WCCP の設定

このセクションでは、WCCP の設定について説明します。

はじめに

Web Cache Communication Protocol（WCCP）はシスコが開発したコンテンツルーティング テクノロジーです。IP パケットを代行受信し、IP パケットに指定されている宛先とは別の宛先にそのパケットをリダイレクトします。パケットは、インターネット上にある宛先の Web サーバから、クライアントのローカルのコンテンツ エンジンにリダイレクトされるのが一般的です。WCCP の展開シナリオによっては、Web サーバからクライアント方向でもトラフィックをリダイレクトする必要があります。WCCP を使用すると、コンテンツ エンジンをネットワーク インフラストラクチャに統合できます。

このマニュアルの作業では、ネットワークにコンテンツエンジンが設定済みであることを前提にしています。

WCCP の前提条件

- WCCP を使用するには、インターネットに接続されたインターフェイス上で IP を設定する必要があります。また、別のインターフェイスをコンテンツエンジンに接続する必要があります。
- コンテンツエンジンに接続するインターフェイスは、ファストイーサネットインターフェイスまたはギガビット イーサネット インターフェイスにする必要があります。

WCCP に関する制約事項

General

Web キャッシュ通信プロトコルバージョン 2（WCCPv2）には、次の制限が適用されます。

- WCCP は、IPv4 ネットワークだけで動作します。
- シスコエクスプレス フォワーディングをイネーブルにすると、WCCPによってネットワーク アドレス変換（NAT）がバイパスされます。
- WCCP には、ネットワークで同時に設定された NAT およびゾーンベース ファイアウォールとの相互運用性がありません。
- サービスグループは、最大 32 のコンテンツエンジンおよび 32 のスイッチで構成できます。
- マルチキャストクラスタにサービスを提供するスイッチの場合、存続可能時間（TTL）の値を 15 以下に設定する必要があります。
- クラスタのすべてのコンテンツエンジンは、クラスタにサービスを提供するすべてのデバイスと通信できるように設定する必要があります。
- マルチキャスト アドレスは、224.0.0.0 ～ 239.255.255.255 の範囲にする必要があります。
- 同じクライアント インターフェイスで同時に最大 8 個のサービス グループがサポートされます。
- レイヤ2のリライト転送メソッド方式はサポートされますが、Generic Routing Encapsulation（GRE）はサポートされません。
- コンテンツエンジンにレイヤ 2 を直接接続する必要があります。1 ホップまたは複数ホップ離れたレイヤ 3 接続はサポートされません。
- Ternary CAM（TCAM）フレンドリ マスクベースの割り当てはサポートされますが、ハッシュ バケットベースの方式はサポートされません。
- TCAMの空きがなくなると、トラフィックはリダイレクトされず、通常どおりに転送されます。
- WCCP バージョン 2 規格では、最大 256 個のマスクをサポートします。ただし、Cisco Catalyst 9000 シリーズ スイッチは、単一のマスクへのマスク割り当てテーブルのみをサポートします。
- マスク割り当てに設定されているコンテンツエンジンが、割り当て方式としてハッシュが選択されているファームに参加しようとする場合、キャッシュ エンジンの割り当て方式が既存のファームの方式と一致しない限り、ファームに参加できません。

Catalyst 9000 シリーズ スイッチのアクセス制御リスト

WCCPがマスク割り当てを使用している場合、リダイレクトリストはアプライアンスのマスク情報にマージされ、その結果としてマージされた ACL は Catalyst 9000 シリーズ スイッチ ハードウェアに渡されます。リダイレクト リストのプロトコルが IP であるか、サービス グループ プロトコルと完全に一致する場合、その許可 ACL または拒否 ACL のエントリだけが、アプライアンスのマスク情報にマージされます。

次の制約事項がリダイレクト リスト ACL に適用されます。

- ACL は、IPv4 拡張 ACL にする必要があります。
- 個々の発信元または宛先のポート番号だけを指定できます。ポート範囲は指定できません。
- 個々の発信元または宛先のポート番号以外の有効な一致基準は **dscp** と **tos** のみです。
- **fragments**、**time-range**、**options** キーワードや、TCP フラグは使用できません。
- リダイレクト ACL がこれらの制約事項を満たさない場合、次のエラー メッセージがログに記録されます。

```
WCCP-3-BADACE: Service <service group>, invalid access-list entry (seq:<sequence>,
reason:<reason>)
```

WCCP に関する情報

WCCP の概要

WCCP は、Cisco Content Engine（または WCCP を実行する他のコンテンツエンジン）を使用して、ネットワークのトラフィックパターンをローカライズし、ローカルでコンテンツ要求を実行できるようにします。トラフィックのローカライズによって伝送コストを引き下げ、ダウンロード時間を短縮できます。

WCCP によって、Cisco IOS XE プラットフォームはコンテンツ要求を透過的にリダイレクトできます。透過的リダイレクションを使用すると、ユーザは、Web プロキシを使用するようにブラウザを設定せずに、コンテンツ要求をローカルで実行できます。ユーザはターゲット URL を使用してコンテンツを要求できます。また、ユーザの要求はコンテンツエンジンに自動的にリダイレクトされます。この場合の「透過的」とは、エンドユーザが要求したファイル（Web ページなど）が、元々指定していたサーバからではなく、コンテンツエンジンから送信されることをそのユーザが意識しないという意味です。

要求を受信したコンテンツエンジンは、独自のローカルキャッシュからサービスを提供しようとします。要求した情報が存在しない場合、コンテンツ エンジンから独自の要求が元のターゲット サーバに発行され、必要な情報が取得されます。コンテンツエンジンは、要求された情報を取得すると、要求元のクライアントに転送し、以降の要求に対応するためにキャッシュします。その結果、ダウンロードのパフォーマンスが最大になり、送信コストが大幅に削減されます。

WCCPにより、一連のコンテンツエンジン（コンテンツエンジンクラスタと呼ばれる）が1つまたは複数のデバイスにコンテンツを提供できるようになります。ネットワーク管理者は、このようなクラスタ処理機能によって容易にコンテンツエンジンを拡張し、高いトラフィック負荷を管理できます。シスコ クラスタ処理テクノロジーを使用すると、各クラスタ メンバを同時に実行できるため、リニア スケーラビリティが実現します。クラスタ処理コンテンツ エンジンによって、キャッシュ ソリューションのスケーラビリティ、冗長性、および可用性が大幅に改善されます。最大 32 個のコンテンツ エンジンをクラスタ処理し、目的の容量まで拡張できます。

WCCP マスク割り当て

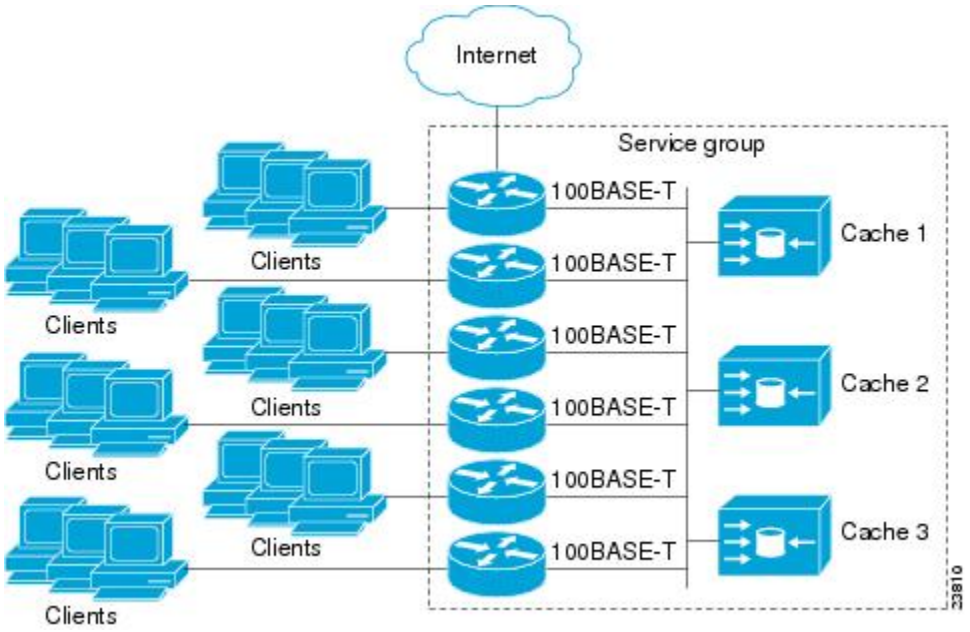
WCCPマスク割り当て機能によって、（デフォルトのハッシュ割り当て方式ではなく）WCCP サービスのロード バランシング方式としてマスク割り当てを使用できます。

Application and Content Networking System（ACNS）ソフトウェアを実行するコンテンツエンジンの場合、**mask-assign** キーワードを指定した **wccp custom-web-cache** コマンドを使用して、マスク割り当てを設定します。Cisco Wide Area Application Services（WAAS）ソフトウェアを実行するコンテンツエンジンの場合、**mask-assign** キーワードを指定した **wccp tcp-promiscuous** コマンドを使用して、マスク割り当てを設定します。

WCCPv2 の設定

複数のデバイスが WCCPv2 を使用して 1 つのコンテンツエンジンクラスタにサービスを提供できます。次の図に、複数のデバイスを使用した設定例を示します。

図 *1 : WCCPv2* を使用した *Cisco* コンテンツ エンジン ネットワーク構成



クラスタ、および同じサービスを実行しているクラスタに接続するデバイス内のコンテンツエンジンのサブセットは、サービスグループと呼ばれます。利用可能なサービスには、TCP および UDP リダイレクションが含まれます。

WCCPv2 の場合、各コンテンツエンジンがサービスグループ内のすべてのデバイスを認識している必要があります。サービスグループ内のすべてのデバイスのアドレスを指定するには、次のいずれかのメソッドを選択する必要があります。

- ユニキャスト：グループ内の各デバイスの IP アドレスリストを、各コンテンツエンジンで設定します。この場合、グループ内の各デバイスのアドレスは、設定の際、コンテンツエンジンごとに明示的に指定する必要があります。
- マルチキャスト：単一のマルチキャストアドレスを各コンテンツエンジンで設定します。マルチキャスト アドレス メソッドの場合、コンテンツエンジンは、サービスグループのすべてのスイッチに提供されるシングルアドレス通知を送信します。たとえば、コンテンツエンジンは、パケットを常にマルチキャストアドレス 224.0.0.100 に送信するように指示できます。その場合、マルチキャストパケットは、WCCP を使用してリッスンしているグループ用に設定されたサービスグループ内のすべてのデバイスに送信されます（詳細については、**ip wccp group-listen** インターフェイス コンフィギュレーション コマンドを参照してください）。

マルチキャスト オプションの場合に必要な操作は、各コンテンツ エンジンで単一のアドレスを指定することだけなので、設定が容易です。このオプションを使用して、サービス グループからルータを動的に追加および削除できます。毎回、異なるアドレス リストを使用してコンテンツ エンジンを再設定する必要はありません。

WCCPv2 での設定は次の順序で行います。

1. 各コンテンツエンジンは、ルータリストを使用して設定されます。
2. 各コンテンツエンジンは、各自の存在と、通信の確立に使用されたすべてのデバイスのリストについて通知します。ルータは、グループ内のコンテンツ エンジンのビュー（リスト）で応答します。
3. そのビューがクラスタ内のすべてのコンテンツエンジンで一貫している場合、1 つのコンテンツエンジンがリードとして指定され、デバイスがパケットのリダイレクト時に展開する必要のあるポリシーが設定されます。

HTTP 以外のサービスの WCCPv2 サポート

WCCPv2 では、さまざまな UDP および TCP トラフィックを含め、HTTP（TCP ポート 80 トラフィック）以外のトラフィックのリダイレクションが可能です。WCCPv2 では他のポート宛てのパケットをリダイレクトできます。たとえば、プロキシ Web キャッシュ処理、ファイル転送プロトコル（FTP）キャッシング、FTP プロキシの処理、80 以外のポートの Web キャッシング、Real Audio、ビデオアプリケーション、およびテレフォニー アプリケーションに使用されるポートなどです。

各種の利用可能なサービスに対応するため、WCCPv2 は複数のサービスグループという概念を導入しました。サービス情報は、ダイナミックサービス識別番号（98 など）または事前定義し

たサービスキーワード（**web-cache** など）を使用して、WCCP コンフィギュレーション コマンドで指定します。この情報は、サービス グループ メンバーが同じサービスを使用または提供していることを確認するために使用されます。

サービス グループのコンテンツ エンジンは、プロトコル（TCP または UDP）によってリダイレクトされるトラフィックと、最大 8 個の発信元ポートまたは宛先ポートを指定します。各サービス グループにはプライオリティ ステータスが割り当てられます。ダイナミック サービスのプライオリティは、コンテンツエンジンによって割り当てられます。プライオリティ値の範囲は、0 ～ 255 です（0 が最も低いプライオリティ）。事前定義した Web キャッシュ サービスには、240 のプライオリティが割り当てられています。

複数デバイスでの WCCPv2 サポート

WCCPv2 では、複数のデバイスをキャッシュエンジンのクラスタに追加できます。サービスグループで複数のデバイスを使用すると、冗長構成、インターフェイスの集約、およびリダイレクトの負荷分散が可能になります。WCCPv2 は、サービスグループごとに最大 32 のデバイスをサポートします。各サービス グループの確立および保守は独立して行われます。

WCCPv2 での MD5 セキュリティ

WCCPv2 には、パスワードとハッシュメッセージ認証コード-メッセージダイジェスト（HMAC MD5）規格を使用して、サービスグループの一部になるスイッチとコンテンツエンジンを制御できる、オプションの認証機能があります。共有秘密キー MD5 ワンタイム認証（**ip wccp password** *password* グローバル コンフィギュレーション コマンドを使用して設定）では、メッセージを代行受信、検査、およびリプレイから保護します。

WCCPv2 での Web キャッシュ パケットのリターン

エラーまたは過負荷のために、コンテンツエンジンが、キャッシュした要求オブジェクトを提供できない場合、コンテンツエンジンは、元々指定されていた宛先サーバに転送するように、要求をデバイスに返します。WCCPv2 には、機能していないコンテンツ エンジンから返送された要求を判断できるパケットのチェック機能があります。デバイスは、この情報を使用して（要求をコンテンツエンジンクラスタに再送信しようとするのではなく）要求を元の宛先サーバに転送できます。このプロセスのエラー処理はクライアントに意識されません。

コンテンツエンジンがパケットを拒否し、パケット返送機能を開始する場合、一般的に次のような理由があります。

- コンテンツ エンジンが過負荷になり、パケットを処理する余裕がなくなった場合
- コンテンツエンジンが、パケットのキャッシング機能が低下する特定の条件についてフィルタリングしている場合（たとえば、IP 認証が有効になった場合）

WCCPv2 での負荷分散

WCCPv2 を使用すると、個々のコンテンツエンジンに割り当てる負荷を調整して、空きリソースを効率的に使用できるようになります。さらに、クライアントに対して高い Quality Of Service（QoS）を確保できます。WCCPv2 を使用すると、指定したコンテンツ エンジンが特定のコンテンツ エンジン上の負荷を調整し、クラスタ内のコンテンツ エンジン全体で負荷を分散できます。WCCPv2 では負荷分散を実行するために、次の 3 つの方法を使用します。

- ホットスポット処理：個々のハッシュバケットをすべてのコンテンツエンジンに分散できます。WCCPv2 の登場までは、1 つのハッシュバケットの情報を転送できるのは、1 つのコンテンツエンジンに対してのみでした。
- ロードバランシング：過負荷のコンテンツエンジンから、空き容量がある他のメンバに負荷を移行するように、コンテンツエンジンに割り当てるハッシュバケットセットを調整できます。
- 負荷制限：コンテンツエンジンの容量を超えないように、スイッチが負荷を選択してリダイレクトできるようにします。

これらのハッシュ処理パラメータを使用すると、コンテンツエンジンの過負荷を防ぎ、障害が発生する可能性を軽減します。

WCCP バイパス パケット

WCCP は IP パケットを代行受信し、IP ヘッダーに指定されている宛先以外の宛先に、そのパケットをリダイレクトします。パケットは、インターネット上にある Web サーバから、宛先のローカルの Web キャッシュにリダイレクトされるのが一般的です。

場合によっては、Web キャッシュでリダイレクトされたパケットを適切に管理できず、パケットを変更せずに元のデバイスに返送することがあります。このようなパケットはバイパスパケットと呼ばれ、カプセル化なしのレイヤ 2 転送（L2）を使用して、発信元のデバイスに返送されます。デバイスはカプセル化を解除し、通常どおりにパケットを転送します。入力インターフェイスと関連付けられている VRF（関連付けられている VRF がない場合はグローバルテーブル）は、パケットを宛先にルーティングするときに使用されます。

WCCP クローズド サービスおよびオープン サービス

パケットを代行受信し、Cisco スイッチまたはルータによって外部 WCCP クライアントデバイスにリダイレクトするアプリケーションの場合、WCCP クライアントデバイスを使用できないと、状況によってはアプリケーションのパケットをブロックする必要があります。このブロックを実行するには、WCCP クローズド サービスを設定します。WCCP サービスがクローズドに設定されている場合、サービスを提供するもののアクティブなクライアントデバイスを持たないパケットは破棄されます。

デフォルトでは、WCCP はオープン サービスとして動作します。この場合、中間デバイスがなくても、クライアントとサーバ間の通信は正常に進行します。

ip wccp service-list コマンドは、クローズドモードとオープンモード両方のサービスに使用できます。アプリケーション プロトコル タイプまたはポート番号を登録するには、**service-list** キーワードと *service-access-list* 引数を使用します。オープンサービスまたはクローズドサービスを選択するには、**mode** キーワードを使用します。

WCCP 発信 ACL チェック

入力インターフェイスで WCCP のリダイレクションが有効になっている場合、パケットは WCCP によってリダイレクトされ、代わりに IP ヘッダーで指定された宛先以外のインターフェイスで出力されます。パケットは、引き続き入力インターフェイスで設定された ACL の影響下にあります。ただし、リダイレクションによって、パケットが元の出力インターフェイスで設定された ACL をバイパスする可能性があります。元の出力インターフェイスで ACL が設定されているためにドロップされたパケットは、リダイレクト出力インターフェイスに送信される場合があります。その結果、セキュリティ上の問題が発生する可能性があります。WCCP アウトバウンド ACL チェック機能を有効にすると、リダイレクトされたパケットは、元の出力インターフェイスで設定された ACL 条件の対象になります。

WCCP サービス グループ

WCCP は、Cisco IOS XE ソフトウェアのコンポーネントで、定義済みの特性を持つトラフィックを元の宛先から代替の宛先へとリダイレクトします。一般的な WCCP アプリケーションには、リモート Web サーバ宛ての発信トラフィックをローカル Web キャッシュにリダイレクトして、応答時間を改善し、ネットワーク リソースの使用状況を最適化する機能があります。

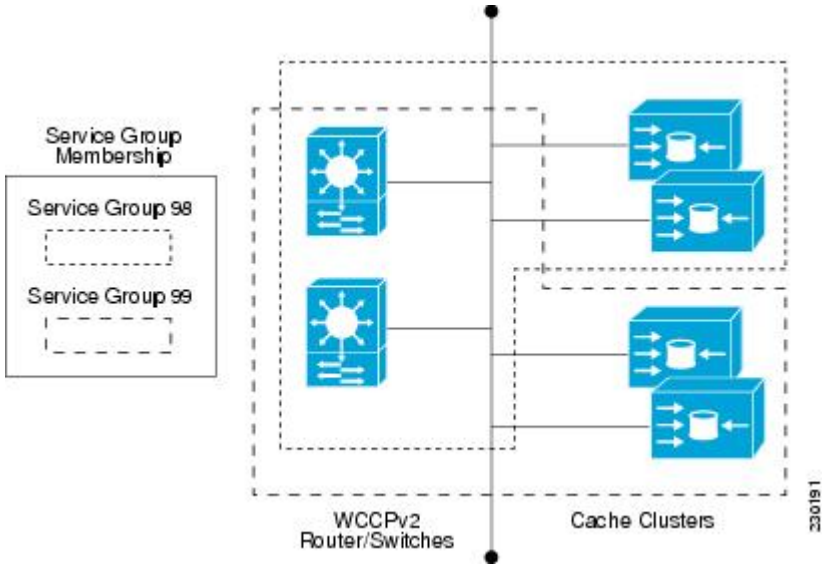
リダイレクトに選択されるトラフィックの性質は、コンテンツエンジンで指定されるサービス グループ（下の図を参照）によって定義され、WCCP を使用してスイッチやルータに伝達されます。

WCCPv2 は、サービスグループごとに最大 32 のスイッチをサポートします。各サービス グループの確立および保守は独立して行われます。

WCCPv2 では、トラフィックの代行受信およびリダイレクションを行うために使用されている論理リダイレクション サービスを基にサービス グループを使用します。標準のサービスは Web キャッシュです。Web キャッシュは TCP ポート 80（HTTP）トラフィックを代行受信し、そのトラフィックをコンテンツ エンジンにリダイレクトします。Web キャッシュ サービスの特徴はスイッチとコンテンツエンジンの両方から認識されているため、このサービスは既知のサービスと呼ばれます。サービスの識別よりも詳細な既知のサービスの説明は必要ありません。標準の Web キャッシュ サービスを指定するには、**ip wccp** コマンドと **web-cache** キーワードを使用します。

（注） スイッチでは同時に複数のサービスが実行できます。また、スイッチとコンテンツエンジンは、同時に複数のサービスグループの一部になることができます。

図 *2 : WCCP* サービス グループ



ダイナミックサービスは、コンテンツエンジンによって定義されます。コンテンツエンジンは、代行受信するプロトコルまたはポート、およびトラフィックの配信方法をスイッチに指示します。ダイナミック サービス グループのトラフィックの特性に関する情報は、スイッチ自体にはありません。この情報は、グループに参加する最初のコンテンツエンジンから提供されるためです。ダイナミック サービスでは、1 つのプロトコルに最大 8 ポートを指定できます。

たとえば、Cisco Content Engine ではダイナミック サービス 99 を使用して、リバース プロキシ サービスを指定します。ただし、他のコンテンツ エンジン デバイスでは、その他のサービスにこのサービス番号を使用する可能性があります。

WCCP：すべてのサービスを確認

インターフェイスは、WCCP サービスを複数使用して設定できます。1 つのインターフェイスに複数の WCCP サービスを設定する場合、サービスの優先順位は、他の設定済みサービスのプライオリティと比較した、そのサービスの相対的なプライオリティによって変わります。各 WCCP サービスには、定義の一部にプライオリティ値があります。複数の WCCP サービスを使用してインターフェイスを設定する場合、パケットの優先順位は、プライオリティ順でサービス グループに対して対応付けられます。

（注） WCCP サービスグループの優先順位は、Cisco IOS XE ソフトウェアで設定できません。

ip wccp check services all コマンドを使用すると、すべての設定済みサービスを一致についてチェックし、必要に応じてそのサービスに関するリダイレクションを実行するように WCCP を設定できます。パケットのリダイレクト先キャッシュは、リダイレクト ACL およびサービスの優先順位で制御できます。複数の WCCP サービスをサポートするには、**ip wccp check services all** コマンドをグローバルレベルで設定する必要があります。

WCCP サービスをリダイレクト ACL を使用して設定する場合、IP パケットに一致するサービスが見つかるまで、プライオリティ順にサービスがチェックされます。パケットに一致するサービスがない場合、パケットはリダイレクトされません。サービスがパケットに一致し、サービスにリダイレクト ACL が設定されている場合、IP パケットは ACL に対してチェックされます。ACL によってパケットが拒否される場合、**ip wccp check services all** コマンドを設定しない限り、低い優先順位のサービスにパケットは渡されません。**ip wccp check services all** コマンドを設定すると、インターフェイスで設定されている残りの低い優先順位のサービスに対して、引き続きパケットのマッチングが試行されます。

WCCP のトラブルシューティングのヒント

WCCP をイネーブルにすると、CPU の使用率が非常に高くなる場合があります。WCCP カウンタを使用すると、直接スイッチでバイパストラフィックを確認できます。また、その原因が WCCP の有効化による CPU の使用率の高さにあるかどうかを示すことができます。場合によっては 10 % のバイパス トラフィックが標準で、他の状況では 10 % が高いこともあります。ただし、25% を超える数値の場合、Web キャッシュの状況をより詳しく調査する必要があります。

バイパス トラフィックのレベルが高いことをカウンタが示している場合、次の手順は、コンテンツ エンジンのバイパス カウンタを確認し、コンテンツ エンジンがトラフィックのバイパスを選択した理由を判定します。さらに詳細に調査するには、コンテンツ エンジン コンソールにログインし、CLI を使用します。カウンタを使用すると、バイパスするトラフィックの割合を決定できます。

特定のサービスに関してデバイスで保持している WCCP 統計情報（カウント）を削除するには、**clear wccp** コマンドを使用します。

すべての WCCP グローバル統計情報（カウント）を表示するには、**show wccp** コマンドを使用します。

WCCP の設定方法

次の設定作業では、ネットワークで使用するコンテンツエンジンのインストールと設定が完了していることを前提としています。クラスタでコンテンツエンジンを設定してから、ルータまたはスイッチの WCCP 機能を設定する必要があります。コンテンツエンジンの設定とセットアップ作業については、『Cisco Cache Engine User Guide』を参照してください。

WCCP の設定

WCCP を設定するには、次の作業を実行します。

ip wccp {**web-cache** | *service-number*} グローバル コンフィギュレーション コマンドを使用して WCCP サービスを設定しない限り、WCCP はデバイスに対して無効です。特定の形式の **ip wccp** コマンドを最初に使用したときに、WCCP が有効になります。

サービスグループのデバイスとコンテンツエンジンのパスワードを設定するには、**ip wccp web-cache password** コマンドを使用します。MD5 パスワードセキュリティの場合、サービスグループのパスワードを使用して、サービスグループに参加させる各デバイスおよびコンテンツエンジンを設定する必要があります。パスワードの長さは、8 文字以下である必要があります。サービスグループの各コンテンツエンジンまたはデバイスは、WCCP メッセージヘッダーの検証後すぐに、受信した WCCP パケットのセキュリティコンポーネントを認証します。認証に失敗したパケットは廃棄されます。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip wccp** {**web-cache** | *service-number*} [**group-address** *multicast-address*] [**redirect-list** *access-list*] [**group-list** *access-list*] [**password** *password* [**0** | **7**]]
4. **interface** *type number*
5. **ip wccp** {**web-cache** | *service-number*} **redirect** {**in** | **out**}
6. **exit**
7. **interface** *type number*
8. **ip wccp redirect exclude in**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip wccp** {**web-cache**	*service-number*} [**group-address** *multicast-address*] [**redirect-list** *access-list*] [**group-list** *access-list*] [**password** *password* [**0**	**7**]] 例： `Device(config)# ip wccp web-cache password pwd`	デバイスで有効にする Web キャッシュまたはダイナミックサービスを指定します。サービスグループで使用する IP マルチキャストアドレスを指定します。使用するアクセスリストを指定します。MD5 認証を使用するかどうかを指定します。WCCP サービスを有効にします。 • （注） パスワードの長さは、8 文字以内にする必要があります。

	コマンドまたはアクション	目的
ステップ 4	**interface** *type number* 例： `Device(config)# interface Gigabitethernet 0/0`	Web キャッシュ サービスを実行するインターフェイス番号を指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	**ip wccp** {**web-cache** | *service-number*} **redirect** {**in** | **out**} 例： `Device(config-if)# ip wccp web-cache redirect in`	WCCP を使用して、発信インターフェイスまたは受信インターフェイスでパケットのリダイレクションをイネーブルにします。 • **out** および **in** キーワードオプションに示されているとおり、発信インターフェイスまたは受信インターフェイスのリダイレクションを指定できます。
ステップ 6	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了します。
ステップ 7	**interface** *type number* 例： `Device(config)# interface GigabitEthernet 0/2/0`	リダイレクトからトラフィックを除外するインターフェイス番号を対象として、インターフェイス コンフィギュレーション モードを開始します。
ステップ 8	**ip wccp redirect exclude in** 例： `Device(config-if)# ip wccp redirect exclude in`	（任意）指定したインターフェイスのトラフィックをリダイレクションから除外します。

クローズド サービスの設定

WCCP 用のサービス グループの数を指定し、クローズド サービスまたはオープン サービスとしてサービス グループを設定し、オプションで全サーバのチェックを指定するには、この作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. 次のいずれかのコマンドを入力します。
   - **ip wccp** *service-number* [**service-list** *service-access-list* **mode** {**open** | **closed**}]
   - または
   - **ip wccp web-cache mode** {**open** | **closed**}

4. **ip wccp check services all**
5. **ip wccp** {**web-cache** | *service-number*}
6. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

ステップ 3	次のいずれかのコマンドを入力します。
	• **ip wccp** *service-number* [**service-list** *service-access-list* **mode** {**open** | **closed**}]
	• または
	• **ip wccp web-cache mode** {**open** | **closed**}
	例：
	`Device(config)# ip wccp 90 service-list 120 mode closed`
	または
	`Device(config)# ip wccp web-cache mode closed`
		ダイナミック WCCP サービスをクローズドまたはオープンとして設定します。
		または
		Web キャッシュ サービスをクローズドまたはオープンとして設定します。
		（注） Web キャッシュ サービスをクローズド サービスとして設定する場合、サービス アクセス リストを指定できません。
		（注） ダイナミック WCCP サービスをクローズド サービスとして設定する場合、サービス アクセス リストを指定する必要があります。

ステップ 4	**ip wccp check services all** 例： `Device(config)# ip wccp check services all`	（任意）WCCP サービスのチェックをイネーブルにします。 • このコマンドを使用すると、一致について他の設定済みサービスをチェックし、必要に応じてそのサービスについてリダイレクションを実行するように WCCP を設定できます。パケットのリダイレクト先キャッシュは、サービス記述だけでなく、リダイレクト ACL によって制御できます。

	コマンドまたはアクション	目的
		（注） **ip wccp check services all** コマンドは、すべてのサービスに適用され、単一のサービスには関連付けられないグローバル WCCP コマンドです。
ステップ 5	**ip wccp** {**web-cache** | *service-number*} 例： `Device(config)# ip wccp 201`	WCCP サービス ID を指定します。 • 標準の Web キャッシュ サービスまたはダイナミック サービス番号（0 ～ 255）を指定できます。 • 指定できるサービスの最大数は 256 です。
ステップ 6	**exit** 例： `Device(config)# exit`	特権 EXEC モードに戻ります。

マルチキャストアドレスへのデバイスの登録

サービスグループにマルチキャストアドレスオプションを使用する場合、デバイスがインターフェイスでマルチキャスト ブロードキャストを待ち受けるように設定する必要があります。

リダイレクトされたトラフィックが仲介デバイスを経由する必要のあるネットワーク設定の場合、経由対象のデバイスは、IPマルチキャストルーティングを実行するように設定する必要があります。仲介デバイスの経由を有効にするには、次の2つのコンポーネントを設定してください。

- **ip multicast-routing** グローバル コンフィギュレーション コマンドを使用して、IP マルチキャストルーティングを有効にします。
- **ip wccp group-listen** インターフェイス コンフィギュレーション コマンドを使用して、キャッシュエンジンの接続先のインターフェイスが、マルチキャストの送信を受信できるようにします。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip multicast-routing** [**vrf** *vrf-name*] [**distributed**]
4. **ip wccp** {**web-cache** | *service-number*} **group-address** *multicast-address*
5. **interface** *type number*
6. **ip pim** {**sparse-mode** | **sparse-dense-mode** | **dense-mode** [**proxy-register** { **list** *access-list* | **route-map** *map-name*}]}
7. **ip wccp** {**web-cache** | *service-number*} **group-listen**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip multicast-routing** [**vrf** *vrf-name*] [**distributed**] 例： `Device(config)# ip multicast-routing`	IP マルチキャスト ルーティングを有効にします。
ステップ 4	**ip wccp** {**web-cache** | *service-number*} **group-address** *multicast-address* 例： `Device(config)# ip wccp 99 group-address 239.1.1.1`	サービス グループのマルチキャスト アドレスを指定します。
ステップ 5	**interface** *type number* 例： `Device(config)# interface ethernet 0/0`	コンテンツ エンジンの接続先インターフェイスが、Web キャッシュ サービスが実行するマルチキャスト送信を受信できるようにし、インターフェイス コンフィギュレーション モードを開始します。
ステップ 6	**ip pim** {**sparse-mode** | **sparse-dense-mode** | **dense-mode** [**proxy-register** { **list** *access-list* | **route-map** *map-name*}]} 例： `Device(config-if)# ip pim dense-mode`	（任意）インターフェイスで Protocol Independent Multicast（PIM）をイネーブルにします。 （注） Catalyst 9000 シリーズ スイッチで **ip wccp group-listen** コマンドを適切に動作させるには、**ip wccp group-listen** コマンドに加えて、**ip pim** コマンドを入力する必要があります。
ステップ 7	**ip wccp** {**web-cache** | *service-number*} **group-listen** 例： `Device(config-if)# ip wccp 99 group-listen`	インターフェイスを設定して、WCCP の IP マルチキャスト パケットの受信をイネーブルまたはディセーブルにします。

WCCP サービス グループのアクセス リストの使用

どのトラフィックをどのコンテンツエンジンに送信するかを決定するためにアクセスリストを使用するようにデバイスを設定するには、次の作業を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**access-list** *access-list-number* **remark** *remark* 例： `Device(config)# access-list 1 remark Give access to user1`	（任意）アクセス リスト エントリに関してユーザにわかりやすいコメントを追加します。 • 最大 100 文字の注釈をアクセス リスト エントリの前または後に指定できます。
ステップ 4	**access-list** *access-list-number* **permit** {*source* [*source-wildcard*] | **any**} [**log**] 例： `Device(config)# access-list 1 permit 172.16.5.22 0.0.0.0`	キャッシュエンジンへのトラフィックリダイレクトを有効または無効にし、送信元アドレスとワイルドカードマスクに基づいて指定された送信元を許可するアクセスリストを作成します。 • すべてのアクセス リストには、1 つ以上の許可文が必要です。許可文は、最初のエントリである必要はありません。 • 標準 IP アクセス リストには、1 ～ 99 または 1300 ～ 1999 の番号を付けます。 • *source-wildcard* を省略すると、0.0.0.0 というワイルドカードマスクが想定されます（つまり、すべての送信元アドレスに一致します）。 • 必要に応じて、*source source-wildcard* の代わりに、キーワード **any** を使用して、送信元と 0.0.0.0 255.255.255.255 の送信元ワイルドカードを指定できます。 • この例では、ホスト 172.16.5.22 がアクセス リストに合格できます。

	コマンドまたはアクション	目的
ステップ 5	**access-list** *access-list-number* **remark** *remark* 例： `Device(config)# access-list 1 remark Give access to user1`	（任意）アクセス リスト エントリに関してユーザにわかりやすいコメントを追加します。 • 最大 100 文字の注釈をアクセス リスト エントリの前または後に指定できます。
ステップ 6	**access-list** *access-list-number* **deny** {*source* [*source-wildcard*] | **any**} | [**log**] 例： `Device(config)# access-list 1 deny 172.16.7.34 0.0.0.0`	送信元アドレスおよびワイルドカードマスクに基づいて、指定した送信元を拒否します。 • *source-wildcard* を省略すると、0.0.0.0 というワイルドカードマスクが想定されます（つまり、すべての送信元アドレスに一致します）。 • 必要に応じて、*source source-wildcard* の代わりに省略形 any を使用すると、送信元と 0.0.0.0 255.255.255.255 の送信元ワイルドカードを指定できます。 • この例では、ホスト 172.16.7.34 はアクセス リストへの合格が拒否されます。
ステップ 7	アクセス リストの基礎とする送信元の指定が完了するまで、ステップ 3 ～ 6 の手順を繰り返します。	明示的に許可されていないすべての送信元は、アクセス リストの末尾にある暗黙的な **deny** ステートメントで拒否されます。
ステップ 8	**ip wccp web-cache group-list** *access-list* 例： `Device(config) ip wccp web-cache group-list 1`	パケットを受け入れるコンテンツエンジンの IP アドレスをデバイスに示します。
ステップ 9	**ip wccp web-cache redirect-list** *access-list* 例： `Device(config)# ip wccp web-cache redirect-list 1`	（任意）特定のクライアントのキャッシングをディセーブルにします。

WCCP 発信 ACL チェックのイネーブル化

（注） ハードウェアですべてのリダイレクションを実行する場合、発信 ACL チェック処理をイネーブルにすると、リダイレクションのモードは変わります。ショートカットをインストールする前に、追加の ACL チェックがソフトウェアで実行できるように、最初のパケットは切り替えられます。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip wccp** {**web-cache** | *service-number*} [**group-address** *multicast-address*] [**redirect-list** *access-list*] [**group-list** *access-list*] [**password** *password*]
4. **ip wccp check acl outbound**
5. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip wccp** {**web-cache**	*service-number*} [**group-address** *multicast-address*] [**redirect-list** *access-list*] [**group-list** *access-list*] [**password** *password*] 例： `Device(config)# ip wccp web-cache`	Cisco Content Engine のサービス グループまたはコンテンツ エンジンのサービス グループのサポートをイネーブルにし、リダイレクト ACL リストまたはグループ ACL を設定します。 （注） **web-cache** キーワードは WCCP バージョン 1 とバージョン 2 に使用することができ、*service-number* 引数は WCCP バージョン 2 のみに使用できます。
ステップ 4	**ip wccp check acl outbound** 例： `Device(config)# ip wccp check acl outbound`	WCCP によってリダイレクトされたパケットの出力インターフェイスのアクセスコントロールリスト（ACL）をチェックします。
ステップ 5	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーションを終了します。

WCCP 設定の確認およびモニタリング

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**show ip wccp** [**web-cache** |*service-number*] [**detail view**] 例： `Device# show ip wccp 24 detail`	WCCP に関連するグローバル情報を表示します。たとえば、実行されているプロトコル バージョン、ルータ サービス グループのコンテンツ エンジンの数、ルータに接続できるコンテンツエンジン グループ、使用するアクセス リストなどです。 • *service-number*：（任意）コンテンツエンジンで制御される Web キャッシュサービスグループのダイナミック番号。有効な範囲は 0 ～ 99 です。Cisco Content Engine を使用する Web キャッシュの場合、逆プロキシ サービスは 99 の値で示されます。 • **web-cache**：（任意）Web キャッシュサービスの統計情報。 • **detail**：（任意）検出済み、または検出されていない特定のサービスグループまたは Web キャッシュの他のメンバ。 • **view**：（任意）ルータまたはすべての Web キャッシュに関する情報。
ステップ 3	**show ip interface** 例： `Device# show ip interface`	「Web Cache Redirect is enabled / disabled」など、いずれかの **ip wccp redirection** コマンドがインターフェイスで設定されているかどうかに関するステータスを表示します。
ステップ 4	**more system:running-config** 例： `Device# more system:running-config`	（任意）実行されている構成ファイルのコンテンツを表示します（**show running-config** コマンドと同じです）。

WCCP の設定例

例：一般的な WCCPv2 セッションの設定

```
Device# configure terminal
Device(config)# ip wccp web-cache group-address 224.1.1.100 password password
Device(config)# ip wccp source-interface GigabitEthernet 0/1/0
Device(config)# ip wccp check services all
! Configures a check of all WCCP services.
Device(config)# interface GigabitEthernet 0/1/0
Device(config-if)# ip wccp web-cache redirect in
Device(config-if)# exit
Device(config)# interface GigabitEthernet 0/2/0
Device(config-if)# ip wccp redirect exclude in
Device(config-if)# exit
```

例：デバイスとコンテンツエンジンのパスワードの設定

```
Device# configure terminal
Device(config)# ip wccp web-cache password password1
```

例：Web キャッシュ サービスの設定

```
Device# configure terminal
Device(config)# ip wccp web-cache
Device(config)# interface GigabitEthernet 0/1/0
Device(config-if)# ip wccp web-cache redirect in
Device(config-if)# exit
Device# copy running-config startup-config
```

次に、ギガビットインターフェイス 0/1/0 に到達する HTTP トラフィックのリダイレクションを有効にするセッションの設定例を示します。

```
Device# configure terminal
Device(config)# interface GigabitEthernet 0/1/0
Device(config-if)# ip wccp web-cache redirect in
Device(config-if)# exit
Device# show ip interface GigabitEthernet 0/1/0
.
.
.
WCCP Redirect inbound is enabled
WCCP Redirect exclude is disabled
.
.
.
```

例：逆プロキシ サービスの実行

次の例では、Cisco Cache Engine を使用してサービス グループを設定し、ダイナミック サービス 99 を使用して逆プロキシ サービスを実行しているという前提です。

```
Device# configure terminal
Device(config)# ip wccp 99
Device(config)# interface gigabitethernet 0/1/0
Device(config-if)# ip wccp 99 redirect out
```

例：マルチキャストアドレスへのデバイスの登録

```
Device# configure terminal
Device(config)# ip wccp web-cache group-address 224.1.1.100
Device(config)# interface gigabitethernet 0/1/0
Device(config-if)# ip wccp web-cache group-listen
```

次に、マルチキャストアドレス 224.1.1.1 を使用してリバースプロキシサービスを実行するようにデバイスを設定する例を示します。リダイレクションは、ギガビットイーサネットインターフェイス 0/1/0 経由で送信されるパケットに適用されます。

```
Device# configure terminal
Device(config)# ip wccp 99 group-address 224.1.1.1
Device(config)# interface gigabitethernet 0/1/0
Device(config-if)# ip wccp 99 redirect out
```

例：アクセス リストの使用

セキュリティを改善するには、標準のアクセスリストを使用して、現在のデバイスに登録するコンテンツエンジンで有効なアドレスがどの IP アドレスかをデバイスに通知します。次に、サンプル ホストのアクセス リスト番号が 10 である標準的なアクセス リストの設定セッション例を示します。

```
Device(config)# access-list 10 permit host 10.1.1.1
Device(config)# access-list 10 permit host 10.1.1.2
Device(config)# access-list 10 permit host 10.1.1.3
Device(config)# ip wccp web-cache group-list 10
```

特定のクライアント、サーバ、またはクライアント/サーバ ペアに対してキャッシングをディセーブルにするには、WCCP アクセス リストを使用します。次に、10.1.1.1 から 10.3.1.1 に送信される要求がキャッシュをバイパスし、その他すべての要求は通常どおりに処理される例を示します。

```
Device(config)# ip wccp web-cache redirect-list 120
Device(config)# access-list 120 deny tcp host 10.1.1.1 any
Device(config)# access-list 120 deny tcp any host 10.3.1.1
Device(config)# access-list 120 permit ip any any
```

次の例では、ギガビットイーサネット 0/1/0 を介して受信した Web 関連のパケットを、209.165.200.224 以外の任意のホストにリダイレクトするようにデバイスを設定します。

```
Device(config)# access-list 100 deny ip any host 209.165.200.224
Device(config)# access-list 100 permit ip any any
Device(config)# ip wccp web-cache redirect-list 100
Device(config)# interface gigabitethernet 0/1/0
Device(config-if)# ip wccp web-cache redirect in
```

例：WCCP 発信 ACL チェックの設定

次に、ネットワーク 10.0.0.0 からのトラフィックがギガビットイーサネットインターフェイス 0/1/0 を離れないようにアクセスリストを設定する例を示します。発信 ACL チェックはイネーブルなので、WCCP はそのトラフィックをリダイレクトしません。WCCP は、パケットのリダイレクト前に、ACL に対してパケットをチェックします。

```
Device(config)# ip wccp web-cache
Device(config)# ip wccp check acl outbound
Device(config)# interface gigabitethernet 0/1/0
Device(config-if)# ip access-group 10 out
Device(config-if)# exit
Device(config)# ip wccp web-cache redirect-list redirect-out
Device(config)# access-list 10 deny 10.0.0.0 0.255.255.255
Device(config)# access-list 10 permit any
```

発信 ACL チェックをディセーブルにする場合、ネットワーク 10.0.0.0 からの HTTP パケットを Web キャッシュにリダイレクトします。そのネットワークアドレスを使用するユーザは、ネットワーク管理者が回避しようとしても、Web ページを取得できます。

例：WCCP 設定の確認

次に、特権 EXEC モードで **more system:running-config** コマンドを使用して設定の変更を検証する例を示します。次に、Web キャッシュサービスおよびダイナミックサービス 99 の両方をデバイスで有効にする例を示します。

```
Device# more system:running-config

 Building configuration...
 Current configuration:
 !
 version 12.0
 service timestamps debug uptime
 service timestamps log uptime
 no service password-encryption
 service udp-small-servers
 service tcp-small-servers
 !
 hostname router4
 !
 enable secret 5 $1$nSVy$faliJsVQXVPW.KuCxZNTh1
 enable password password1
 !
 ip subnet-zero
 ip wccp web-cache
 ip wccp 99
 ip domain-name cisco.com
 ip name-server 10.1.1.1
```

```
ip name-server 10.1.1.2
ip name-server 10.1.1.3
!
!
!
interface GigabitEthernet0/1/1
ip address 10.3.1.2 255.255.255.0
no ip directed-broadcast
ip wccp web-cache redirect in
ip wccp 99 redirect in
no ip route-cache
no ip mroute-cache
!
interface GigabitEthernet0/1/0
ip address 10.4.1.1 255.255.255.0
no ip directed-broadcast
ip wccp 99 redirect in
no ip route-cache
no ip mroute-cache
!
interface Serial0
no ip address
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
shutdown
!
interface Serial1
no ip address
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
shutdown
!
ip default-gateway 10.3.1.1
ip classless
ip route 0.0.0.0 0.0.0.0 10.3.1.1
no ip http server
!
!
!
line con 0
transport input none
line aux 0
transport input all
line vty 0 4
password password1
login
!
end
```

次に、WCCP に関連したグローバル統計情報を表示する方法の例を示します。

```
Device# show ip wccp web-cache detail

WCCP Client information:
WCCP Client ID:      10.1.1.2
Protocol Version:    2.0
State:               Usable
Redirection:         L2
Packet Return:       L2
Packets Redirected:  0
Connect Time:        00:20:34
Assignment:          MASK
```

```
Mask  SrcAddr    DstAddr    SrcPort DstPort
----  -------    -------    ------- -------
0000: 0x00000000 0x00001741 0x0000  0x0000
Value SrcAddr    DstAddr   SrcPort DstPort CE-IP
----- -------    -------   ------- ------- -----
0000: 0x00000000 0x00000000 0x0000 0x0000 0x3C010102 (10.1.1.2)
0001: 0x00000000 0x00000001 0x0000 0x0000 0x3C010102 (10.1.1.2)
0002: 0x00000000 0x00000040 0x0000 0x0000 0x3C010102 (10.1.1.2)
0003: 0x00000000 0x00000041 0x0000 0x0000 0x3C010102 (10.1.1.2)
0004: 0x00000000 0x00000100 0x0000 0x0000 0x3C010102 (10.1.1.2)
0005: 0x00000000 0x00000101 0x0000 0x0000 0x3C010102 (10.1.1.2)
0006: 0x00000000 0x00000140 0x0000 0x0000 0x3C010102 (10.1.1.2)
```

show ip wccp web-cache コマンドの詳細については、『*Cisco IOS IP Application Services Command Reference*』を参照してください。

WCCP の機能情報

表 *1 : WCCP* の機能情報

機能名	リリース	機能情報
Cisco Catalyst 9400 シリーズ スイッチでの WCCP サポート	Cisco IOS XE Everest 16.6.1	Web Cache Communication Protocol（WCCP）はシスコが開発したコンテンツルーティングテクノロジーです。IP パケットを代行受信し、IP パケットに指定されている宛先とは別の宛先にそのパケットをリダイレクトします。 WCCP を使用すると、コンテンツエンジンをネットワーク インフラストラクチャに統合できます。 .