WCCP の設定

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。

Cisco IOS Release 12.1 以降では、WCCP version 1（WCCPv1）または version 2（WCCPv2）を使用できます。

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。Cisco Content Engine および WCCP に関連するハードウェアおよびネットワークの計画の詳細については、次の URL にある Cisco Content Engine のマニュアルを参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/webscale/content/index.htm

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。この章に記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「WCCP の機能情報」（P.29）を参照してください。

プラットフォーム サポートとシスコ ソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

この章の構成

WCCP の前提条件

- WCCP を使用するには、インターネットに接続しているインターフェイスに IP を設定し、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

一般

次の制約事項が WCCPv1 および WCCPv2 に適用されます。

- WCCP は、IPv4 ネットワークの場合だけ機能します。

WCCPv1

次の制約事項が WCCPv1 に適用されます。

- WCCPv1 は HTTP（TCP ポート 80）トラフィックのリダイレクションだけをサポートします。
- WCCPv1 では、複数のルータをコンテンツ エンジンのクラスタに接続できません。

WCCPv2

次の制約事項が WCCPv2 に適用されます。

- WCCP は、IPv4 ネットワークの場合だけ機能します。
- マルチキャスト クラスタにサービスを提供するルータの場合、Time To Live（TTL; 存続可能時間）値を 15 以下に設定する必要があります。
- サービス グループは、最大 32 個のコンテンツ エンジンおよび 32 個のルータで構成できます。
- 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ルータ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。

WCCP VRF のサポート

Cisco IOS Release 12.2(33)SRE では、この機能が Cisco 7200 NPE-G2 ルータと Cisco 7304-NPE-G100 ルータ上でのみサポートされます。

レイヤ 2 フォワーディングおよび返送

次の制約事項が WCCP および WCCP レイヤ 2 フォワーディングおよび返送に適用されます。

- レイヤ 2 リダイレクションの場合、各 WCCP ルータ上のインターフェイスにコンテンツ エンジンを直接接続する必要があります。マルチキャスト IP アドレスを使用しない場合、コンテンツ エンジンの WCCP 設定は、WCCP ルータの直接接続されているインターフェイスの IP アドレスを常に参照します。WCCP ルータに設定されているループバック IP アドレスまたは他の IP アドレスは参照されません。

Cisco ASR 1000 シリーズ集約サービス ルータ

- Cisco ASR 1000 シリーズ集約サービス ルータは、WCCPv1 をサポートしません。
- 通過パケットは、6-Rack-Unit（6RU）と 13RU シャーシ上で Forwarding Processor（FP）フェールオーバーが発生したときに失われます。
- 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ルータと通信できるように設定する必要があります。
- WCCP サービスのロード バランシング方式としてのハッシュ割り当ては、サポートされません。Cisco IOS XE Release 3.1S 以降では、HASH 割り当てを送信するクライアントがルータによってオンラインになることはできません。Cisco ASR 1000 ルータ上で **show ip wccp 61 detail** コマンドを発行すると、Hash が互換性のない割り当て手段であることが表示されます。
- **show ip wccp** コマンドを使用すると、ソフトウェアベース（プロセス、ファスト、およびシスコ エクスプレス フォワーディング（CEF））の WCCP パケットの転送に関する情報が表示されます。Cisco ASR 1000 は、CEF またはプロセススイッチング パスではなく、ハードウェア内に WCCP が実装されています。そのため、**show ip wccp** コマンドを入力すると、パケット カウントは 0 になります。**show platform software wccp interface counters** コマンドまたは **show platform software wccp counters** コマンドを使用して、Cisco ASR 1000 上の WCCP に関するグローバル統計情報を表示します。

  Cisco IOS-XE Release 3.1S で **show ip wccp** コマンドを発行すると、リダイレクトされた WCCP パケットが表示されます。
- 発信インターフェイス上での WCCP パケットのリダイレクトは、XE Release 3.1S よりも前の XE リリースでサポートされていません。

Cisco Catalyst 4500 シリーズ スイッチ

次の制約事項が Cisco Catalyst 4500 シリーズ スイッチに適用されます。

- Catalyst 4500 シリーズ スイッチは WCCPv1 をサポートしません。
- 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（L2）のリライト フォワーディング方式はサポートされますが、Generic Route 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（L2）を直接接続する必要があります。1 つまたは複数ホップ離れたレイヤ 3（L3）接続はサポートされません。
- Ternary Content Addressable Memory（TCAM; Ternary CAM）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。
- クライアント インターフェイス上の WCCP に関するリダイレクト Access Control List（ACL; アクセス コントロール リスト）はサポートされません。
- インターフェイス上の受信トラフィックのリダイレクションはサポートされますが、発信トラフィックのリダイレクション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、Catalyst 4500 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だけをサポートします。

Cisco Catalyst 6500 シリーズ スイッチ

次の制約事項が Cisco Catalyst 6500 シリーズ スイッチに適用されます。

- Policy Feature Card 2（PFC2; ポリシー フィーチャ カード 2）が搭載されているため、リリース 12.2(17d)SXB 以降のリリースは WCCP をサポートします。
- PFC3 が搭載されているため、リリース 12.2(18)SXD1 以降のリリースは WCCP をサポートします。

- WCCP レイヤ 2 PFC リダイレクション機能を使用するには、この章の説明に従って Catalyst 6500 シリーズ スイッチ で WCCP を設定します。また、次の URL で参照できる「*Transparent Caching*」に従って、キャッシュ エンジンで加速 WCCP を設定します。

  http://www.cisco.com/en/US/docs/app_ntwk_services/waas/acns/v42/configuration/guide/transprt.html

- Cisco Application and Content Networking System（ACNS）ソフトウェア リリース 4.2.2 よりも後のリリースは、WCCP レイヤ 2 ポリシー フィーチャ カード（PFC）のリダイレクション ハードウェア アクセラレーションをサポートします。
- 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。
- サービス グループのフォワーディング方式として WCCP レイヤ 2 PFC リダイレクションを使用する場合、**show ip wccp** *service-number* コマンド出力のパケット カウンタには、パケット カウントではなく、フロー カウントが表示されます。

Catalyst 6500 シリーズ スイッチおよび Cisco 7600 シリーズ ルータのアクセス コントロール 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結合され、結果の結合されたアクセス コントロール リスト（ACL）は、Catalyst 6500 シリーズ スイッチまたは Cisco 7600 シリーズ ルータ ハードウェアに渡されます。

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 簡易または拡張 ACL にする必要があります。
- プロトコルは、IP、UDP、または TCP 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のほかに、唯一の有効なマッチング条件は、**dscp** または **tos** です。
- **fragments**、**time-range**、**options**、または TCP フラグは使用できません。

リダイレクト ACL が上記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 はパケットのリダイレクトを継続しますが、アクセス リストが調整されるまで、ソフトウェアでリダイレクションが実行されます（NetFlow スイッチング）。

WCCP の概要

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 Web トラフィック パターンをローカライズします。それによって、ローカルでコンテンツ要求を実行できます。トラフィックのローカライズによって、送信コストとダウンロード時間が削減されます。

WCCP によって、Cisco IOS ルーティング プラットフォームは、透過的にコンテンツ要求をリダイレクトできるようになります。透過的リダイレクションの主な利点は、Web プロキシを使用するためにユーザがブラウザを設定する必要がないことです。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。

コンテンツ エンジンでは、要求の受信時に、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。そのため、ダウンロードのパフォーマンスが大きく向上し、送信コストが大幅に削減されます。

WCCP によって、コンテンツ エンジン クラスタと呼ばれる一連のコンテンツ エンジンは、1 つまたは複数のルータ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。

レイヤ 2 フォワーディング、リダイレクション、および返送

WCCP は、Generic Routing Encapsulation（GRE）またはレイヤ 2（L2）を使用して、IP トラフィックをリダイレクトまたは返送します。WCCP が GRE を介してトラフィックを転送すると、リダイレクトされたパケットは GRE ヘッダー内でカプセル化されます。また、このパケットには WCCP リダイレクト ヘッダーも含まれます。WCCP が L2 を使用してトラフィックを転送すると、IP パケットの元の MAC ヘッダーは上書きされ、WCCP クライアントの MAC ヘッダーで置換されます。

フォワーディング方式として L2 を使用すると、以降の検索を行わずに、コンテンツ エンジンに直接転送できます。レイヤ 2 リダイレクションには、ルータおよびコンテンツ エンジンが直接接続されている（つまり同じ IP サブネット上にある）必要があります。

WCCP が GRE を介してトラフィックを返送すると、返送されたパケットは GRE ヘッダー内でカプセル化されます。宛先 IP アドレスはルータのアドレスで、発信元アドレスは WCCP クライアントのアドレスです。WCCP が L2 を介してトラフィックを返送すると、元の IP パケットは、ヘッダー情報を追加せずに返送されます。パケットの返送先ルータは、パケットの発信元を認識し、リダイレクションを回避します。

WCCP リダイレクション方式は、返送方式と一致する必要はありません。

L2 フォワーディング、返送、またはリダイレクションは、一般的にハードウェア アクセラレーション プラットフォームに使用します。Cisco IOS Release 12.4(20)T 以降のリリースでは、L2 フォワーディング、返送、およびリダイレクトをソフトウェア スイッチング プラットフォームにも使用できます。

Cisco ASR 1000 シリーズ集約サービス ルータでは、GRE および L2 両方のフォワーディング / 返送方式にハードウェアが使用されるため、大幅なパフォーマンスの低下はありません。

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、**l2-redirect** キーワードを指定した **wccp custom-web-cache** コマンドを使用して、L2 リダイレクションを設定します。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、**l2-redirect** キーワードを指定した **wccp tcp-promiscuous** コマンドを使用して、L2 リダイレクションを設定します。

Cisco Content Engine の設定に使用する Cisco ACNS コマンドの詳細については、次の URL の『*Cisco ACNS Software Command Reference*, Release 5.5.13』を参照してください。

http://www.cisco.com/en/US/docs/app_ntwk_services/waas/acns/v55_13/command/reference/5513cref.html

Cisco Content Engine の設定に使用する WAAS コマンドの詳細については、次の URL の『*Cisco Wide Area Application Services Command Reference (Software Versions 4.2.1)*』を参照してください。

http://www.cisco.com/en/US/docs/app_ntwk_services/waas/waas/v421/command/reference/cmdref.html

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。

Cisco Content Engine の設定に使用する Cisco ACNS コマンドの詳細については、次の URL の『*Cisco ACNS Software Command Reference*, Release 5.5.13』を参照してください。

http://www.cisco.com/en/US/docs/app_ntwk_services/waas/acns/v55_13/command/reference/5513cref.html

Cisco Content Engine の設定に使用する WAAS コマンドの詳細については、次の URL の『*Cisco Wide Area Application Services Command Reference (Software Versions 4.2.1)*』を参照してください。

http://www.cisco.com/en/US/docs/app_ntwk_services/waas/waas/v421/command/reference/cmdref.html

ハードウェア アクセラレーション

Catalyst 4500 シリーズ スイッチには、直接接続された Cisco Content Engine 用にハードウェア アクセラレーション機能があります。

Catalyst 6500 シリーズ スイッチおよび Cisco 7600 シリーズ ルータには、WCCP レイヤ 2 ポリシー フィーチャ カード（PFC）リダイレクション ハードウェア アクセラレーション機能があります。互換性のあるスイッチまたはルータに直接接続する場合、ハードウェア アクセラレーションを使用すると、Cisco Content Engine では L2 MAC アドレスのリライト リダイレクション方式を実行できます。

スイッチングまたはルーティング ハードウェアの場合、リダイレクション プロセスは加速されます。これは、Generic Routing Encapsulation（GRE）を使用した L3 リダイレクションよりも効率的です。L2 リダイレクションはスイッチまたはルータで実行され、マルチレイヤ スイッチ フィーチャ カード（MSFC）からは不可視です。WCCP L2 PFC リダイレクション機能には、MSFC での設定は必要ありません。**show ip wccp** {*service-number* | **web-cache**} **detail** コマンドを使用すると、各コンテンツ エンジンで現在使用されているリダイレクション方式が表示されます。

ルータまたはスイッチでハードウェア リダイレクションを最大限に活用するためには、「レイヤ 2 フォワーディング、リダイレクション、および返送」（P.5）を参照して、L2 リダイレクションおよびマスク割り当てを使用してコンテンツ エンジンを設定する必要があります。

L2 リダイレクションおよびマスク割り当てを強制するには、ハードウェアベースのプラットフォームで **ip wccp web-cache accelerated** コマンドを使用します。このコマンドを使用すると、アプライアンスが L2 およびマスク割り当て用に設定されている場合にだけ、サービス グループを構成し、パケットをリダイレクトするようにルータが設定されます。

次の注意事項が WCCP レイヤ 2 PFC リダイレクションに適用されます。

- WCCP レイヤ 2 PFC リダイレクション機能によって、IP フロー マスクは full-flow モードに設定されます。
- Cisco Cache Engine ソフトウェア リリース 2.2 以降のリリースを設定して、WCCP レイヤ 2 PFC リダイレクション機能を使用できます。
- L2 リダイレクションは PFC で実行され、MSFC からは不可視です。MSFC で **show ip wccp** {*service-number* | **web-cache**} **detail** コマンドを使用すると、L2 リダイレクト フローの最初のパケットだけに関する統計情報が表示されます。この情報から、L2 リダイレクションを使用しているフロー数（パケット数ではない）がわかります。**show mls entries** コマンドを入力すると、L2 リダイレクト フローの他のパケットが表示されます。PFC3 には、GRE 用のハードウェア アクセラレーション機能があります。GRE とともに WCCP レイヤ 3 リダイレクションを使用する場合、カプセル化にはハードウェア サポートがありますが、PFC3 での、WCCP GRE トラフィックの非カプセル化にはハードウェア サポートがありません。

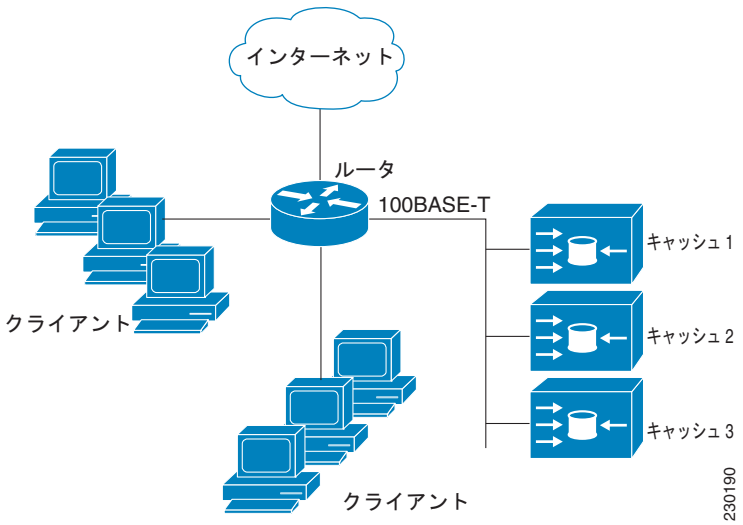
Cisco ASR 1000 シリーズ集約サービス ルータ

Cisco ASR 1000 シリーズ集約サービス ルータの WCCP 実装は、デフォルトでハードウェア アクセラレーションです。ハードウェア アクセラレーションをイネーブルにするために、Cisco ASR ルータで **ip wccp web-cache accelerated** コマンドを設定する必要はありません。

WCCPv1 の設定

WCCPv1 の場合、1 つのクラスタにサービスを提供できるのは 1 つのルータだけです。このシナリオでは、このルータがすべての IP パケット リダイレクションを実行するデバイスです。図 1 に、WCCPv1 の設定を示します。

図 1　　WCCPv1 の設定



コンテンツ エンジンで、コンテンツは重複しません。コンテンツ エンジンを複数使用する利点は、複数の物理コンテンツ エンジンをクラスタ処理して 1 つの論理キャッシュのように見せることで、キャッシング ソリューションを拡張できることです。

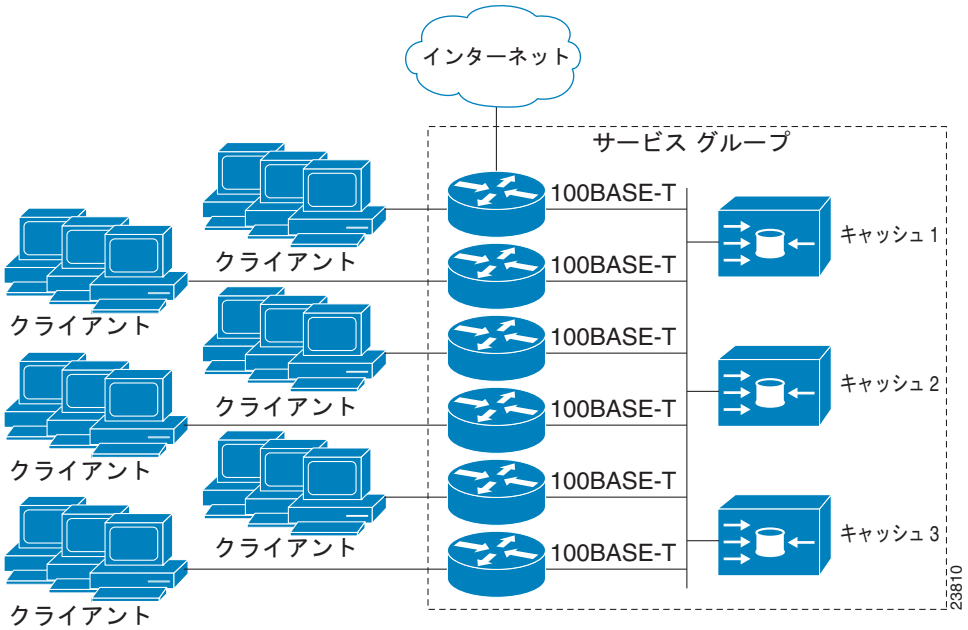
次の一連のイベントで、WCCPv1 設定の動作の詳細について説明します。

1. 各コンテンツ エンジンは、制御ルータの IP アドレスを使用してシステム管理者が設定します。最大 32 個のコンテンツ エンジンを単一の制御ルータに接続できます。
2. コンテンツ エンジンは、WCCP を使用して自身の IP アドレスを制御ルータに送信して、プレゼンスを示します。ルータおよびコンテンツ エンジンは、制御チャネルを介して相互に通信します。このチャネルは、UDP ポート 2048 に基づいています。
3. この情報は、制御ルータがクラスタ ビュー（クラスタ内のキャッシュ リスト）を作成するときに使用されます。このビューはクラスタ内の各コンテンツ エンジンに送信され、基本的にすべてのコンテンツ エンジンが相互を認識するようになります。クラスタのメンバシップが変化せずに一定の時間が経過すると、安定したビューが確立します。
4. 安定したビューが確立すると、リード コンテンツ エンジンとして 1 つのコンテンツ エンジンが選択されます（リードとは、IP アドレスが最も低いクラスタですべてのコンテンツ エンジンから見えるコンテンツ エンジンのことです）。このリード コンテンツ エンジンでは、WCCP を使用して、IP パケット リダイレクションの実行方法を制御ルータに示します。具体的には、リード コンテンツ エンジンは、リダイレクトされるトラフィックをクラスタのコンテンツ エンジン全体に分散する方法を指定します。

WCCPv2 の設定

複数のルータが 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。この設定は WCCPv1 と対照的です。WCCPv1 では、1 つのルータだけがコンテンツ要求をクラスタにリダイレクトできます。図 2 に、複数のルータを使用する設定例を示します。

図 2　　WCCPv2 を使用する Cisco Cache Engine のネットワーク設定



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ルータ内のコンテンツ 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。使用できるサービスには、TCP および User Datagram Protocol（UDP; ユーザ データグラム プロトコル）リダイレクションなどがあります。

WCCPv1 では、単一ルータのアドレスを使用して、コンテンツ エンジンが設定されました。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ルータを認識する必要があります。サービス グループ内のすべてのルータのアドレスを指定するには、次のいずれかの方式を選択できます。

- ユニキャスト：グループ内の各ルータのルータ 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、グループ内の各ルータのアドレスは、設定時に各コンテンツ エンジンについて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 アドレス方式の場合、コンテンツ エンジンは、サービス グループのすべてのルータに提供するシングル 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 に送信するように示すことができます。それによって、マルチキャスト パケットは、WCCP を使用してリ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ルータに送信されます（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。

次の一連のイベントで、WCCPv2 設定の動作の詳細について説明します。

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します。
2. 各コンテンツ エンジンはプレゼンスと、通信の確立に使用されたすべてのルータ リストをアナウンスします。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 エンジンをリードとして指定し、ルータがパケットのリダイレクト時に展開する必要があるポリシーを設定します。

HTTP 以外のサービスのサポート

WCCPv2 では、多様な UDP および TCP トラフィックなど、HTTP（TCP ポート 80 トラフィック）以外のトラフィックをリダイレクトできます。WCCPv1 は HTTP（TCP ポート 80）トラフィックのリダイレクションだけをサポートしていました。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、File Transfer Protocol（FTP; ファイル転送プロトコル）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。

使用可能な多様な種類のサービスに対応するために、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 メンバがすべて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ています。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。

複数ルータのサポート

WCCPv2 では、複数のルータをキャッシュ エンジンのクラスタに接続できます。1 つのサービス グループでルータを複数使用すると、冗長化、インターフェイスの集約、リダイレクション負荷の分散ができます。WCCPv2 は、サービス グループごとに最大 32 個のルータをサポートします。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。

MD5 セキュリティ

WCCPv2 には、パスワードと HMAC MD5 規格を使用して、サービス グループの一部になるルータとコンテンツ 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。共有シークレット MD5 ワンタイム認証（**ip wccp** [**password** [**0** | **7**] *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）を使用すれば、傍受、検査、およびリプレイからメッセージを保護することができます。

Web キャッシュ パケット返送

コンテンツ エンジンが、エラーまたは過負荷のために、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前方転送するように、要求をルータに返送します。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。ルータ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）

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 つの技術を使用しています。

- 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 よりも前のリリースでは、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 エンジンに対してだけでした。
- 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、ルータ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 VRF のサポート

WCCP VRF サポート機能は、Virtual Routing and Forwarding（VRF）のサポートを実装することで、既存の WCCPv2 プロトコルを強化します。

WCCP VRF サポート機能を使用すると、グローバル定義に加え、VRF ベースでサービス グループを設定できます。

サービス ID の他に、ルータに到着する WCCP プロトコル パケットの VRF が、設定されたサービス グループにキャッシュ エンジンを関連付けるために使用されます。

リダイレクトが適用されたインターフェイス、キャッシュ エンジンに接続されたインターフェイス、およびリダイレクトされなかったパケットが残されるインターフェイスを 1 つの VRF に含める必要があります。

Cisco IOS Release 12.2(33)SRE では、この機能が Cisco 7200 NPE-G2 ルータと Cisco 7304-NPE-G100 ルータ上でのみサポートされます。

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ルータ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 フォワーディング（L2）を使用して、または Generic Routing Encapsulation（GRE）でカプセル化して、発信元のルータに返送されます。ルータはカプセル化を解除し、通常どおり、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。

GRE はシスコが開発したトンネリング プロトコルで、IP トンネル内部でさまざまなプロトコルから派生したパケット タイプをカプセル化して、IP ネットワーク上に仮想ポイントツーポイント リンクを構築します。

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 フローを代行受信し、Cisco IOS 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 フロー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 サービスをクローズドに設定すると、WCCP では登録されている WCCP クライアントがないパケットが破棄され、リダイレクトされたトラフィックが受信されます。

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 コマンドを使用できるのは、クローズド モード サービスの場合だけです。アプリケーション プロトコルの種類またはポート番号を登録するには、**service-list** キーワードおよび *service-access-list* 引数を使用します。

サービスリスト ACL と、キャッシュ エンジンから受信された定義が一致しなかった場合は、サービスを開始できません。

WCCP 発信 ACL チェック

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、リダイレクト ルータのローカルの Web キャッシュにリダイレクトされるのが一般的です。

アクセス コントロール リスト（ACL）は、ルーティング処理したパケットを転送するか、ルータ インターフェイスでブロックするかを制御して、ネットワーク トラフィックをフィルタ処理します。各パケットは確認され、ACL に指定されている基準に従って、転送するかドロップするかが判断されます。ACL の条件には、トラフィックの発信元アドレス、トラフィックの宛先アドレス、または上位レイヤのプロトコルを指定できます。IP ACL は、IP アドレスに適用する許可条件と拒否条件の一連のコレクションです。ルータは、同時に 1 つずつ、ACL の条件に対してアドレスをテストします。最初の一致によって、そのアドレスを受け入れるか拒否するかが決まります。最初の一致後に Cisco IOS ソフトウェアは条件のテストを停止するため、条件の順序が重要です。一致する条件がない場合、暗黙的な「deny all」句によって、ルータはそのアドレスを拒否します。

リダイレクションが実行されるインターフェイスに、発信 ACL が設定されている場合、状況によっては、トラフィックのリダイレクト先ホストが宛先へのアクセス権を取得します（アクセス権がなければブロックされる宛先です）。

WCCP 発信 ACL チェック機能によって、発信 ACL チェック処理は元のインターフェイスで実行されるため、チェック処理はセキュアであり、すべてのプラットフォームおよび Cisco IOS スイッチング パスで一貫しています。

WCCP サービス グループ

WCCP は、定義済みの特徴を使用して、元の宛先から代替の宛先へとトラフィックをリダイレクトする Cisco IOS ソフトウェアのコンポーネントです。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。

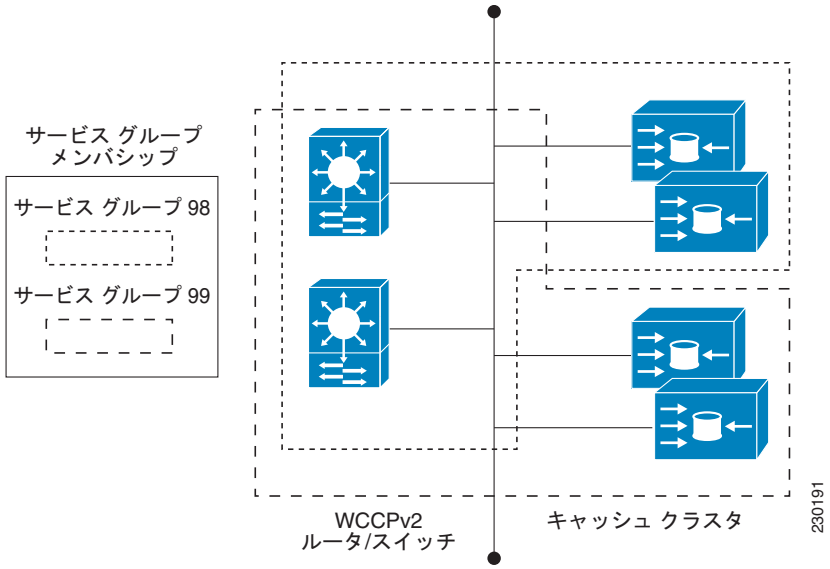
リダイレクションに選択されるトラフィックの性質は、コンテンツ エンジンで指定されるサービス グループによって定義され、WCCP を使用してルータに通信されます。Cisco IOS Release 12.3(14)T よりも前の Cisco IOS リリースに実装されている最新の WCCP では、最大 8 個のサービス グループを定義できました。この最大値によって、キャッシングの展開が制限されていました。Cisco IOS Release 12.3(14)T 以降のリリースで、すべての VRF で使用できるサービス グループの最大数が 256 に増えました。

WCCPv2 は、サービス グループごとに最大 32 個のルータをサポートします。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。

トラフィックの代行受信およびリダイレクトのために展開されている論理リダイレクション サービスに基づいて、WCCPv2 はサービス 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。このサービスは、Web キャッシュ サービスの特徴はルータとコンテンツ エンジンの両方から認識されているため、*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、**web-cache** キーワードを指定して **ip wccp** コマンドを使用します。

（注） 1 つのルータで同時に複数のサービスを実行できます。また、ルータおよびコンテンツ エンジンは、同時に複数のサービス グループに参加できます。

図 3　　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分散方法をルータに指示します。ダイナミック サービス グループのトラフィックの特徴に関する情報は、ルータ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、単一のプロトコルに最大 8 個の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。このマニュアルの構成情報では、Cisco ルータで一般的なサービスをイネーブルにする方法について説明しています。

WCCP：Check Services All

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 グループのプライオリティは、Cisco IOS 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、一致についてすべて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、リダイレクト ACL およびサービスのプライオリティによって制御できます。

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** コマンドを設定していない限り、低いプライオリティ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、インターフェイスに設定されている残りの低いプライオリティ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 サービスを設定するまで、ルータの WCCP はディセーブルです。**ip wccp** 形式のコマンドを初めて使用すると、WCCP がイネーブルになります。デフォルトで、WCCPv2 がサービスに使用されますが、WCCPv1 の機能を使用することもできます。WCCP の実行バージョンをバージョン 2 からバージョン 1 に変更するには、または最初の変更後に WCCPv2 に戻すには、グローバル コンフィギュレーション モードで **ip wccp version** コマンドを使用します。

WCCPv1 で使用できない機能の場合、エラー プロンプトが画面に出力されます。たとえば、WCCPv1 がルータ上で実行され、ダイナミック サービスを設定しようとしている場合、「WCCP V1 only supports the web-cache service」というメッセージが表示されます。**show ip wccp** EXEC コマンドを使用すると、ルータで現在実行されている WCCP プロトコル バージョン番号が表示されます。

ip wccp web-cache password コマンドを使用すると、サービス グループのルータおよびコンテンツ エンジンのパスワードを設定できます。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ルータおよびコンテンツ エンジンを設定する必要があります。パスワードは最大 8 文字で構成できます。サービス グループの各コンテンツ エンジンまたはルータは、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破棄されます。

手順の概要

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

手順の詳細

	コマンド	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# 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 version** {**1** | **2**} **例：** `Router(config)# ip wccp version 2`	ルータで設定する WCCP のバージョンを指定します。WCCPv2 がデフォルトの実行バージョンです。
ステップ 4	**ip wccp** [**vrf** *vrf-name*] {**web-cache** | *service-number*} [**group-address** *group-address*] [**redirect-list** *access-list*] [**group-list** *access-list*] [**password** *password* [**0** | **7**]] **例：** `Router(config)# ip wccp web-cache password password1`	ルータでイネーブルにする Web キャッシュまたはダイナミック サービスを指定し、サービス グループに関連付ける VRF 名を指定し、サービス グループに使用される IP マルチキャスト アドレスを指定し、使用するアクセス リストを指定し、MD5 認証を使用するかどうかを指定し、WCCP サービスをイネーブルにします。
ステップ 5	**interface** *type number* **例：** `Router(config)# interface ethernet0/0`	Web キャッシュ サービスが実行するインターフェイス番号をターゲットにし、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 wccp** [**vrf** *vrf-name*] {**web-cache** | *service-number*} **redirect** {**out** | **in**} **例：** `Router(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 オプションの指定に従って、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 7	**exit** **例：** `Router(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 8	**interface** *type number* **例：** `Router(config)# interface GigabitEthernet0/2/0`	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 9	**ip wccp redirect exclude in** **例：** `Router(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. **ip wccp** [**vrf** *vrf-name*] *service-number* **service-list** *service-access-list* **mode** {**open** | **closed**}

   または

   ip wccp [**vrf** *vrf-name*] **web-cache mode** {**open** | **closed**}
4. **ip wccp check services all**
5. **ip wccp** [**vrf** *vrf-name*] {**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： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# 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** [**vrf** *vrf-name*] *service-number* **service-list** *service-access-list* **mode** {**open** | **closed**}
	または
	ip wccp [**vrf** *vrf-name*] **web-cache mode** {**open** | **closed**}
	
	例：
	`Router(config)# ip wccp 90 service-list 120 mode closed`
	または
	
	例：
	`Router(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。

	コマンドまたはアクション	目的
ステップ 4	**ip wccp check services all** 例： `Router(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。 **ip wccp check services all** 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。 （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** [**vrf** *vrf-name*] {**web-cache** | *service-number*} 例： `Router(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： `Router(config)# exit`	特権 EXEC モードに戻ります。

マルチキャスト アドレスへのルータの登録

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、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リスンできるようにルータを設定する必要があります。

リダイレクトされるトラフィックが仲介ルータを通過する必要があるネットワーク構成の場合、通過するルータを設定して、IP マルチキャスト ルーティングを実行するようにします。次の 2 つのコンポーネントを設定して、仲介ルータを通過できるようにします。

- **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 ルーティングをイネーブルにします。
- **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** [**vrf** *vrf-name*] {**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** [**vrf** *vrf-name*] {**web-cache** | **service-number**} **group-listen**

手順の詳細

	コマンド	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# 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：** `Router(config)# ip multicast-routing`	IP マルチキャスト ルーティングをイネーブルにします。
ステップ 4	**ip wccp** [**vrf** *vrf-name*] {**web-cache** | *service-number*} **group-address** *multicast-address* **例：** `Router(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：** `Router(config)# interface ethernet0/0`	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：** `Router(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 6500 シリーズ スイッチおよび Cisco 7600 シリーズ ルータで **ip wccp group-listen** コマンドが適切に動作するために、**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** [**vrf** *vrf-name*] {**web-cache** | *service-number*} **group-listen** **例：** `Router(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 グループでのアクセス 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ルータの設定作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **access-list** *access-list-number* **remark** *remark*
4. **access-list** *access-list-number* **permit** {*source* [*source-wildcard*] | **any**} [**log**]
5. **access-list** *access-list-number* **remark** *remark*
6. **access-list** *access-list-number* **deny** {*source* [*source-wildcard*] | **any**} [**log**]
7. アクセス リストの基礎とする発信元を指定し終わるまで、ステップ 3 ～ 6 の組み合わせを繰り返します。
8. **ip wccp web-cache group-list** *access-list*
9. **ip wccp web-cache redirect-list** *access-list*

手順の詳細

	コマンド	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# 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： `Router(config)# access-list 1 remark Give access to user1`	（任意）アクセス リスト エントリについて、ユーザにわかりやすいコメントを追加します。 • 最大 100 文字の注記を、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： `Router(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のリダイレクションをイネーブルまたはディセーブルにするアクセス リストを作成します。 発信元アドレスおよびワイルドカード マスクに基づいて、指定した発信元を許可します。 • 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。 • 標準の IP アクセス リストは、1 ～ 99 または 1300 ～ 1999 の番号が付けられています。 • *source-wildcard* を省略すると、0.0.0.0 のワイルドカード マスクが想定されます。これは、発信元アドレスのすべてのビットに一致することを示します。 • オプションで、*source source-wildcard* の代わりとして、キーワード **any** を使用し、発信元および 0.0.0.0 255.255.255.255 の発信元ワイルドカードを指定します。 • この例では、ホスト 172.16.5.22 がアクセス リストに適合します。

	コマンド	目的
ステップ 5	**access-list** *access-list-number* **remark** *remark* 例： `Router(config)# access-list 1 remark Give access to user1`	（任意）アクセス リスト エントリについて、ユーザにわかりやすいコメントを追加します。 • 最大 100 文字の注記を、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： `Router(config)# access-list 1 deny 172.16.7.34 0.0.0.0`	発信元アドレスおよびワイルドカード マスクに基づいて、指定した発信元を拒否します。 • *source-wildcard* を省略すると、0.0.0.0 のワイルドカード マスクが想定されます。これは、発信元アドレスのすべてのビットに一致することを示します。 • オプションで、source source-wildcard の代わりとして、省略形 *any* を使用し、発信元および 0.0.0.0 255.255.255.255 の発信元ワイルドカードを指定します。 • この例では、ホスト 172.16.7.34 はアクセス リストに適合しません。
ステップ 7	アクセス リストの基礎とする発信元を指定し終わるまで、ステップ 3 ～ 6 の組み合わせを繰り返します。	明示的に許可されていないすべてのソースは、アクセス リストの末尾で暗黙的な **deny** 文によって拒否されます。
ステップ 8	**ip wccp** [**vrf** *vrf-name*] **web-cache group-list** *access-list* 例： `Router(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 アドレスをルータに示します。
ステップ 9	**ip wccp** [**vrf** *vrf-name*] **web-cache redirect-list** *access-list* 例： `Router(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** [**vrf** *vrf-name*] {**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： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# 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** [**vrf** *vrf-name*] {**web-cache** | *service-number*} [**group-address** *multicast-address*] [**redirect-list** *access-list*] [**group-list** *access-list*] [**password** *password*] 例： `Router(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 に使用でき、*service-number* 引数は WCCP バージョン 2 だけで使用できます。
ステップ 4	**ip wccp check acl outbound** 例： `Router(config)# ip wccp check acl outbound`	発信元インターフェイスで ACL 発信チェックをイネーブルにします。
ステップ 5	**exit** 例： `Router(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 コンフィギュレーション設定の確認とモニタリング

WCCP のコンフィギュレーション設定を確認およびモニタするには、EXEC モードで次のコマンドを使用します。

手順の概要

1. **enable**
2. **show ip wccp** [**vrf** *vrf-name*] [*service-number* | **web-cache**] [**detail** | **view**]
3. **show ip interface**
4. **more system:running-config**

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：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**show ip wccp** [**vrf** *vrf-name*] [*service-number* | **web-cache**] [**detail** | **view**] **例：** `Router# 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、現在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。引数およびキーワードは次のとおりです。 • *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。値の範囲は 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：** `Router# show ip interface`	すべての **ip wccp redirection** コマンドがインターフェイスに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。たとえば、「Web キャッシュ リダイレクトがイネーブルかディセーブルか」などです。
ステップ 4	**more system:running-config** **例：** `Router# more system:running-config`	（任意）現在実行されているコンフィギュレーション 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）。

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ため、問題が発生しました。カウンタによって、直接ルータでバイパス トラフィックを決定し、それが原因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。

WCCP の設定例

例：ルータ上での WCCP バージョンの変更

次に、WCCP バージョンをデフォルトの WCCPv2 から WCCPv1 に変更し、WCCPv1 で Web キャッシュ サービスをイネーブルにする例を示します。

```
Router# show ip wccp

% WCCP version 2 is not enabled

Router# configure terminal
Router(config)# ip wccp version 1
Router(config)# end
Router# show ip wccp

% WCCP version 1 is not enabled
Router# configure terminal
Router(config)# ip wccp web-cache
Router(config)# end
Router# show ip wccp

Global WCCP information:
    Router information:
        Router Identifier:                  10.4.9.8
        Protocol Version:                   1.0
.
.
.
```

例：一般的な WCCPv2 セッションの設定

次に、一般的な WCCPv2 セッションを設定する例を示します。

```
Router# configure terminal
 ip wccp web-cache group-address 224.1.1.100 password password1
 interface ethernet0
 ip wccp web-cache redirect out
 exit
 ip wccp check services all ! Configures a check of all WCCP services.
```

例：ルータとコンテンツ エンジンのパスワードの設定

次に、パスワードが password1 の WCCPv2 パスワードを設定する例を示します。

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

例：Web キャッシュ サービスの設定

```
Router# configure terminal
Router(config)# ip wccp web-cache
Router(config)# interface ethernet 0
Router(config-if)# ip wccp web-cache redirect out
Router(config-if)# exit
Router# copy running-config startup-config
```

次に、イーサネット インターフェイス 0/1 に到達する HTTP トラフィックのリダイレクションをイネーブルにするセッションを設定する例を示します。

```
Router# configure terminal
Router(config)# interface ethernet 0/1
Router(config-if)# ip wccp web-cache redirect in
Router(config-if)# exit
Router# show ip interface ethernet 0/1
.
.
.
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。

```
Router# configure terminal
Router(config)# ip wccp 99
Router(config)# interface ethernet 0
Router(config-if)# ip wccp 99 redirect out
```

例：マルチキャスト アドレスへのルータの登録

次に、224.1.1.100 のマルチキャスト アドレスにルータを登録する例を示します。

```
Router(config)# ip wccp web-cache group-address 224.1.1.100
Router(config)# interface ethernet 0
Router(config-if)# ip wccp web cache group-listen
```

次に、224.1.1.1 のマルチキャスト アドレスを使用して、逆プロキシ サービスを実行するようにルータを設定する例を示します。リダイレクションは、インターフェイス イーサネット 0 を介するパケットの発信に適用されます。

```
Router(config)# ip wccp 99 group-address 224.1.1.1
Router(config)# interface ethernet 0
Router(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、現在のルータ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 アドレスかをルータに通知します。次に、いくつかのサンプル ホストについて、アクセス リスト番号が 10 である標準のアクセス リストのコンフィギュレーション セッションの例を示します。

```
Router(config)# access-list 10 permit host 11.1.1.1
Router(config)# access-list 10 permit host 11.1.1.2
Router(config)# access-list 10 permit host 11.1.1.3
Router(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 ペアのキャッシングをディセーブルにするには、WCCP アクセス リストを使用できます。次に、10.1.1.1 から 12.1.1.1 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機能する例を示します。

```
Router(config)# ip wccp web-cache redirect-list 120
Router(config)# access-list 120 deny tcp host 10.1.1.1 any
Router(config)# access-list 120 deny tcp any host 12.1.1.1
Router(config)# access-list 120 permit ip any any
```

次の例では、インターフェイス イーサネット 0/1 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ルータを設定します。

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

例：WCCP 発信 ACL チェックの設定

次に、アクセス リストによって、ファスト イーサネット インターフェイス 0/0 を介するネットワーク 10.0.0.0 からのトラフィックを回避する設定例を示します。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。

```
Router(config)# ip wccp web-cache
Router(config)# ip wccp check acl outbound
Router(config)# interface fastethernet0/0
Router(config-if)# ip access-group 10 out
Router(config-if)# exit
Router(config)# ip wccp web-cache redirect-list redirect-out
Router(config)# access-list 10 deny 10.0.0.0 0.255.255.255
Router(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 の両方をルータでイネーブルにする例を示します。

```
Router# 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 Ethernet0
    ip address 10.3.1.2 255.255.255.0
    no ip directed-broadcast
    ip wccp web-cache redirect out
    ip wccp 99 redirect out
    no ip route-cache
    no ip mroute-cache
    !

    interface Ethernet1
    ip address 10.4.1.1 255.255.255.0
    no ip directed-broadcast
    ip wccp 99 redirect out
    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 alaska1
login
!
end
```

次に、Cisco IOS のスイッチング パスであるプロセス、ファスト、および CEF について、バイパスしたパケットの情報を表示する例を示します。

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

WCCP Client information:
 Web Client ID:          10.10.10.1
 Protocol Version:       2.0
 State:                  Usable
 Initial Hash Info:      00000000000000000000000000000000
                         00000000000000000000000000000000
 Assigned Hash Info:     FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
                         FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
 Hash Allotment:         256 (100.00%)
 Packets Redirected:     4320
 Connect Time:           00:04:53
 Bypassed Packets
 Process:                0
 Fast:                   0
 CEF:                    250
```

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。

その他の参考資料

関連資料

内容	参照先
Cisco IOS コマンド	『*Cisco IOS Master Commands List, All Releases*』
Cisco ACNS ソフトウェア設定情報	• 『*Cisco ACNS Software Caching Configuration Guide*, Release 4.2』 • Cisco.com の「Cisco ACNS Software」リスト ページ
IP アクセス リストの概要、設定作業、およびコマンド	• 『*IP Access List Features Roadmap*』 • 『*Cisco IOS Security Command Reference*』
IP アドレッシングおよびサービス コマンド、および設定作業	• 『*Cisco IOS IP Addressing Services Configuration Guide*』 • 『*Cisco IOS IP Addressing Services Command Reference*』
WCCP コマンド：コマンド構文、コマンド モード、コマンド履歴、デフォルト設定、使用に関する注意事項および例	『*Cisco IOS IP Application Services Command Reference*』

規格

規格	タイトル
新しい規格または変更された規格はサポートされていません。また、既存の規格に対するサポートに変更はありません。	—

MIB

MIB	MIB リンク
新しい MIB または変更された MIB はサポートされていません。また、既存の MIB に対するサポートに変更はありません。	選択されたプラットフォーム、シスコ ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
新しい RFC または変更された RFC はサポートされていません。また、既存の RFC に対するサポートに変更はありません。	

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

WCCP の機能情報

表 1 に、この章に記載されている機能および具体的な設定情報へのリンクを示します。

プラットフォーム サポートとソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator を使用すると、特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームをサポートするソフトウェア イメージを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 表 1 に、特定のソフトウェア リリース トレイン内の機能に対するサポートが導入されたソフトウェア リリースだけを示します。特に断りのないかぎり、そのソフトウェア リリース トレイン以降のリリースでもその機能がサポートされます。

表 1　WCCP の機能情報

機能名	リリース	機能情報
WCCP バイパス カウンタ	12.3(7)T 12.2(25)S	WCCP バイパス カウンタ機能を使用すると、Web キャッシュによってバイパスされ、元のルータに返送され、通常どおりに転送されたパケットのカウントを表示できます。 この機能に関する詳細については、次の各項を参照してください。 • 「WCCP バイパス パケット」（P.11） • 「例：WCCP 設定の確認」（P.26） **show ip wccp** コマンドはこの機能によって変更されました。
WCCP クローズド サービス	12.4(11)T	WCCP クローズド サービス機能では、WCCP が常にこのようなサービスのトラフィックを代行受信するように WCCP サービスを設定できますが、このトラフィックを受信するように登録された WCCP クライアント（コンテンツ エンジンなど）がない場合、パケットは破棄されます。 この動作は Application-Oriented Network Services（AONS）アプリケーションをサポートします。AONS は WCCP を使用してトラフィックを透過的に代行受信する必要がありますが、WCCP クライアントがパケットを処理できない場合は、パケットを宛先に転送しません（これは、キャッシュがなくてもユーザから見える動作が変化しないという、キャッシュを補助する WCCP の従来の使用方法とは対照的です）。 この機能に関する詳細については、次の各項を参照してください。 • 「WCCP クローズド サービスおよびオープン サービス」（P.11） • 「クローズド サービスの設定」（P.16） • 「例：一般的な WCCPv2 セッションの設定」（P.23） **ip wccp** コマンドは、この機能によって変更されました。
WCCP Increased Service	12.3(14)T 12.2(33)SRA 12.2(33)SXH	WCCP Increased Service 機能によって、WCCP でサポートされるサービス数が VRF 全体で最大 256 に増えます。 この機能に関する詳細については、次の各項を参照してください。 • 「WCCP サービス グループ」（P.12） • 「クローズド サービスの設定」（P.16） • 「WCCP の設定」（P.14） • 「例：WCCP 設定の確認」（P.26） **ip wccp**、**ip wccp check services all**、**ip wccp outbound-acl-check**、および **show ip wccp** コマンドがこの機能によって変更されました。

表 1　WCCP の機能情報 （続き）

機能名	リリース	機能情報
WCCP レイヤ 2 リダイレクション/フォワーディング	12.4(20)T	WCCP レイヤ 2 リダイレクション/フォワーディング機能を使用すると、直接接続している Cisco Content Engine でレイヤ 2 リダイレクトを使用できます。これは、GRE カプセル化を介するレイヤ 3 リダイレクションよりも効率的です。直接接続しているキャッシュ エンジンを設定して、WCCP レイヤ 2 リダイレクション/フォワーディング機能の使用をネゴシエートできます。WCCP レイヤ 2 リダイレクション/フォワーディング機能には、ルータまたはスイッチに設定は必要ありません。 この機能に関する詳細については、次の各項を参照してください。 • 「WCCP に関する制約事項」（P.2） • 「レイヤ 2 フォワーディング、リダイレクション、および返送」（P.5） • 「HTTP 以外のサービスのサポート」（P.9） この機能に関連する新しいコマンドや変更されたコマンドはありません。
WCCP L2 返送	12.4(20)T	WCCP L2 返送機能を使用すると、レイヤ 3 GRE トンネル内のルータにパケットをトンネル処理するのではなく、発信元および宛先の MAC アドレスを交換することで、コンテンツ エンジンから、レイヤ 2 で直接接続されている WCCP ルータにパケットを返送できます。 この機能に関する詳細については、次の各項を参照してください。 • 「レイヤ 2 フォワーディング、リダイレクション、および返送」（P.5） この機能に関連する新しいコマンドや変更されたコマンドはありません。
WCCP マスク割り当て	12.4(20)T	WCCP マスク割り当て機能では、キャッシュ エンジン割り当て方式として、ACNS/WAAS デバイスのサポートを導入します。 この機能については、次の項に説明があります。 • 「WCCP マスク割り当て」（P.6） この機能に関連する新しいコマンドや変更されたコマンドはありません。

表 1　WCCP の機能情報 （続き）

機能名	リリース	機能情報
WCCP 発信 ACL チェック	12.3(7)T 12.2(25)S	WCCP 発信 ACL チェック機能を使用すると、入力インターフェイスで WCCP によってリダイレクトされるトラフィックが、必ず発信 ACL チェックを受けるようにできます。これは、リダイレクト前に終了インターフェイスで設定できます。 この機能は、Web Cache Communication Protocol（WCCP）バージョン 1 およびバージョン 2 でサポートされます。 この機能に関する詳細については、次の各項を参照してください。 • 「WCCP 発信 ACL チェック」（P.12） • 「WCCP 発信 ACL チェックのイネーブル化」（P.20） • 「例：WCCP 発信 ACL チェックの設定」（P.25） **ip wccp** コマンドおよび **ip wccp check acl outbound** コマンドが、この機能で導入または変更されました。
受信インターフェイスでの WCCP のリダイレクション	12.1(3)T 15.0(1)S	受信インターフェイスでの WCCP のリダイレクション機能によって、特定の WCCP サービスのために入力リダイレクションのインターフェイスを設定できます。インターフェイスでこの機能をイネーブルにすると、そのインターフェイスに到達するすべてのパケットは、指定した WCCP サービスに対して比較されます。パケットが一致する場合、そのパケットはリダイレクトされます。 この機能に関する詳細については、次の各項を参照してください。 • 「WCCP に関する制約事項」（P.2） • 「WCCP の設定」（P.14） • 「例：Web キャッシュ サービスの設定」（P.24） **ip wccp redirect-list** コマンドは、この機能で導入または変更されました。

表 1　WCCP の機能情報 （続き）

機能名	リリース	機能情報
WCCP バージョン 2	12.0(3)T 15.0(1)S	WCCP バージョン 2 のいくつかの機能が強化され、次のように WCCP プロトコルに機能が追加されました。 • 複数のルータがコンテンツ エンジン クラスタにサービスを提供できます。 • 多様な UDP および TCP トラフィックなど、HTTP（TCP ポート 80 トラフィック）以外のトラフィックをリダイレクトできます。 • パスワードと HMAC MD5 規格を使用して、サービス グループの一部になるルータとコンテンツ 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。 • 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。 • 個々のコンテンツ エンジンの負荷を調整して、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。 この機能に関する詳細については、次の各項を参照してください。 • 「WCCP に関する制約事項」（P.2） • 「WCCPv2 の設定」（P.8） • 「HTTP 以外のサービスのサポート」（P.9） • 「例：一般的な WCCPv2 セッションの設定」（P.23） **clear ip wccp**、**ip wccp**、**ip wccp group-listen**、**ip wccp redirect**、**ip wccp redirect exclude in**、**ip wccp version**、**show ip wccp** の各コマンドが、この機能で導入または変更されました。
WCCP VRF のサポート	15.0(1)M、 12.2(33)SRE	WCCP VRF のサポート機能によって、VRF の認識をサポートする既存の WCCPv2 プロトコルが強化されています。 Cisco IOS Release 12.2(33)SRE では、この機能が Cisco 7200 NPE-G2 ルータと Cisco 7304-NPE-G100 ルータ上でのみサポートされます。 この機能に関する詳細については、次の各項を参照してください。 • 「WCCP VRF のサポート」（P.11） • 「WCCP の設定」（P.14） **clear ip wccp**、**debug ip wccp**、**ip wccp**、**ip wccp group-listen**、**ip wccp redirect**、**show ip wccp** の各コマンドが、この機能で導入または変更されました。

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。