シリアル クラスタは、連続的にトラフィック パスで接続される 2 つ以上の WAE デバイスで構成されます。1 つの Cisco WAE Inline Network Adapter の WAN ポートは、図 4-12 に示すように、次の Cisco WAE Inline Network Adapter の LAN ポートなどに接続されます。

図 4-12　インライン クラスタ



1	WAE-1 のインライン LAN ポート	3	WAE-2 のインライン LAN ポート
2	WAE-1 のインライン WAN ポート	4	WAE-2 のインライン WAN ポート

シリアル クラスタでは、スイッチとルータの間のすべてのトラフィックは、すべてのインライン WAE を通過します。図 4-12 では、接続しきい値に達するまで、WAE-1 による TCP 接続が最適化されます。さらに、WAE-2 によって接続が最適化されます。この変更はスピルオーバー負荷共有と言われます。

WAE に障害があった場合、自動的にトラフィックをバイパスし、これは、クラスタの別の WAE で処理されます。

シリアルでクラスタ化された WAE のポリシー設定は同じである必要があります。異なる場合は、スピルオーバー負荷分散とフェールオーバー機能は、ポリシーに合ったトラフィックのクラスのみに適用されます。

CIFS クライアント要求の要求リダイレクション

IP ベースのブランチ オフィスのネットワークでは、クライアントは Common Internet File System（CIFS）プロトコルを使用して、ネットワーク接続されたサーバにファイル サービスとプリント サービスを要求します。

WAFS ソフトウェアは、クライアントから Edge WAE として動作する WAE へ CIFS 要求をリダイレクトするための方式を複数の方法をサポートしています。ここでは、次の内容について説明します。

インライン モードを使用した CIFS クライアント要求の透過的なリダイレクション

IP ベースのブランチ オフィスのネットワークでは、クライアントは CIFS プロトコルを使用して、ネットワーク接続されたサーバにファイル サービスとプリント サービスを要求します。WAAS は、Cisco WAE Inline Network Adapter のあるインライン モードを使用した CIFS 要求の透過的な代行受信をサポートしています。

この代行受信およびリダイレクション プロセスは、内容を要求しているクライアントにはまったく見えず、つまり透過的であるため、デスクトップを変更する必要はありません。Edge WAE 動作はネットワークに透過的です。

Edge WAE は、透過インライン モードで動作している場合は、サーバ名を公開しません。CIFS クライアントは、ブランチ オフィスの IT インフラストラクチャを使用して、CIFS サーバ名を IP アドレス（DNS、WINS）に解決します。クライアントがファイル サーバに接続しているとき、インライン WAE は TCP パケットを代行受信し、元のターゲット サーバ IP アドレスに抽出し、要求を処理します。

Edge WAE によってキャッシュされない CIFS サーバへのクライアント接続は、サポートされています。インライン WAE はこれらの要求を代行受信しませんが、代わりに送信先に通過させます。

WCCP を使用した CIFS クライアント要求の透過的なリダイレクション

IP ベースのブランチ オフィスのネットワークでは、クライアントは CIFS プロトコルを使用して、ネットワーク接続されたサーバにファイル サービスとプリント サービスを要求します。WAAS は、WCCP バージョン 2 を使用した CIFS 要求の透過的な代行受信をサポートしています。この CIFS 要求の透過的な代行受信は、IP ヘッダー情報と TCP ヘッダー情報に基づいて、Edge WAE として動作する WAE へ CIFS 要求をリダイレクションします。

WAAS ソフトウェアは、TCP 無差別モードサービスという WCCP バージョン 2 サービス（WCCP バージョン 2 サービス 61 および 62）をサポートしています。TCP 無差別モード サービスを使用すると、WCCP バージョン 2 を使用してすべての TCP トラフィックを透過的に代行受信し、Edge WAE へリダイレクトすることができます。

この代行受信およびリダイレクション プロセスは、内容を要求しているクライアントにはまったく見えず、つまり透過的であるため、デスクトップを変更する必要はありません。Edge WAE の動作はネットワークに対して透過的です。WCCP 対応ルータは、リダイレクトされていないトラフィックに対する通常の役割とまったく変わらずに動作します。

Edge WAE は、透過モードで動作している場合は、サーバ名を公開しません。CIFS クライアントは、ブランチ オフィスの IT インフラストラクチャを使用して、CIFS サーバ名を IP アドレス（DNS、WINS）に解決します。クライアントがファイル サーバに接続している場合は、ルータが TCP パケットを代行受信し、WAE にリダイレクトします。WAE は、オリジナルのターゲット サーバの IP アドレスを抽出し、要求を処理します。

Edge WAE によってキャッシュされない CIFS サーバへのクライアント接続は、サポートされています。WCCP 対応ルータに受け入れ / 拒否ターゲット IP リストを設定できます。この設定では、ルータはパケットを Edge WAE へリダイレクトせず、すぐに、その宛先へ転送します。

WAE は、キャッシュされないターゲット サーバ宛ての TCP パケットを受信すると、そのパケットを処理するために、WCCP パケット リターン方式を使用してパケットをルータへ戻します。

（注）　キャッシュされないサーバ（異なるサブネットに常駐するローカル サーバ、またはリモート サーバのどちらか）宛ての大量の CIFS トラフィックが、ブランチ オフィスのルータ経由でルーティングされると予想される場合は、そのルータに受け入れ / 拒否ターゲット IP リストを設定することを推奨します。セントラル オフィスのルータで受け入れ / 拒否ターゲット IP リストを設定すると、ルータとキャッシュの両方の処理が過剰になったために WCCP パケット返信方式が使用されるときに性能が低下する場合があります。

明示的な共有命名を使用した明示的な CIFS クライアント要求の代行受信

Microsoft 社の Distributed File System（DFS; 分散ファイル システム）は、複数のファイル サーバを 1 つのネーム スペースに接続するためのインフラストラクチャを提供します。特に、1 台のファイル サーバを DFS ルートとして動作させ、その他のファイル サーバをそのルート ディレクトリのサブディレクトリとして登録できます。たとえば、メインのファイル サーバ \\main-fs は、ルート ディレクトリ \\main-fs\engineering を持つことができます。そのディレクトリの下に、特定のエンジニアリング グループのファイル サーバ \\eng1\ を \\main-fs\engineering\eng1 としてリンクできます。

クライアントがサブディレクトリ \\main-fs\engineering\eng1 にあるファイルにアクセスを試み、Microsoft DFS によって要求の代行受信が実行されると、次のことが起こります。

1. メインのファイル サーバ（DFS ルート サーバ）が、ここでは、このディレクトリをホスティングしていないと宣言しているクライアントに応答を送信します。
2. その後、クライアントは、このディレクトリをどこから検索できるかを質問するために、Referrer-Request メッセージをメインのファイル サーバへ送信します。
3. メインのファイル サーバは、\\eng1\ から検索できることを応答します。
4. クライアントは \\eng1\ に接続し、指定したファイルを要求します。

WAFS ソフトウェアは、複数のサーバを 1 つのディレクトリ用のサーバ（「レプリカ」とも呼ばれる）として登録できる DFS インフラストラクチャ機能をサポートしています。そのため、レプリカ サーバ間の負荷分散とフェールオーバーが可能です。クライアントが、複数のサーバを保持するディレクトリについて Referrer-Request を送信すると、DFS ルート サーバは、そのクライアントにサーバのリストを提供します。クライアントは、通常、リストの最初のサーバを選択して、そのサーバと通信します。ただし、最初のサーバが到達不能な場合は、2 番めのサーバとの接続を試すといった具合に、到達可能なサーバが見つかるまでリスト順に試行していきます。DFS ルート サーバは、各リストの最初のサーバがそれぞれ異なるレプリカ サーバになっているリストを多数作成し、それらのリストをクライアントに提供することで、レプリカ サーバ間で負荷を分散することができます。

ブランチ オフィスでキャッシュする必要があるネットワーク データセンターのファイル サーバの内容は、DFS ルート サーバにサブディレクトリとして登録されます。ブランチ オフィスのすべての WAE は、DFS ルート サーバのサブディレクトリに対応するレプリカ サーバとして設定されます。クライアントがサブディレクトリ内のファイルへアクセスを試みると、DFS ルート サーバは（Active-Directory 設定を使用して）そのクライアントを、クライアントと同じブランチ オフィスにある WAE へダイレクトします。このリダイレクション方式は、クライアントには透過的です。

Microsoft DFS を使用した CIFS クライアント要求の代行受信

Microsoft DFS を使用すると、WAFS で透過的または非透過的に IFS クライアント要求を代行受信することができます。WAE は、名前の公開を使用するか、WCCP バージョン 2 に依存して CIFS クライアント要求を受信することができます。

WAE で明示的な共有命名を使用するときは、クライアントに透過的ではありません。クライアントには、ファイルにアクセスするためにブランチ オフィス WAE にアクセスするように、明示的に通知されます。具体的には、ブランチ オフィス A のクライアントは、ファイル データにアクセスするために、\\default-prefix-identifying-exported-file-server\file-server-name から共有をマウントするように通知されます。WAFS ソフトウェアでは、管理者は元のファイル サーバを表す任意の名前（プレフィックスだけでなく）を定義できます。たとえば、ユーザがローカル ファイル サーバ LFS1 にアクセスしたあと、そのファイル サーバがデータセンターにグループ化されたとします。集中化された後、データは中央のファイル サーバへ移行されていますが、ユーザは引き続き LFS1 を使用できます。

ブランチ オフィスの WAE は、DNS プロトコルと WINS/NetBIOS プロトコルの両方を使用して、\\WAE-at-the-branch を WAE の IP アドレスに解決します。解決順序は、クライアントのタイプによって異なります。Windows 2000 および XP クライアントは、最初に DNS、次に WINS、その次にブロードキャストを使用してアドレスの解決を試みます。Windows 98 は、逆の順序でアドレスを解決します。DNS を使用してアドレスを解決するには、WAE を \\WAE-at-the-branch として、企業の DNS サーバに登録する必要があります。WAFS ソフトウェアは、スタティック DNS だけをサポートします。WINS/NetBIOS を使用してアドレスを解決する場合は、起動時に、WAE が自分自身を \\WAE-at-the-branch として WINS サーバ（WAE に事前に設定されている）に登録します。WINS サーバが存在せず、DNS が使用できないか、WAE が DNS に登録されていない場合、WAE はクライアントからのブロードキャスト クエリーに応答します。ブロードキャスト方式は、WAE が CIFS クライアント サブネットとの追加インターフェイスに接続しているか、非透過モードで使用される場合のみ動作します。WAE に障害が発生した場合、クライアントは引き続きファイル データへアクセスできるように、自身の設定を変更する必要があります。設定を変更するには、スタートアップ スクリプトを使用します。