CHAPTER 5

WCCPv2 の設定

この章では、Cisco NX-OS デバイス上で Web Cache Communication Protocol バージョン 2（WCCPv2）を設定する方法について説明します。

この章では、次の内容について説明します。

WCCPv2 について

WCCPv2 は、1 つ以上の Cisco NX-OS ルータや 1 つ以上のキャッシュ エンジンの間での相互作用を指定します。WCCPv2 は選択されたタイプのトラフィックを、ルータのグループを経由して透過的にリダイレクトします。選択されたトラフィックは、リソースの使用状況の最適化と応答時間の短縮のためキャッシュ エンジンのグループにリダイレクトされます。

Cisco NX-OS では、WCCPv1 はサポートされていません。

ここでは、次の内容について説明します。

WCCPv2 の概要

WCCPv2 により、Cisco NX-OS ルータはパケットを透過的にキャッシュ エンジンにリダイレクトできます。WCCPv2 はルータの通常の動作には影響しません。WCCPv2 を使用すると、ルータは設定済みのインターフェイスでの要求を、目的のホスト サイトではなくキャッシュ エンジンにリダイレクトすることができます。ルータは WCCPv2 によりキャッシュ エンジンのクラスタ（キャッシュ クラスタ）内でトラフィックの負荷を分散し、クラスタのフォールト トレラントでフェール セーフな動作を確保します。キャッシュ クラスタでキャッシュ エンジンの追加や削除を行うと、パケットは WCCPv2 により現在使用可能なキャッシュ エンジンに動的にリダイレクトされます。

WCCPv2 はキャッシュ エンジンでトラフィックを許可し、トラフィックの送信元（クライアント）との接続を確立します。キャッシュ エンジンは元の宛先サーバと同様に機能します。要求されたオブジェクトがキャッシュ エンジン上で使用できない場合、キャッシュ エンジンは、そのオブジェクトを取得するために元の宛先サーバへの独自の接続を確立します。

WCCPv2 はルータとキャッシュ エンジンの間の通信を、UDP ポート 2048 で行います。

WCCPv2 ではキャッシュ クラスタを複数のルータに接続できるため、キャッシュ エンジンが多数のインターフェイスに接続しなければならない場合に冗長性と分散アーキテクチャを実現できます。さらに、WCCPv2 により、すべてのキャッシュ エンジンを同一のクラスタに保持することができます。これにより、複数のクラスタにまたがって Web ページが無駄に重複することがなくなります。

ここでは、次の内容について説明します。

WCCPv2 サービスの種類

サービスとは、ルータが WCCPv2 プロトコルによりキャッシュ エンジンにリダイレクトするよう定義されたトラフィック タイプです。

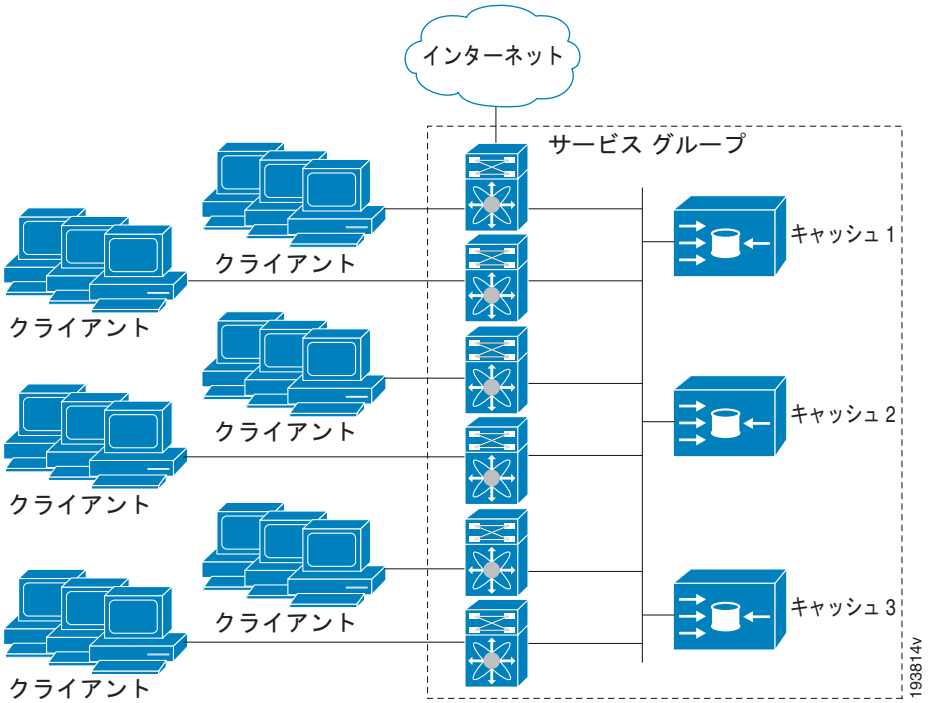
次のいずれかのキャッシュ関連サービスをルータが実行するよう設定することができます。

- Well-known : ルータとキャッシュ エンジンはトラフィック タイプを認識しています（HTTP 用の TCP ポート 80 での Web キャッシュ サービスなど）。
- ダイナミック サービス : ルータにリダイレクトされるトラフィックのタイプがキャッシュ エンジンにより説明されます。

サービス グループ

サービス グループはクラスタ内のキャッシュ エンジンと、そのクラスタに接続していて同じサービスを実行しているルータのサブセットです。図 5-1 にキャッシュ クラスタ内のサービス グループを示します。キャッシュ エンジンとルータは複数のサービス グループの一部となることもできます。

図 5-1　WCCPv2 キャッシュ クラスタおよびサービス グループ



サービス グループはオープンまたはクローズに設定できます。オープン サービス グループは、トラフィックのリダイレクト先のキャッシュ エンジンがない場合、トラフィックをリダイレクトせずに転送します。クローズ サービス グループは、トラフィックのリダイレクト先のキャッシュ エンジンがない場合、トラフィックをドロップします。

サービス グループによって、サービス グループ内の個々のキャッシュ エンジンにリダイレクトされるトラフィックが定義されます。サービス グループ定義には次の項目があります。

- サービス ID（0 ～ 255）
- サービス タイプ
- サービス グループのプライオリティ
- リダイレクトするトラフィックのプロトコル（TCP または UDP）
- サービス フラグ
- 最大 8 件の TCP または UDP ポート番号（すべての発信元ポート番号、またはすべての宛先ポート番号）

サービス グループ リスト

WCCPv2 では、各キャッシュ エンジンがサービス グループ内のすべてのルータを認識している必要があります。各キャッシュ エンジンのグループ内にある各ルータのルータ アドレスのリストを設定できます。

WCCPv2 での設定は次の順序で行います。

ステップ 1　各キャッシュ エンジンにルータのリストを設定します。

ステップ 2　各キャッシュ エンジンはその存在を通知し、通信を確立している相手のすべてのルータのリストを生成します。

ステップ 3　ルータは、ルータが保有しているグループ内のキャッシュ エンジンのビュー（リスト）を返します。

キャッシュ エンジンとルータは制御メッセージを交換します（デフォルトでは 10 秒ごと）。

WCCPv2 代表キャッシュ エンジン

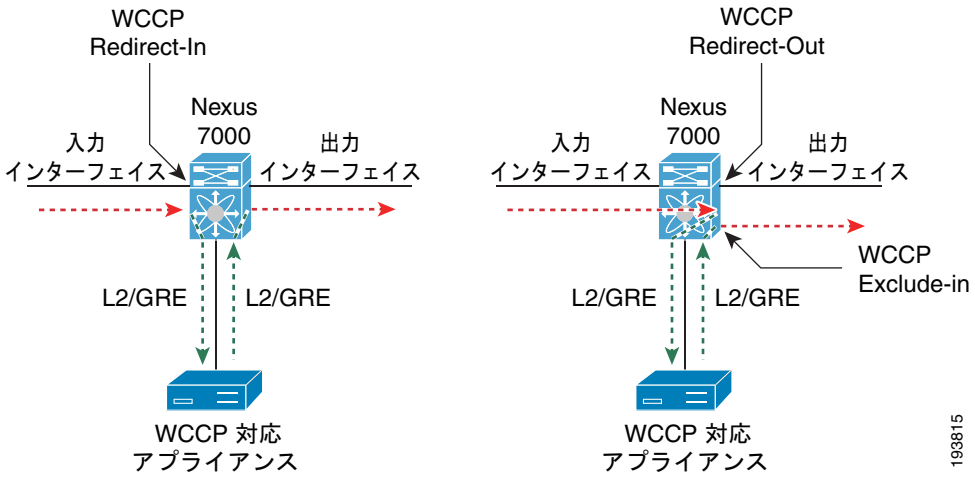
WCCPv2 は 1 つのキャッシュ エンジンを代表として指定します。キャッシュ エンジンのグループが存在する場合、すべてのルータが認識しているキャッシュ エンジンの中で IP アドレスの値が最も小さいものが代表キャッシュ エンジンとなります。代表キャッシュ エンジンはキャッシュ エンジン間でのトラフィックの割り当てを決定します。トラフィックの割り当て方式は代表キャッシュ エンジンからサービス グループ全体に伝達されます。これによりグループ内のルータはパケットをリダイレクトできるようになり、グループ内のキャッシュ エンジンによるトラフィック負荷の管理が向上します。

Cisco NX-OS はマスク方式を使用してトラフィックを割り当てます。代表キャッシュ エンジンは、WCCP リダイレクト割り当てメッセージでマスクおよび値のセットをルータに割り当てます。ルータはこれらのマスクおよび値のセットを各パケットの送信元 IP アドレス、宛先 IP アドレス、送信元ポート、宛先ポートと照合します。割り当てられているマスクおよび値のセットとパケットが一致する場合、ルータはパケットをキャッシュ エンジンにリダイレクトします。割り当てられているマスクおよび値のセットとパケットが一致しない場合、ルータはパケットをリダイレクトせずに転送します。

リダイレクション

IP アクセス リストをリダイレクト リストとして使用し、WCCPv2 でリダイレクトするトラフィックのサブセットを指定できます。このアクセス リストは、インターフェイスの入力トラフィックまたは出力トラフィックに適用できます。図 5-2 に、入力トラフィックまたは出力トラフィックへのリダイレクションの適用を示します。

図 5-2　WCCP リダイレクション



また、インターフェイスの入力トラフィックは除外し、同じインターフェイスの出力リダイレクションは許可することもできます。

WCCPv2 認証

WCCPv2 はデバイスをサービス グループに追加する前に、そのデバイスを認証する必要があります。メッセージ ダイジェスト（MD5）認証により、各 WCCPv2 サービス グループのメンバは秘密キーを使用して発信パケットの一部としてキー付きの MD5 ダイジェスト ストリングを生成することができます。受信側では、着信パケットのキー付きダイジェストが生成されます。生成されたダイジェストが着信パケット内の MD5 ダイジェストと一致しない場合、WCCP はパケットを無視します。

WCCPv2 は次の場合に、パケットを拒否します。

- 認証方式がルータと着信パケットの間で異なっている。
- MD5 ダイジェストがルータと着信パケットの間で異なっている。

リダイレクション方式

WCCPv2 はルータとキャッシュ エンジンの間のパケット リダイレクション方式のネゴシエーションを行います。Cisco NX-OS はこのトラフィック リダイレクション方式をサービス グループ内のすべてのキャッシュ エンジンに使用します。

WCCPv2 は次の転送方式を使用してパケットをリダイレクトします。

- レイヤ 2 宛先 MAC リライト：WCCPv2 はパケットの宛先 MAC アドレスを、パケットの処理に必要なキャッシュ エンジンの MAC アドレスに置き換えます。キャッシュ エンジンとルータは、レイヤ 2 に隣接している必要があります。

また、リダイレクト リストと呼ばれる Access Control List（ACL; アクセス コントロール リスト）を WCCPv2 サービス グループに対して設定できます。この ACL は、パケットに対する WCCPv2 リダイレクション プロセスを許可するか、または WCCP リダイレクションを拒否してパケットを通常のパケット転送プロシージャにより送信することができます。

パケット返送方式

WCCPv2 はパケットのフィルタリングにより、リダイレクトされたパケットのうちキャッシュ エンジンから返送されたものとそうでないものを判別します。WCCPv2 は返送されたパケットをリダイレクトしません。キャッシュ エンジンはこれらのパケットをキャッシュしないよう判断しているためです。WCCPv2 は、キャッシュ エンジンが処理しないパケットを、送信元のルータに返送します。

キャッシュ エンジンがパケットを返送する理由として、次のようなものが考えられます。

- キャッシュ エンジンが過負荷のためパケットを処理できない
- キャッシュ エンジンが特定の条件をフィルタリングしているため、パケットのキャッシングによりパフォーマンス低下が生じる（たとえば、IP 認証がオンになっている場合）。

WCCPv2 はルータとキャッシュ エンジンの間のパケット返送方式のネゴシエーションを行います。Cisco NX-OS はこのトラフィック返送方式をサービス グループ内のすべてのキャッシュ エンジンに使用します。

WCCPv2 は次の転送方式を使用してパケットを返送します。

- 宛先 MAC リライト：WCCPv2 はパケットの宛先 MAC アドレスを、パケットを最初にリダイレクトしたルータの MAC アドレスに置き換えます。キャッシュ エンジンとルータは、レイヤ 2 に隣接している必要があります。

WCCPv2 のハイ アベイラビリティ

WCCPv2 は、ステートフル リスタートおよびステートフル スイッチオーバーをサポートします。ステートフル リスタートは、WCCPv2 が障害を処理してリスタートするときに行われます。ステートフル スイッチオーバーは、アクティブ スーパーバイザがスタンバイ スーパーバイザに切り替わるときに行われます。Cisco NX-OS は実行中の設定をスイッチオーバー後に適用します。

WCCPv2 の仮想化のサポート

WCCPv2 は、仮想ルーティング/転送（VRF）インスタンスをサポートします。VRF は仮想化デバイス コンテキスト（VDC）内にあります。デフォルトでは、特に別の VDC および VRF を設定しない限り、Cisco NX-OS によりデフォルト VDC およびデフォルト VRF が使用されます。

WCCP リダイレクトは VRF 内で発生します。キャッシュ エンジンとの間でやり取りされる転送トラフィックと戻りトラフィックが、同じ VRF の一部であるインターフェイスから発生するように WCCP キャッシュ エンジンを設定する必要があります。

インターフェイス上の WCCP に使用する VRF は、そのインターフェイスで設定されている VRF と一致している必要があります。

インターフェイスの VRF メンバーシップを変更すると、Cisco NX-OS によって WCCPv2 を含め、すべてのレイヤ 3 設定が削除されます。

詳細については、『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide, Release 5.x*』および第 14 章「レイヤ 3 仮想化の設定」を参照してください。

SPM 動作のための WCCPv2 エラー処理

Service Policy Manager（SPM）スーパーバイザ コンポーネントは、WCCP マネージャのデータ パス マネージャとして機能します。WCCP マネージャは、SPM によって基になるプラットフォームの細部から保護されているため、さまざまなプラットフォームに移植できます。WCCP マネージャには、ハードウェアでマッピングおよびプログラミングされている設定を渡すための一連の SPM API があります。これらの API は、単一のハンドラに実装および保持されているアプリケーション データを処理し、解析することができます。

SPM でプログラミングできなかったインターフェイス リダイレクトは、CLI または RA メッセージを通してサービス グループの設定変更が発生するまで保存されます。WCCP マネージャは、以前に失敗したプログラミング ポリシーを再試行します。

WCCP マネージャは、ハードウェアで TCAM エントリをプログラミングする間隔でポリシー更新を SPM に送信します。これらのポリシー更新は、CLI または RA（Redirect-Assign）メッセージで起動できます。WCCP に SPM エラーが通知された場合は、syslog メッセージが表示されます。

設定可能なサービス グループ タイマーのサポート

1 つの WCCP サービス グループには、最大 32 台のルータと 32 のキャッシュ エンジンを含めることができます。キャッシュ エンジンは、WCCP の HIA（Here I Am）メッセージを使用して、そのプロパティをルータに送信します。HIA メッセージは、デフォルトでは 10 秒ごとに送信されます。サービス グループごとに HIA タイマーを設定する必要があります。このタイマーは、そのサービス グループ上のすべてのクライアントの HIA タイムアウトを判定するために使用されます。

WCCPv2 のライセンス要件

次の表に、この機能のライセンス要件を示します。

製品	ライセンス要件
Cisco NX-OS	WCCPv2 にはライセンスは不要です。ライセンス パッケージに含まれていない機能はすべて Cisco NX-OS システム イメージにバンドルされており、追加費用は一切発生しません。Cisco NX-OS のライセンス スキームの詳細については、『*Cisco NX-OS Licensing Guide*』を参照してください。

WCCPv2 の前提条件

WCCPv2 には、次の前提条件があります。

- WCCPv2 機能をグローバルでイネーブルにする必要があります（「WCCPv2 のイネーブル化」（P.5-8）を参照）。
- WCCPv2 の設定はレイヤ 3 または VLAN インターフェイスでのみ可能です（『*Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 6.x*』を参照）。
- VDC を設定するには、Advanced Services ライセンスをインストールし、所定の VDC を開始してください（『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide, Release 5.x*』を参照）。

WCCPv2 の注意事項および制約事項

WCCPv2 の設定時の注意事項および制約事項は、次のとおりです。

- WCCPv2 サービス グループは、最大 32 のルータと 32 のキャッシュ エンジンをサポートします。
- クラスタ内のすべてのキャッシュ エンジンには、その設定に含まれているクラスタにサービスを提供するすべてのルータが含まれている必要があります。クラスタ内のあるキャッシュ エンジンに、その設定に含まれている 1 つ以上のルータが含まれていない場合は、サービス グループによって不整合が検出され、そのキャッシュ エンジンはそのサービス グループ内の動作を許可されません。
- WCCPv2 は IPv4 ネットワークでのみ機能します。
- ポリシーベース ルーティングと WCCPv2 を同じインターフェイスで設定しないでください。
- VDC、インターフェイス VRF メンバーシップ、ポート チャネル メンバーシップを変更した場合、またはポート モードをレイヤ 2 に変更した場合は、Cisco NX-OS によってインターフェイス上のすべてのレイヤ 3 設定が削除されます。

デフォルト設定

表 5-1 に、WCCPv2 パラメータのデフォルト設定値を示します。

表 5-1　デフォルト WCCPv2 パラメータ

パラメータ	デフォルト
認証	認証なし
WCCPv2	ディセーブル

WCCPv2 の設定

WCCPv2 を設定する手順は、次のとおりです。

ステップ 1　WCCPv2 機能をイネーブルにします。「WCCPv2 のイネーブル化」（P.5-8）を参照してください。

ステップ 2　サービス グループを設定します。「WCCPv2 サービス グループの設定」（P.5-9）を参照してください。

ステップ 3　WCCPv2 リダイレクションをインターフェイスに適用します。「インターフェイスへの WCCPv2 リダイレクションの適用」（P.5-10）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。

（注）　Cisco IOS の CLI に慣れている場合、この機能に対応する Cisco NX-OS コマンドは通常使用する Cisco IOS コマンドと異なる場合があるので注意してください。

WCCPv2 のイネーブル化

WCCPv2 を設定するには、その前に WCCPv2 機能をイネーブルにする必要があります。

はじめる前に

正しい VDC を使用していることを確認します（または **switchto vdc** コマンドを使用します）。

手順の詳細

WCCPv2 機能をイネーブルにするには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
feature wccp 例： `switch(config)# feature wccp`	VDC で WCCPv2 機能をイネーブルにします。

VDC で WCCPv2 機能をディセーブルにして、関連付けられている設定をすべて削除するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
no feature wccp 例： switch(config)# no feature wccp	VDC で WCCPv2 機能をディセーブルにして、関連するすべての設定を削除します。

WCCPv2 サービス グループの設定

WCCPv2 サービス グループを設定します。任意で次のように設定できます。

- オープン モードまたはクローズ モード（サービス リストあり）：このサービス グループが処理するトラフィックの種類を制御します。
- WCCPv2 認証：MD5 ダイジェストを使用して WCCPv2 メッセージを認証します。WCCPv2 は認証に失敗したメッセージを破棄します。

（注） WCCPv2 サービス グループのすべてのメンバに同じ認証を設定する必要があります。

- リダイレクション制限：キャッシュ エンジンにリダイレクトされるトラフィックを制御します。

ダイナミック サービス グループのクローズ モードでは、サービス グループで使用されるプロトコルとポートの情報を指定するサービス リスト ACL が必要です。サービス グループ内にメンバが存在しない場合、**service-list** ACL に一致するパケットはドロップされます。

（注） **service-list** キーワード ACL にはプロトコルおよびポートの情報しか格納できません。リダイレクションの対象となるトラフィックを制限するには、**redirect-list** キーワードを使用します。

（注） **ip wccp** コマンドには必要なすべてのパラメータを入力する必要があります。それ以降に **ip wccp** コマンドを入力すると、以前の設定は上書きされます。

はじめる前に

正しい VDC を使用していることを確認します（または **switchto vdc** コマンドを使用します）。

WCCPv2 機能をイネーブルにします（「WCCPv2 のイネーブル化」（P.5-8）を参照）。

手順の詳細

WCCPv2 サービス グループを設定するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的

ip wccp {*service-number* | **web-cache**} [**mode** {**open** [**redirect-list** *acl-name*] | **closed** **service-list** *acl-name*}][**password** [**0**-**7**] *pwstring*]
 	
例：
`switch(config)# ip wccp web-cache`
 	
例：
`switch(config)# ip wccp 10 password Test1 redirect-list httpTest`
	オープンまたはクローズ モード サービス グループを作成します。サービス リストは、サービスに該当するパケットを定義する名前付き拡張 IP アクセス リストを識別します。このリストは、サービスがクローズ モードとして定義されている場合にのみ必要です。*service-access-list* には、大文字と小文字が区別される 64 文字以下の任意の英数字の文字列を使用できます。
	
	オプション パラメータは次のとおりです。
	• **mode**：サービス グループをオープン モードまたはクローズ モードに設定します。デフォルトは open です。クローズ モードでは、このキーワードを使用して、このサービスに該当するトラフィック タイプを定義するための IP アクセス リストを設定します。
	• **password**：サービス グループの MD5 認証を設定します。**password 0** *pwstring* を使用すると、パスワードがクリア テキストで保存されます。**password 7** *pwstring* を使用すると、パスワードが暗号化形式で保存されます。暗号化済みのパスワードには **password 7** キーワードを使用できます。
	• **redirect-list**：サービス グループのグローバル WCCPv2 リダイレクション リストを設定し、キャッシュ エンジンにリダイレクトされるトラフィックを制御します。
	• **service-list**：サービス グループによりリダイレクトされるトラフィックの種類を定義する IP アクセス リストを設定します。
	
	service-number の指定できる範囲は 1 ～ 255 です。*acl-name* には最大 64 文字の英数字を使用できます。大文字と小文字は区別されます。*pwstring* には最大 8 文字の英数字を使用できます。大文字と小文字は区別されます。

インターフェイスへの WCCPv2 リダイレクションの適用

インターフェイスで WCCPv2 リダイレクションを適用するには、インターフェイス コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
ip wccp *service-number* **redirect** {**in** | **out**} 例： switch(config-if)# ip wccp 10 redirect in	WCCPv2 リダイレクションをこのインターフェイスの入力または出力トラフィックに適用します。
ip wccp web-cache redirect {**in** | **out**} 例： switch(config-if)# ip wccp web-cache redirect out	WCCPv2 リダイレクションを、このインターフェイスの入力または出力 Web キャッシュ トラフィックに適用します。
ip wccp redirect exclude in 例： switch(config-if)# ip wccp redirect exclude in	このインターフェイスの WCCP リダイレクションからの入力トラフィックを除外します。

次に、宛先 19.20.2.1 が設定されていない Web 関連のパケットを Web キャッシュにリダイレクトするようルータを設定する例を示します。

```
switch(config)# access-list 100
switch(config-acl)# deny ip any host 192.0.2.1
switch(config-acl)# permit ip any any
switch(config-acl)# exit
switch(config)# ip wccp web-cache redirect-list 100
switch(config)# interface ethernet 2/1
switch(config-if)# ip wccp web-cache redirect out
```

VRF での WCCPv2 の設定

VRF のインターフェイスで WCCPv2 リダイレクションを設定できます。

（注）　WCCPv2 の VRF は、インターフェイスで設定されている VRF と一致する必要があります。

手順の概要

1. **configure terminal**
2. **vrf-context** *vrf-name*
3. **ip wccp** {*service-number* | **web-cache**} [**mode** {**open** [**redirect-list** *acl-name*] | **closed service-list** *acl-name*}]] [**password** [**0**-**7**] *pwstring*]
4. （任意）**show ip wccp** [**vrf** *vrf-name*]
5. （任意）**copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** **例：** switch# configure terminal switch(config)#	コンフィギュレーション モードを開始します。
ステップ 2	**vrf context** *vrf-name* **例：** switch(config)# vrf context Red switch(config-vrf)#	VRF コンフィギュレーション モードを開始します。*vrf-name* には最大 63 文字の英数字を使用できます。大文字と小文字は区別されます。
ステップ 3	**ip wccp** {*service-number* | **web-cache**} [**mode** {**open** [**redirect-list** *acl-name*] | **closed service-list** *acl-name*}][**password** [**0**-**7**] *pwstring*] 例： switch(config-vrf)# ip wccp 10 例： switch(config-vrf)# ip wccp web-cache password Test1 redirect-list httpTest	オープンまたはクローズ モード サービス グループを作成します。サービス リストは、サービスに該当するパケットを定義する名前付き拡張 IP アクセス リストを識別します。このリストは、サービスがクローズ モードとして定義されている場合にのみ必要です。 オプション パラメータは次のとおりです。 • **mode**：サービス グループをオープン モードまたはクローズ モードに設定します。デフォルトは open です。クローズ モードでは、このキーワードを使用して、このサービスに該当するトラフィック タイプを定義するための IP アクセス リストを設定します。 • **password**：サービス グループの MD5 認証を設定します。**password 0** *pwstring* を使用すると、パスワードがクリア テキストで保存されます。**password 7** *pwstring* を使用すると、パスワードが暗号化形式で保存されます。暗号化済みのパスワードには **password 7** キーワードを使用できます。 • **redirect-list**：サービス グループのグローバル WCCPv2 リダイレクション リストを設定し、キャッシュ エンジンにリダイレクトされるトラフィックを制御します。 • **service-list**：サービス グループによりリダイレクトされるトラフィックの種類を定義する IP アクセス リストを設定します。 *service-number* の指定できる範囲は 1 ～ 255 です。*acl-name* には最大 64 文字の英数字を使用できます。大文字と小文字は区別されます。*pwstring* には最大 8 文字の英数字を使用できます。大文字と小文字は区別されます。

	コマンド	目的
ステップ 4	**show ip wccp** [**vrf** *vrf-name*] 例： switch(config-vrf)# show ip wccp vrf Red	（任意）WCCPv2 に関する情報を表示します。 *vrf-name* には最大 64 文字の英数字文字列を指定します。大文字と小文字は区別されます。
ステップ 5	**copy running-config startup-config** **例：** switch(config-vrf)# copy running-config startup-config	（任意）この設定の変更を保存します。

次に、インターフェイス イーサネット 2/1 上で VRF Red で WCCPv2 を設定する例を示します。

```
switch# configure terminal
switch(config)# vrf context Red
switch(config-vrf)# ip wccp web-cache password Test1 redirect-list httpTest
switch(config-vrf)# interface ethernet 2/1
switch(config-if)# vrf member Red
switch(config-if)# ip wccp web-cache redirect out
```

WCCPv2 設定の確認

WCCPv2 設定を表示するには、次のいずれかの作業を行います。

コマンド	目的
show ip wccp [**vrf** *vrf-name*] [*service-number* | **web-cache**]	VRF のすべてのグループ、またはいずれか 1 つのグループの WCCPv2 ステータスを表示します。
show ip interface [*ethernet-number*]	WCCPv2 インターフェイス情報を表示します。
show ip wccp [*service-number* | **web-cache**]	WCCPv2 サービス グループのステータスを表示します。
show ip wccp [*service-number* | **web-cache**] **detail**	WCCPv2 サービス グループのクライアントを表示します。
show ip wccp [*service-number* | **web-cache**] **mask**	WCCPv2 マスクの割り当てを表示します。
show ip wccp [*service-number* | **web-cache**] **service**	WCCPv2 サービス グループの定義を表示します。
show ip wccp [*service-number* | **web-cache**] **view**	WCCPv2 グループ メンバーシップを表示します。

WCCPv2 の統計情報を消去するには、**clear ip wccp** コマンドを使用します。

WCCPv2 の設定例

次に、ルータ上の WCCPv2 認証を、192.0.2.1 の宛先が含まれていない Web 関連のパケットを Web キャッシュにリダイレクトするように設定する例を示します。

```
access-list 100
 deny ip any host 192.0.2.1
 permit ip any any
feature wccp
ip wccp web-cache password 0 Test1 redirect-list 100
interface ethernet 1/2
 ip wccp web-cache redirect out
 no shutdown
```

（注）　IP アクセス リストについては、『*Cisco Nexus 7000 Series NX-OS Security Configuration Guide, Release 6.x*』を参照してください。

その他の関連資料

WCCPv2 の実装に関連する詳細情報については、次の項を参照してください。

- 「関連資料」（P.5-14）
- 「標準」（P.5-14）

関連資料

関連項目	マニュアル名
WCCPv2 CLI コマンド	『*Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference*』

標準

標準	タイトル
この機能でサポートされる新規または改訂された標準規格はありません。また、この機能による既存の標準規格サポートの変更はありません。	—

WCCPv2 機能の履歴

表 5-2 は、この機能のリリースの履歴です。

表 5-2　WCCPv2 機能の履歴

機能名	リリース	機能情報
WCCPv2	6.0(1)	Release 5.2 以降、変更はありません。
WCCPv2	5.2(1)	Release 5.1 以降、変更はありません。
SPM 動作のための WCCPv2 エラー処理	5.1(1)	この機能が導入されました。
WCCPv2	5.0(2)	Release 4.2 以降、変更はありません。
WCCPv2	4.2(1)	この機能が導入されました。