CHAPTER 5

ネットワーク設定の構成

この章では、ネットワーク トラフィックをサポートするために追加のネットワーク インターフェイスの作成、DNS サーバの指定、Cisco Discovery Protocol（CDP; シスコ検出プロトコル）の有効化、ファイアウォール トラバースに関する問題を回避するためにピア WAE で UDP カプセル化を使用してトラフィックを交換する directed 動作モードの構成など、基本的なネットワーク設定を構成する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 Wide Area Application Engine（WAE）を総称する用語として「WAAS デバイス」を使用します。WAE という用語は、WAE アプライアンス、WAE ネットワーク モジュール（NME-WAE ファミリのデバイス）、および WAAS を実行する SM-SRE モジュールを指します。

この章の構成は、次のとおりです。

ネットワーク インターフェイスの設定

初期設定時に、初期インターフェイスを選択し、DHCP 用に設定するか、固定 IP アドレスを指定しました。この項では、冗長性、ロード バランシング、およびパフォーマンス最適化用のオプションを使用して、追加のインターフェイスを設定する方法について説明します。

ここでは、次の内容について説明します。

- 「DHCP 用のインターフェイスの設定」（P.5-8）

WAAS CLI でなく、WAAS Central Manager GUI を使用して、ネットワーク設定を構成することを推奨します。ただし、CLI を使用する場合は、『*Cisco Wide Area Application Services Command Reference*』で **interface**、**ip address**、**port-channel**、および **primary-interface** コマンドを参照してください。

（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。半二重接続の場合は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。

スタンバイ インターフェイスの設定

この手順では、「スタンバイ インターフェイス」と呼ばれる論理インターフェイスを設定します。この論理インターフェイス用のパラメータを設定したあとで、物理インターフェイスをスタンバイ インターフェイスに関連付けて、スタンバイ グループを作成する必要があります（スタンバイ グループは、物理インターフェイスから構成されます）。WAAS Central Manager GUI で、物理インターフェイスをスタンバイ グループに参加させ、1 つの物理インターフェイスをプライマリに割り当てることによって、スタンバイ グループを作成します（「プライマリ スタンバイ インターフェイスの設定」（P.5-4）を参照してください）。

スタンバイ インターフェイスは、アクティブなインターフェイスが故障するまで、未使用の状態のままです。アクティブ ネットワーク インターフェイスに障害（ケーブルの問題、レイヤ 2 スイッチの障害、またはその他の障害が原因で）が発生し、そのインターフェイスがスタンバイ グループに属している場合は、スタンバイ インターフェイスがトラフィックを伝送し、障害の生じたインターフェイスの負荷を担うことができます。スタンバイ インターフェイスを設定すると、ある時点でただ 1 つのインターフェイスだけが使用中になります。

スタンバイ インターフェイスを設定するには、各物理インターフェイスをスタンバイ グループに割り当てる必要があります。次の動作に関する考慮事項は、スタンバイ グループに適用されます。

- スタンバイ グループは、物理インターフェイスから構成されます。
- Wide Area Application Service（WAAS）デバイス上のスタンバイ グループの最大数は 1 です。
- スタンバイ グループには、グループのすべてのメンバーが共有する固有のスタンバイ IP アドレスが割り当てられます。
- スタンバイ グループに属するインターフェイスの二重性と速度を設定すると、信頼性が向上します。
- スタンバイ グループに属する物理インターフェイスで、IP ACL を設定できます。
- スタンバイ グループの 1 つのインターフェイスがプライマリ スタンバイ インターフェイスに指定されます。プライマリ インターフェイスだけが、グループ IP アドレスを使用します。
- 使用中のインターフェイスに障害が発生した場合、そのスタンバイ グループにある別のインターフェイスが引き継ぎ、トラフィックを伝送します。
- スタンバイ グループのすべてのメンバーで障害が生じ、その後、1 つが回復した場合、WAAS ソフトウェアは、動作状態のインターフェイスでスタンバイ グループを起動します。
- スタンバイ グループ内のプライマリ インターフェイスは、実行時に変更できます（デフォルトの動作では、異なるインターフェイスがプライマリになった場合、現在使用中インターフェイスが優先的に使用されます）。
- 物理インターフェイスがスタンバイ グループのメンバーである場合、同時にポート チャネルのメンバーになることはできません。

- 1 つの IP アドレスをスタンバイ グループとポート チャネルの両方に割り当てることはできません。1 つの IP アドレスで設定できる仮想インターフェイスは 1 つだけです。
- VLAN タギング プロトコルを使用し、同じ VLAN タグを各インターフェイスに割り当てた場合、スタンバイ グループに属するインターフェイスは異なるスイッチに接続できます。

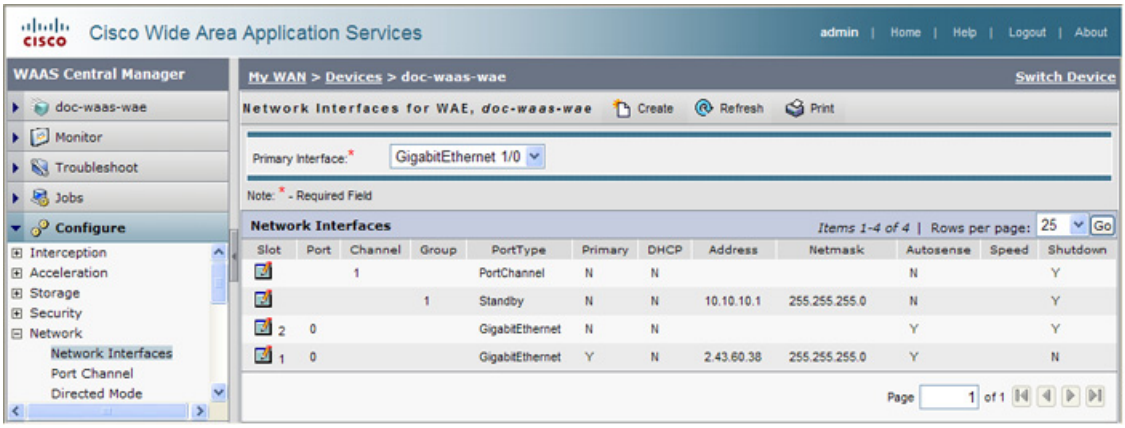
スタンバイ インターフェイスを設定するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices] を選択します。[Devices] ウィンドウが表示されます。

ステップ 2　スタンバイ インターフェイスを設定するデバイスの横にある [Edit] アイコンをクリックします。[Device Dashboard] ウィンドウが表示されます。

ステップ 3　ナビゲーション ペインで、[Configure] > [Network] > [Network Interfaces] を選択します。デバイス用の [Network Interfaces] ウィンドウが表示されます（図 5-1 を参照）。

図 5-1　[Device] ウィンドウのネットワーク インターフェイス



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

ステップ 5　[Port Type] ドロップダウン リストから、[Standby] を選択します。ウィンドウが更新され、スタンバイ グループ設定を構成するためのフィールドが表示されます。

ステップ 6　[Address] フィールドで、スタンバイ グループの IP アドレスを指定します。

ステップ 7　[Netmask] フィールドで、スタンバイ グループのネットマスクを指定します。

ステップ 8　[Shutdown] チェックボックスを選択して、ハードウェア インターフェイスを停止します。このオプションはデフォルトで無効になっています。

ステップ 9　[Gateway] フィールドで、デフォルト ゲートウェイ IP アドレスを入力します。インターフェイスが DHCP 用に設定されている場合、このフィールドは読み取り専用です。

ステップ 10　[Submit] をクリックします。

ステップ 11　「プライマリ スタンバイ インターフェイスの設定」（P.5-4）の説明に従って、インターフェイスの優先順位を設定します。

プライマリ スタンバイ インターフェイスの設定

WAAS Central Manager GUI を使用して論理スタンバイ インターフェイスを設定したあとで、物理インターフェイスをスタンバイ グループに参加させ、1 つの物理インターフェイスをプライマリ スタンバイ インターフェイスに設定することで、スタンバイ グループを設定します。スタンバイ グループのプライマリ インターフェイスは、スタンバイ グループの IP アドレスを使用します。インターフェイスをプライマリに設定する前に、スタンバイ インターフェイス設定されている必要があります（「スタンバイ インターフェイスの設定」（P.5-2）を参照してください）。

インターフェイスをスタンバイ グループに関連付け、プライマリ スタンバイ インターフェイスに設定するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI から、[My WAN] > [Manage Devices] を選択します。[Devices] ウィンドウが表示されます。

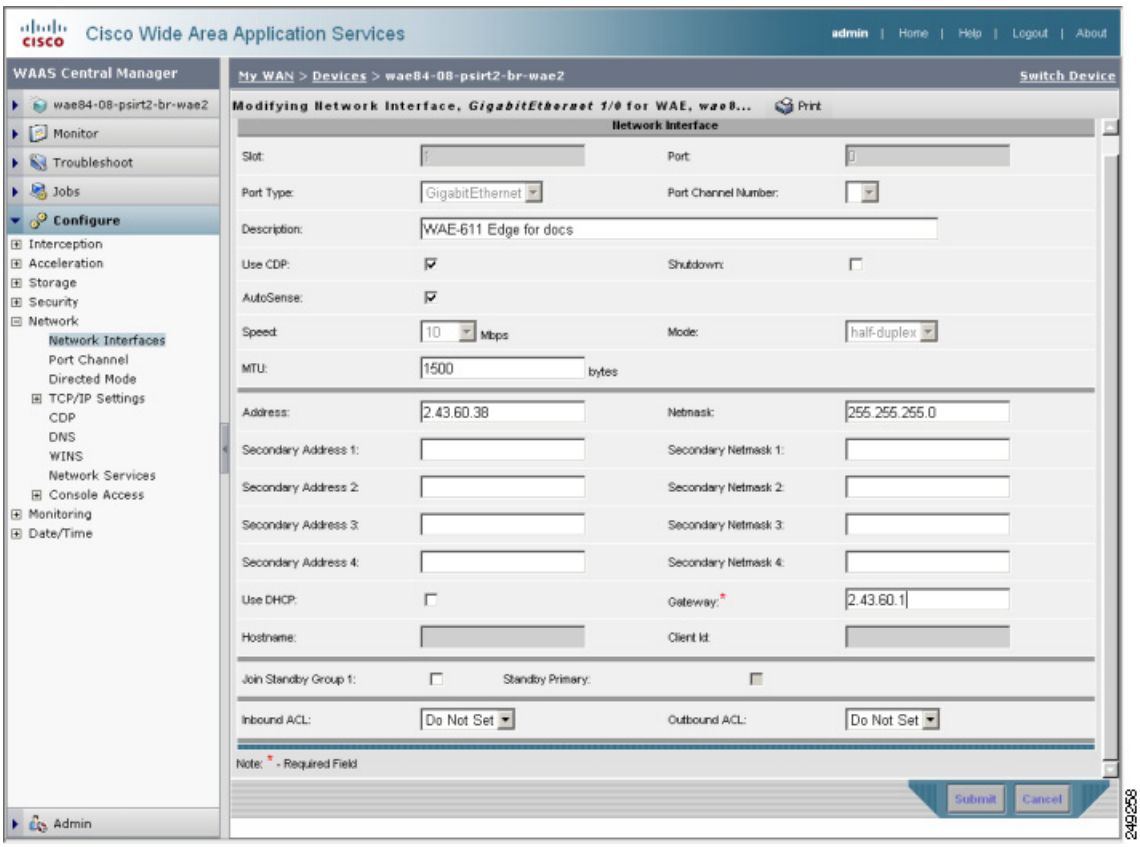
ステップ 2　スタンバイ インターフェイスを設定するデバイスの横にある [Edit] アイコンをクリックします。[Device Dashboard] ウィンドウが表示されます。

ステップ 3　ナビゲーション ペインで、[Configure] > [Network] > [Network Interfaces] を選択します。デバイス用の [Network Interfaces] ウィンドウが表示されます。

ステップ 4　スタンバイ グループに参加させる物理インターフェイスの横にある [Edit] アイコンをクリックします。[Modifying Network Interface] ウィンドウが表示されます（図 5-2 を参照）。

この手順で、論理インターフェイス（スタンバイまたはポート チャネル）を選択しないでください。

図 5-2　[Modifying Network Interface] ウィンドウ



ステップ 5　インターフェイスをスタンバイ グループに参加させ、プライマリ スタンバイ インターフェイスに指定するには、次の手順に従ってください。

a. [Join Standby Group 1] チェックボックスを選択します。

b. （任意）インターフェイスをスタンバイ グループのプライマリ（アクティブ）インターフェイスにする場合は、[Standby Primary] チェックボックスを選択します。

ステップ 6　[Submit] をクリックします。

1 つのインターフェイスへの複数の IP アドレスの設定

1 つのインターフェイスに、最大 4 つのセカンダリ IP アドレスを設定できます。この設定によりデバイスが複数のサブネットに存在でき、データをルータでリダイレクションせずに、WAAS デバイスから、情報を要求するクライアントへ直接転送できるので、デバイスを使用して応答時間を最適化できます。また、WAAS デバイスとクライアントは同じサブネット上に設定されるため、クライアントから WAAS デバイスを認識できます。

1 つのインターフェイスに複数の IP アドレスを設定するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices] を選択します。[Devices] ウィンドウが表示されます。

ステップ 2　インターフェイスを設定するデバイスの横にある [Edit] アイコンをクリックします。[Device Dashboard] ウィンドウが表示されます。

ステップ 3　ナビゲーション ペインで、[Configure] > [Network] > [Network Interfaces] を選択します。[Network Interfaces] リスト ウィンドウが表示されます。

ステップ 4　変更するギガビット イーサネット物理インターフェイス用の [Edit] アイコンをクリックします。[Modifying Network Interface] ウィンドウが表示されます。

（注）　この手順で、論理インターフェイス（スタンバイまたはポート チャネル）を選択しないでください。論理インターフェイスには、複数のインターフェイスを設定できません。

ステップ 5　[Secondary Address] および [Secondary Netmask] フィールド 1 ～ 4 で、インターフェイス用の最大 4 つの IP アドレスとセカンダリ ネットマスクを入力します。

ステップ 6　[Submit] をクリックします。

ギガビット イーサネット インターフェイス設定の変更

既存のギガビット イーサネット インターフェイスの設定を変更するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices] 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　インターフェイス設定を変更するデバイスの横にある [Edit] アイコンをクリックします。

[Device Dashboard] ウィンドウが表示されます。

ステップ 3　ナビゲーション ペインで、[Configure] > [Network] > [Network Interfaces] を選択します。

[Network Interfaces] ウィンドウが表示され、特定のスロットとポートに設定されているネットワーク インターフェイスが表示されます。

（注）　On an NME-WAE デバイスでは、ルータへの内部インターフェイスはスロット 1、ポート 0 に指定され、外部インターフェイスはスロット 2、ポート 0 に指定されます。設定の詳細については、『*Configuring Cisco WAAS Network Modules for Cisco Access Routers*』を参照してください。

ステップ 4　変更するギガビット イーサネット インターフェイスの横にある [Edit Network Interface] アイコンをクリックします。

[Modifying Network Interface] ウィンドウが表示され、特定のスロットとポート上のインターフェイス設定が表示されます（図 5-2 を参照）。

（注）　ウィンドウの一部のフィールドは、使用できません。スロット、ポート、およびポートの種類用のインターフェイス設定は、最初の起動時または WAAS CLI を使用して物理インターフェイス用に設定されます。

（注）　NME-WAE デバイスで内部インターフェイス（GigabitEthernet 1/0）を設定するときは、[Port Channel Number]、[AutoSense]、[Speed]、[Mode]、[Address]、[Netmask]、[Use DHCP]、および [Standby Group] フィールドまたはチェックボックスは変更できません。これらの値を変更して [Submit] をクリックすると、Central Manager はエラーを表示します。内部インターフェイスのこれらの設定は、ホスト ルータ CLI を使用しないと設定できません。詳細については、『*Configuring Cisco WAAS Network Modules for Cisco Access Routers*』を参照してください。

ステップ 5　インターフェイスで CDP を有効にするには、[Use CDP] チェックボックスを選択します。

有効にすると、CDP は、ネイバー デバイスのプロトコル アドレスを取得し、それらのデバイスのプラットフォームを検出します。また、ルータが使用するインターフェイスに関する情報を表示します。

[CDP Settings] ウィンドウから CDP を設定すると、CDP がすべてのインターフェイスでグローバルに有効になります。CDP 設定を構成する方法については、「CDP 設定の構成」（P.5-14）を参照してください。

ステップ 6　[Shutdown] チェックボックスを選択して、ハードウェア インターフェイスを停止します。

ステップ 7　速度とモードを自動ネゴシエーションするようにインターフェイスを設定するには、[AutoSense] チェックボックスを選択します。

このチェックボックスを選択すると、手動の [Speed and Mode] ドロップダウン リスト設定が無効になります。

（注）　自動感知が有効の場合、手動設定が変更されます。自動感知を開始するには、WAAS デバイスをリブートする必要があります。

ステップ 8　インターフェイスの伝送速度設定とモード設定を手動で構成するには、次の手順に従ってください。

a.　[AutoSense] チェックボックスの選択を解除します。

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。

全二重送信では、インターフェイスまたはケーブルを通じて、データを同時に両方の方向に伝送できます。半二重設定では、ある時点でデータが片方の方向だけに伝送されることが保証されます。全二重の方が高速ですが、インターフェイスがこのモードで効果的に動作できない場合があります。過度の衝突やネットワーク エラーが発生する場合は、インターフェイスを全二重でなく、半二重に設定してください。

（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。半二重接続の場合は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　[MTU] フィールドに値（バイト単位）を指定して、インターフェイスの Maximum Transmission Unit（MTU; 最大伝送ユニット）サイズを設定します。

範囲は、88 ～ 1500 バイトです。MTU は、特定のデータ リンク接続を使用して転送できる IP データグラムの最大サイズです。

ステップ 10　[Address] フィールドに新しい IP アドレスを入力して、インターフェイス IP アドレスを変更します。

ステップ 11　[Netmask] フィールドに新しいネットマスクを入力して、インターフェイス ネットマスクを変更します。

ステップ 12　[Submit] をクリックします。

ポート チャネル設定の構成

WAFS ソフトウェアでは、最大 4 個の同じ速度のネットワーク インターフェイスを 1 つの仮想インターフェイスにグループ化することができます。このグループ化機能によって、2 つのギガビット イーサネット インターフェイスから構成される 1 つの仮想インターフェイスを設定または削除することができます。また、この機能は、Cisco ルータ、スイッチ、およびその他のネットワーキング デバイスやホストと相互運用可能で、各インターフェイスの現在のリンク ステータスに基づいて、EtherChannel、ロード バランシング、障害の自動検出と回復をサポートします。EtherChannel は、「ポート チャネル」とも呼びます。

ポート チャネル設定を構成するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices] を選択します。[Devices] ウィンドウが表示されます。

ステップ 2　インターフェイスを設定するデバイスの名前の横にある [Edit] アイコンをクリックします。[Device Dashboard] ウィンドウが表示されます。

ステップ 3　ナビゲーション ペインで、[Configure] > [Network] > [Network Interfaces] を選択します。[Network Interfaces] ウィンドウが表示され、選択したデバイス用のすべてのインターフェイスが表示されます。

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

ステップ 5　[Port Type] ドロップダウン リストから、[Port Channel] を選択します。

ウィンドウが更新され、ネットワーク インターフェイス設定を構成するためのフィールドが表示されます。

ステップ 6　[Port Channel Number] ドロップダウン リストで、ポート チャネル インターフェイス番号 [1] を選択します（サポートされるポート チャネルは 1 つだけです）。

ステップ 7　[Shutdown] チェックボックスを選択して、このインターフェイスを停止します。このオプションはデフォルトで無効になっています。

ステップ 8　[Gateway] フィールドで、デフォルト ゲートウェイ IP アドレスを入力します。

ステップ 9　[Address] フィールドで、インターフェイスの IP アドレスを指定します。

ステップ 10　[Netmask] フィールドで、インターフェイスのネットマスクを指定します。

ステップ 11　（任意）[Inbound ACL] ドロップダウン リストから、着信パケットに適用する IP ACL を選択します。ドロップダウン リストには、システムに設定されているすべての IP ACL が表示されています。

ステップ 12　（任意）[Outbound ACL] ドロップダウン リストから、発信パケットに適用する IP ACL を選択します。

ステップ 13　[Submit] をクリックします。

次の動作に関する考慮事項は、ポート チャネル仮想インターフェイスに適用されます。

- 物理インターフェイスはポート チャネルまたはスタンバイ グループのメンバーになれますが、同時に両方のメンバーになることはできません。
- 1 つの IP アドレスをポート チャネルとスタンバイ グループの両方に割り当てることはできません。1 つの IP アドレスで設定できる仮想インターフェイスは 1 つだけです。

（注）　両方のデバイス インターフェイスがポートチャネル インターフェイスとして設定されている場合は、自動登録を無効にする必要があります。

DHCP 用のインターフェイスの設定

（注）　手動で DHCP 用にインターフェイスを設定する前に、自動登録を無効にする必要があります。

WAAS デバイスは、ネットワーク情報を要求するときに、設定されているクライアント ID とホスト名を DHCP サーバへ送信します。WAAS デバイスが送信しているクライアント ID 情報とホスト名情報を識別し、WAAS デバイスに割り当てられている特定のネットワーク設定を返信するように、DHCP サーバを設定できます。

DHCP 用のインターフェイスを有効にするには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices] を選択します。[Devices] ウィンドウが表示されます。

ステップ 2　インターフェイス設定を行うデバイスの名前の横にある [Edit] アイコンをクリックします。[Device Dashboard] ウィンドウが表示されます。

ステップ 3　ナビゲーション ペインで、[Configure] > [Network] > [Network Interfaces] を選択します。[Network Interfaces] リスト ウィンドウが表示されます。

ステップ 4　変更するギガビット イーサネット物理インターフェイス用の [Edit] アイコンをクリックします。[Modifying Network Interface] ウィンドウが表示されます。

（注）　論理インターフェイスには DHCP を設定できないため、この手順では論理インターフェイス（スタンバイまたはポート チャネル）を選択しないでください。また、内部インターフェイスはホスト ルータ CLI を使用しないと設定できないため、NME-WAE デバイスでは内部インターフェイス（GigabitEthernet 1/0）を選択しないでください。詳細については、『*Configuring Cisco WAAS Network Modules for Cisco Access Routers*』を参照してください。

ステップ 5　ウィンドウを下方向へ移動し、[Use DHCP] チェックボックスを選択します。

このチェックボックスを選択すると、セカンダリ IP アドレスとネットマスクのフィールドが無効になります。

ステップ 6　[Hostname] フィールドで、WAAS デバイスまたは他のデバイスのホスト名を指定します。

ステップ 7　[Client Id] フィールドで、デバイス用に設定されているクライアント ID を指定します。

DHCP サーバは、WAAS デバイスがデバイス用のネットワーク情報を要求するとき、この ID を使用します。

ステップ 8　[Submit] をクリックします。

インターフェイス用のロード バランシング方式の設定

ロード バランシングを設定する前に、「ポート チャネル設定の構成」（P.5-7）の説明に従って、ポート チャネルが設定されていることを確認してください。

ロード バランシングを設定するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices]（または [Manage Device Groups]）を選択します。

ステップ 2　ロード バランシングを設定するポート チャネルを持つ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　ナビゲーション ペインで、[Configure] > [Network] > [Port Channel] を選択します。

ステップ 4　[Load Balancing Method] ドロップダウン リストから、ロード バランシング方式を選択します。

- [round robin]：ラウンド ロビン方式によって、チャネル グループ内のすべてのインターフェイスにトラフィックを均等に分散できます。他のロード バランシング方式を使用すると、イーサネット フレームを送信するときに、（IP アドレスで）特定のインターフェイスを柔軟に選択できます。このオプションは、デフォルトで選択されています。
- [src-dst-ip-port]：分散機能は、送信元および宛先 IP アドレス / ポートの組み合わせに基づいて実行されます。WAAS バージョン 4.1.3 以降が稼動するデバイスでは、dst-ip 方式がこのロード バランシング方式に置き換わりました。

ステップ 5　[Submit] をクリックします。

CLI からロード バランシング方式を設定するには、**port-channel** グローバル コンフィギュレーション コマンドを使用できます。

TCP 設定の構成

クライアントとサーバ間のデータ トランザクションや照会では、ウィンドウとバッファのサイズが重要であるため、TCP スタック パラメータを調整してキャッシュ パフォーマンスを最大化します。

TCP パラメータは複雑であるため、これらのパラメータを調整するときは注意してください。ほとんどすべての環境で、デフォルトの TCP 設定は適切です。TCP 設定の調整は、適切な経験を持ち、TCP の動作を完全に理解しているネットワーク管理者が行ってください。

TCP および IP 設定を構成するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices]（または [Manage Device Groups]）を選択します。

ステップ 2　TCP 設定を構成する WAAS 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。[Device Dashboard] ウィンドウが表示されます。

ステップ 3　ナビゲーション ペインで、[Configure] > [Network] > [TCP/IP Settings] > [TCP/IP] を選択します。[TCP/IP Settings] ウィンドウが表示されます

ステップ 4　TCP 設定に必要な変更を行います。

このウィンドウの各 TCP フィールドの説明については、表 5-1 を参照してください。

ステップ 5　[Submit] をクリックします。

デフォルトまたはデバイス グループ設定を適用したあとでまだ保存されていない変更があると、[Current Settings] 行の横に、「Click Submit to Save」メッセージが赤で表示されます。また、[Reset] をクリックすると、以前の設定に戻すことができます。[Reset] ボタンは、デフォルトまたはグループ設定を適用して現在のデバイス設定を変更し、まだ変更を送信していない場合にだけ表示されます。

表 5-1　TCP 設定

TCP 設定	説明
[TCP General Settings]	
[Enable Explicit Congestion Notification]	データ送信の遅延やパケット損失を軽減します。これにより、RFC 2581 に対応した TCP がサポートされます。このオプションはデフォルトで無効になっています。詳細については、「明示的輻輳通知について」（P.5-11）を参照してください。
[Initial Send Congestion Window Size]	初期の輻輳ウィンドウ サイズの値（セグメント数）。範囲は、1 ～ 10 セグメントです。デフォルトは、2 セグメントです。詳細については、「輻輳ウィンドウ」（P.5-11）を参照してください。
[ReTransmit Time Multiplier]	TCP アルゴリズムが決定する基数を 1 ～ 3 倍して、再送信タイマーの長さを変更するために使用する係数。デフォルトは 1 です。再送信タイマーの長さは変更されません。範囲は、1 ～ 3 です。詳細については、「再送信時間倍率」（P.5-11）を参照してください。 **（注）**　この係数の変更には、注意が必要です。信頼性の高い低速の接続で TCP を使用するときはスループットが向上しますが、信頼性の低いパケット配信環境では変更しないでください。
[Keepalive Probe Count]	接続が失敗と見なされる前に WAAS デバイスが接続を再試行できる回数。範囲は、1 ～ 120 回です。デフォルトは、4 回です。

表 5-1　TCP 設定 （続き）

TCP 設定	説明
[Keepalive Probe Interval]	WAAS デバイスがアイドル状態の接続を開いておく時間の長さ。デフォルトは、75 秒です。
[Keepalive Timeout]	WAAS デバイスが切断する前に接続を開いておく時間の長さ。範囲は、1 ～ 120 秒です。デフォルトは、90 秒です。
[Enable Path MTU Discovery]	さまざまなリンク間の転送パスに沿って許容可能な最大サイズの IP パケットを検出できるようにし、パケット サイズの正しい値を自動的に設定します。このオプションはデフォルトで無効になっています。詳細については、「パス MTU 検出」（P.5-12）を参照してください。

CLI から TCP 設定を構成するには、**tcp** グローバル コンフィギュレーション コマンドを使用できます。

CLI から MTU 検出ユーティリティを有効にするには、**ip path-mtu-discovery enable** グローバル コンフィギュレーション コマンドを使用できます。

ここでは、次の内容について説明します。

明示的輻輳通知について

TCP の Explicit Congestion Notification（ECN; 明示的輻輳通知）機能では、中間のルータが末端のホストに差し迫ったネットワーク輻輳を通知できます。また、この機能は、遅延やパケット損失の影響を受けやすいアプリケーションに関連する TCP セッションのサポートを強化します。ECN に関する主な問題は、ECN の動作に対応するために、ルータと TCP ソフトウェア スタックの両方の動作を変更する必要があることです。

輻輳ウィンドウ

輻輳ウィンドウ（*cwnd*）は、TCP 送信側が、TCP 伝送の受信側から Acknowledgment（ACK; 確認応答）を受信する前に、ネットワークへ送信できるデータ量を制限する TCP 状態変数です。TCP *cwnd* 変数は、TCP 輻輳回避アルゴリズムによって実装されます。輻輳回避アルゴリズムの目的は、送信側がデータのフロー全体の中で使用できるネットワーク容量の増減を自動的に感知して、送信速度を継続的に変更することです。（パケット損失として）輻輳が発生すると、送信速度が引き下げられ、送信側がネットワークの追加容量を継続的に検査しながら次第に引き上げられます。

再送信時間倍率

TCP 送信側は、タイマーを使用して、データ セグメントを送信してから、TCP 伝送の受信側から対応する ACK を受信するまでに経過する時間を測定します。この再送信タイマーがタイムアウトすると、送信側は、（TCP 輻輳制御に関する RFC 規格に従って）送信速度を下げる必要があります。ただし、

送信側は、ネットワーク輻輳に応えて送信速度を下げないため、ネットワークの現在の状態に関する有効な仮定を行うことができません。したがって、必要以上に大量のデータを送信してネットワークが輻輳するのを防止するために、送信側は、1 回の送信当たりの送信速度を 1 セグメントに下げるスロー スタート アルゴリズムを実装します（「TCP スロー スタート」（P.5-12）を参照してください）。

WAAS Central Manager GUI の [Retransmit Time Multiplier] フィールドを使用して、送信側の再送信タイマーを変更できます。再送信時間倍率は、輻輳制御用に使用している TCP アルゴリズム決定に従って、基数の 1 ～ 3 倍の範囲で再送信タイマーの長さを変更します。

再送信タイマーを調整するときは、パフォーマンスと効率に影響することに注意してください。再送信タイマーが短すぎると、送信側は必要以上にネットワークに重複データを送信し、再送信タイマーが長すぎると、送信側は必要以上にアイドル状態に留まり、データのフローが遅くなります。

TCP スロー スタート

スロー スタートは、TCP が使用する 4 つの輻輳制御アルゴリズムの中の 1 つです。スロー スタート アルゴリズムは、ネットワークの容量が不明なときに、TCP セッションの開始時にネットワークに送信するデータ量を制御します。

たとえば、TCP セッションの開始時にネットワークに大量のデータを送信すると、そのほとんどが失われる場合があります。その代わりに、TCP は、最初に控えめな量のデータを送信するので、送信が成功する確率が高くなります。次に、TCP は、ネットワークが輻輳している徴候がない限り、送信するデータ量を増やしてネットワークを検査します。

スロー スタート アルゴリズムは、最初に輻輳ウィンドウ（*cwnd*）変数で決定される速度でパケットを送信します（「輻輳ウィンドウ」（P.5-11）を参照してください）。アルゴリズムは、スロー スタートしきい値（*ssthresh*）変数で設定された制限値に到達するまで、送信速度を上げていきます。*ssthresh* 変数の値は、受信側の最大セグメント サイズ（RMSS）に初期設定されます。ただし、輻輳が発生すると、*ssthresh* 変数は、*cwnd* 変数の現在の値の半分に設定され、ネットワーク輻輳の新しい指標になります。

cwnd 変数の値は、送信側が送信できる最大セグメントのサイズである送信側の最大セグメント サイズ（SMSS）に初期設定されます。送信側は 1 つのデータ セグメントを送信し、輻輳ウィンドウは 1 セグメントのサイズに等しいため一杯になります。次に、送信側は、伝送の受信側からの対応する ACK を待ちます。ACK を受信したら、送信側が、1 SMSS 分だけ *cwnd* 変数の値を大きくすることによって、その輻輳ウィンドウ サイズを増やします。これで、送信側は、輻輳ウィンドウは再び一杯になる前に 2 つのセグメントを送信でき、これらのセグメントに対応する ACK を待ちます。スロー スタート アルゴリズムは、ACK を受信するたびに 1 SMSS だけ *cwnd* 変数の値を増やして、輻輳ウィンドウのサイズを増やしていきます。*cwnd* 変数の値が *ssthresh* 変数の値を超えると、TCP フロー制御アルゴリズムが、スロー スタート アルゴリズムから輻輳回避アルゴリズムへ変化します。

パス MTU 検出

WAAS ソフトウェアは、RFC 1191 に規定された IP パス MTU 検出方式をサポートしています。有効にすると、パス MTU 検出機能は、さまざまなリンク間の転送パスに沿って許容可能な最大サイズの IP パケットを検出し、パケット サイズの正しい値を自動的に設定します。リンクが処理できる最大 MTU を使用することで、送信側デバイスは、送信する必要があるパケットの数を最小限に抑えることができます。

IP パス MTU 検出は、ネットワークでリンクが停止し、別の異なる MTU サイズのリンクを使用しなければならない場合に有用です。また、IP パス MTU 検出は、接続が初めて確立され、送信側が中間に存在するリンクに関する情報を持っていない場合にも有用です。

（注）　IP パス MTU 検出は、送信側デバイスが開始するプロセスです。サーバが IP パス MTU 検出をサポートしていない場合、受信側デバイスには、サーバによって生成されるデータグラムの断片化を避ける手段がありません。

デフォルトで、この機能は無効になっています。この機能を無効にすると、送信側デバイスは、576 バイトかネクストホップ の MTU のどちらか小さい方のパケット サイズを使用します。この機能を有効または無効にしても、既存の接続に影響しません。

固定 IP ルートの設定

WAAS ソフトウェアを使用すると、ネットワークまたはホスト用の固定ルートを設定できます。指定した送信先のすべての IP パケットが、設定されたルートを使用します。

固定 IP ルートを設定するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices]（または [Manage Devices Group]）を選択します。

ステップ 2　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　ナビゲーション ペインで、[Configure] > [Network] > [TCP/IP Settings] > [Static Routes] を選択します。[IP Route Entries] ウィンドウが表示されます。

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

ステップ 5　[Destination Network Address] フィールドに、送信先のネットワーク IP アドレスを入力します。

ステップ 6　[Netmask] フィールドに、送信先ホストのネットマスクを入力します。

ステップ 7　[Gateway's IP Address] フィールドに、ゲートウェイ インターフェイスの IP アドレスを入力します。

ゲートウェイ インターフェイスの IP アドレスは、いずれかのデバイスのネットワーク インターフェイスと同一のネットワークにある必要があります。

ステップ 8　[Submit] をクリックします。

CLI から固定ルートを設定するには、**ip route** グローバル コンフィギュレーション コマンドを使用できます。

IP ルートの集約

各 WAE デバイスに IP ルートを定義して、他の IP ルートが定義されたデバイス グループに所属させることができます。

[IP Route Entries] ウィンドウの [Aggregate Settings] オプション ボタンは、各デバイスの IP ルートを集約する方法を制御します。

- デバイスをそのデバイス自体および所属するデバイス グループに定義されているすべての IP ルートで設定する場合は、[Yes] を選択します
- デバイスをそのデバイス自体に定義されている IP ルートだけに制限する場合は、[No] を選択します。

設定を変更すると次のメッセージが表示されます。「This option will take effect immediately and will affect the device configuration. Do you wish to continue?」。[OK] をクリックして続行します。

CDP 設定の構成

CDP は、すべてのシスコ デバイス上で稼動するデバイス検出プロトコルです。CDP を使用すると、ネットワーク内の各デバイスは、ネットワーク内の他のすべてのデバイスに定期的にメッセージを送信します。すべてのデバイスは、その他のデバイスが送信した定期的なメッセージを受信して、ネイバー デバイスについて学習し、それらのインターフェイスのステータスを判断します。

CDP を使用して、ネットワーク管理アプリケーションは、ネイバー デバイスのデバイス タイプと Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）エージェント アドレスを学習できます。アプリケーションは、ネットワーク内に SNMP クエリーを送信できます。また、CiscoWorks2000 は、起動後に WAAS デバイスが送信した CDP パケットを使用して、WAAS デバイスを検出します。

デバイス関連の作業では、WAAS デバイス プラットフォームの存在、種類、およびバージョンをシステム マネージャに通知できるように、WAAS デバイス プラットフォームが CDP をサポートしている必要があります。

CDP 設定を構成するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices]（または [Manage Device Groups]）を選択します。

ステップ 2　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　ナビゲーション ペインで、[Configure] > [Network] > [CDP] を選択します。[CDP Settings] ウィンドウが表示されます

ステップ 4　[Enable] チェックボックスを選択して、CDP サポートを有効にします。デフォルトで、このオプションは有効になっています。

ステップ 5　[Hold Time] フィールドに、受信側が CDP パケットを保持する時間の長さを指定する時間（秒）を入力します。

範囲は、10 ～ 255 秒です。デフォルトは、180 秒です。

ステップ 6　[Packet Send Rate] フィールドに、CDP アドバタイズメントの間隔（秒）を入力します。

範囲は、5 ～ 254 秒です。デフォルトは、60 秒です。

ステップ 7　[Submit] をクリックします。

CLI から CDP 設定を構成するには、**cdp** グローバル コンフィギュレーション コマンドを使用できます。

DNS サーバの設定

DNS を使用すると、ネットワークは、要求に入っているドメイン名をそれに関連する IP アドレスに変換できます。WAAS デバイスで DNS を設定するには、次の作業を完了する必要があります。

- ネットワークが、要求されたドメイン名を、WAAS デバイスがドメイン名を解決するために使用する必要がある IP アドレスに変換するために使用する、DNS サーバのリストを指定します。
- WAAS デバイスで DNS を有効にします。

WAAS デバイス用の DNS サーバ設定を構成するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices]（または [Manage Device Groups]）を選択します。

ステップ 2　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　ナビゲーション ペインで、[Configure] > [Network] > [DNS] を選択します。[DNS Settings] ウィンドウが表示されます。

ステップ 4　[Local Domain Name] フィールドに、ローカル ドメインの名前を入力します。最大 3 つのローカル ドメイン名を設定できます。リスト内の項目をスペースで区切ります。

ステップ 5　[List of DNS Servers] フィールドに、ネットワークがホスト名を IP アドレスに解決するために使用する DNS サーバのリストを入力します。

最大 3 台の DNS サーバを設定できます。リスト内の項目をスペースで区切ります。

ステップ 6　[Submit] をクリックします。

デフォルトおよびデバイス グループ設定を適用したあとでまだ保存されていない変更があると、[Current Settings] 行の横に、「Click Submit to Save」メッセージが赤色で表示されます。以前のウィンドウ設定に戻すには、[Reset] をクリックします。[Reset] ボタンは、デフォルトまたはグループ設定を適用して現在のデバイス設定を変更し、まだ変更を送信していない場合にだけ表示されます。

CLI から DNS ネーム サーバを設定するには、**ip name-server** グローバル コンフィギュレーション コマンドを使用できます。

Windows ネーム サービスの設定

デバイスまたはデバイス グループ用の Windows ネーム サービスを設定するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices]（または [Manage Device Groups]）を選択します。

ステップ 2　Windows ネーム サービス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　ナビゲーション ペインで、[Configure] > [Network] > [WINS] を選択します。[Windows Name Services Settings] ウィンドウが表示されます。

ステップ 4　[Workgroup or Domain Name] フィールドに、選択したデバイスまたはデバイス グループが存在するワークグループ（またはドメイン）の名前を入力します。

この名前は、127 文字以内の短縮形で入力する必要があります。有効な文字は、英数字、円（¥）、アンダースコア（_）、およびハイフン（-）です。

たとえば、ドメイン名が cisco.com の場合、短縮形は cisco です。

ステップ 5　ワークグループまたはドメインが Windows NT 4 ドメインの場合は、[NT] チェックボックスを選択します。たとえば、ドメイン名が cisco.com の場合、短縮形は cisco です。ワークグループまたはドメインが Windows 2000 または Windows 2003 ドメインの場合は、[NT] チェックボックスを選択しないでください。このオプションはデフォルトで無効になっています。

ステップ 6　[WINS server] フィールドに、Windows Internet Naming Service（WINS）サーバのホスト名または IP アドレスを入力します。

ステップ 7　[Submit] をクリックします。

CLI から Windows ネーム サービスを設定するには、**windows-domain** グローバル コンフィギュレーション コマンドを使用できます。

directed モードの設定

デフォルトでは、WAAS はピア WAE との新規 TCP 接続を透過的に設定します。これにより、WAAS デバイスがトラフィックを最適化しようとする際、ファイアウォール トラバースに関する問題が発生することがあります。WAE デバイスがトラフィックの最適化を阻止するファイアウォールの背後にある場合、ピア WAE への通信に directed モードを使用できます。directed モードでは、ピア WAE に送信されるすべての TCP トラフィックは UDP にカプセル化されるため、ファイアウォールはトラフィックをバイパスするか、トラフィックを検査できます（UDP 検査ルールを追加して）。

2 つの WAE ピア間のすべてのファイアウォールを、ポート 4050 で、またはデフォルト以外のポートが使用されている場合は directed モードに設定されているすべてのカスタム ポートで、UDP トラフィックを通過させるように設定する必要があります。また、directed モードで UDP トラフィックの送信が開始される前に、WAAS 自動ディスカバリ プロセスで TCP オプションが使用されるため、ファイアウォールは TCP オプションを通過させるように設定する必要があります。シスコのファイアウォールは、**ip inspect waas** コマンド（IOS 12.4(11)T2 以降の場合）または **inspect waas** コマンド（FWSM 3.2(1) 以降および PIX 7.2(3) 以降の場合）を使用することで、TCP オプションを許可するように設定できます。

WAN パケットは UDP を使用して WAE 間で直接ルーティングされますが、directed モードをアクティブにしたあと、WAE は LAN から送信されたパケットだけを透過的に代行受信します。

directed モードは、設定可能なすべてのトラフィック代行受信方法で動作します。directed モードでは、WAAS デバイス（または Cisco WAE Inline Network Adapter）をルーティング可能な非 NAT IP アドレスで設定する必要があります。directed モードをインライン モードとともに使用する場合、インターフェイス上で Cisco WAE Inline Network Adapter をルーティング可能 IP アドレスで設定する必要があります。このように設定しないと、トラフィックはブラック ホール化されます。

ピア WAE 接続のどちらかの端の WAE が directed モードに指定されていて、両方の WAE が directed モードをサポートする場合、明示的に directed モードが設定されていなくても、両方の WAE が directed モードを使用します。ピア WAE が directed モードをサポートしていない場合、ピアは最適化されていないトラフィックを通過させ、各 WAE が directed モードの試行に失敗したことを記述したトランザクション ログ エントリを作成します。

directed モード動作は、次の方法で起動できます。

- WAAS Central Manager GUI または CLI で、directed モードを明示的にアクティブにできます。
- ピア WAE が directed モードの使用を要求したときに、directed モードを自動的に起動できます。

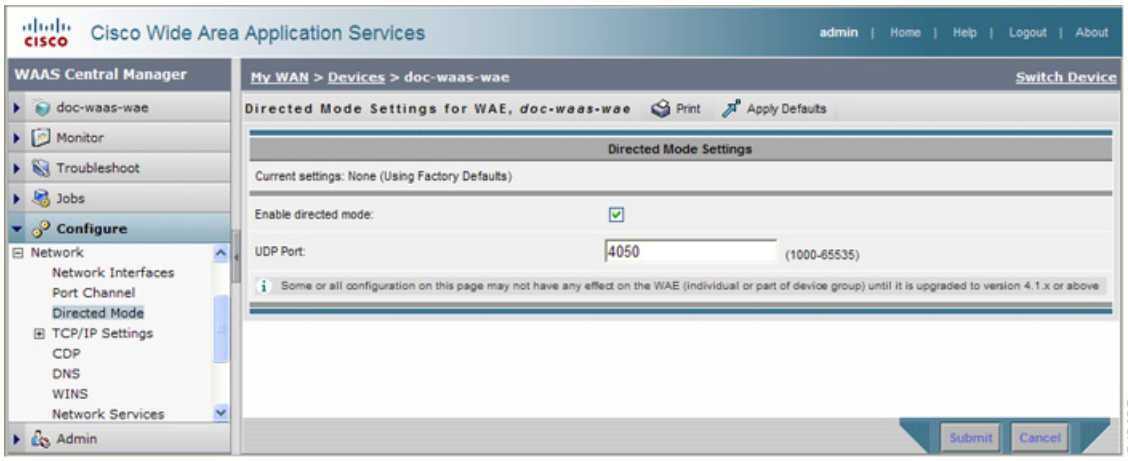
directed モードをアクティブにするには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices]（または [Manage Device Groups]）を選択します。

ステップ 2　directed モードを設定するデバイス（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　ナビゲーション ペインで、[Configure] > [Network] > [Directed Mode] を選択します。[Directed Mode Settings] ウィンドウが表示されます（図 5-3 を参照）。

図 5-3　[Directed Mode Settings] ウィンドウ



ステップ 4　[Enable directed mode] チェックボックスを選択して、directed モードをアクティブにします。

ステップ 5　[UDP Port] フィールドにポート番号を入力して、directed モード用のカスタム UDP ポートを設定します。デフォルトは、ポート 4050 です。

ステップ 6　[Submit] をクリックして、設定を保存します。

CLI から directed モードを設定するには、**directed-mode** グローバル コンフィギュレーション コマンドを使用します。