



# スタンドアロン Content Engine の 透過リダイレクションの設定

この章では、コンテンツ要求をスタンドアロン Content Engine へ透過的にリダイレクトするための次の方法を説明します。

- コンテンツ要求を代行受信し、スタンドアロン Content Engine にリダイレクトする Web Cache Communication Protocol (WCCP) 対応ルータ
- コンテンツ要求を代行受信し、スタンドアロン Content Engine にリダイレクトするレイヤ 4 スイッチ

この章の構成は、次のとおりです。

- [WCCP 透過リダイレクションの概要 \(P. 6-2\)](#)
- [WCCP 透過リダイレクションのスタンドアロン Content Engine の設定 \(P. 6-8\)](#)
- [スタンドアロン Content Engine の WCCP フロー リダイレクションの無効化および再有効化 \(P. 6-17\)](#)
- [スタンドアロン Content Engine における WCCP のシャットダウン \(P. 6-17\)](#)
- [WCCP 透過リダイレクション用のルータの設定 \(P. 6-19\)](#)
- [ルータ上での WCCP サービスの設定 \(P. 6-27\)](#)
- [ルータ上での WCCP 統計情報の削除 \(P. 6-37\)](#)
- [WCCP レイヤ 2 のサポートの設定 \(P. 6-37\)](#)
- [スタンドアロン Content Engine の WCCP サービス設定例 \(P. 6-42\)](#)
- [リダイレクション方式としてのレイヤ 4 スwitチングの設定 \(P. 6-55\)](#)

Cisco ACNS 透過キャッシング ソリューションは、WCCP 対応のルータと各種の高度な技法を使用して、Web ブラウザが動作しない場合や、Web サーバが HTTP に準拠していない場合でも、Content Engine の透過性を確保します。これらの技術の 1 つは、バイパス機能です。バイパス機能の設定方法については、「[スタンドアロン Content Engine でのバイパスの設定](#)」(P. 15-3) を参照してください。



(注) この章で使用される Content Engine CLI コマンドの構文と使用方法については、『Cisco ACNS Software Command Reference, Release 5.3』を参照してください。

WCCP の詳細については、『Cisco IOS Configuration Fundamentals Configuration Guide』および『Cisco IOS Configuration Fundamentals Command Reference』を参照してください。

## WCCP 透過リダイレクションの概要

ルータまたはスイッチが、IP、UDP、および TCP ヘッダ情報に基づいてパケットを代行受信し、透過的にそれらのパケットを ACNS 5.x ソフトウェアを実行している Content Engine にリダイレクトできるようにするために、シスコは Cisco IOS ソフトウェアに組み込まれた WCCP を開発しました。

WCCP には、Version 1 と Version 2 の 2 つのバージョンがあります。WCCP Version 1 は、1 つの WCCP サービス（標準 Web キャッシュ サービス [サービス 0] および 1 つのルータ）だけをサポートしています。WCCP Version 1 の主な機能は、次のとおりです。

- 1 つのルータだけをサポート（ホーム ルータ）
- トラフィック リダイレクションをポート 80 のみでサポート
- 各 WCCP サービスにつき、最大 32 の Content Engine をサポート
- バイパス サポートなし（たとえば、静的なバイパス、エラー バイパスおよび認証バイパスは、サポートされていません）。
- 戻りの GRE（Generic Routing Encapsulation）なし

WCCP Version 2 では、より多くの TCP ポート向けトラフィックを Content Engine にリダイレクトできます。以前は、TCP ポート 80 を宛先とする Web キャッシュ情報だけをリダイレクトできましたが、多くのアプリケーションでは、他のポートを宛先とするパケットもリダイレクトする必要があります。たとえば、プロキシ Web キャッシュ処理、FTP プロキシキャッシング、ポート 80 以外のポートに対する Web キャッシング、RealAudio、およびビデオなどのアプリケーションです。

WCCP Version 2 の使用をお勧めします。それは、この方がさまざまな機能やサービス（表 6-3 を参照）のほか、複数のルータをサポートしているためです。



(注) WCCP は IP ネットワークだけで動作します。

## WCCP を使用したパケットのリダイレクション

WCCP 対応ルータによる透過リダイレクションが要求を Content Engine にリダイレクトするために使用される場合、Web クライアントはコンテンツ要求をソースに送信しますが、その要求が WCCP 対応ルータにより Content Engine にリダイレクトされていることを認識していません。この代行受信およびリダイレクションのプロセスは、コンテンツを要求しているクライアントからはまったく「見えない」または「透過的」なので、デスクトップを変更する必要はありません（クライアントは特定のプロキシ サーバを指定するために、自分のブラウザまたはメディア プレーヤーを設定する必要があります）。Content Engine の動作はネットワークからは透過的なので、WCCP 対応ルータはリダイレクトされないトラフィックに対しては、通常の機能で動作します。

WCCP 透過リダイレクションを使用するには、最初に WCCP 対応ルータ上で WCCP サービスを定義する必要があります。特定のサービスのためのパラメータは、その名前、サービス、ID（サービス番号）、およびこの WCCP サービスのサポートに使用される ルータ インターフェイスです。

Content Engine の WCCP の実装では、現在、すべての WCCP サービスに適用されるグローバル設定（たとえば、ヒーリング パラメータ、スロースタート）が可能です。マルチ サービス モデルでもその仕様は変更されず、該当する設定値は WCCP システム全体に対して、グローバルなまま維持されます。

Content Engine クラスタの一部である Content Engine でヒーリング モードを設定する方法については、「Content Engine クラスタのヒーリング モードの設定」(P. 7-72) を参照してください。WCCP スロー スタートなどの拡張キャッシング機能の設定については、第 15 章「スタンドアロン Content Engine の WCCP サービスの設定」を参照してください。

## Content Engine クラスタおよび WCCP 対応ルータを使用したパケットのリダイレクション

Content Engine のクラスタ（グループ）がある場合、すべて WCCP Version 2 対応ルータから認識され、最小の IP アドレス番号をもつ Content Engine がリード Content Engine になります。このリード Content Engine は、クラスタの Content Engine 間でどのようにトラフィックを割り当てるかを決定します。この割り当て情報は、指定されたリード Content Engine からサービス グループ全体に送られます。これより、グループの WCCP 対応ルータはパケットを適切にリダイレクトでき、グループ内の Content Engine がそれらの負荷をより適切に管理できます。

次に、Content Engine クラスタ内の 1 台の Content Engine をリード Content Engine に指定する方法を説明します。

1. 各 Content Engine が WCCP 対応ルータのリストを使用して設定されます。

WCCP Version 1 では、1 台の WCCP 対応ルータが 1 つのクラスタを処理し、そのルータがクラスタのデフォルト ホーム ルータになります。

WCCP Version 2 では、複数の WCCP 対応ルータ（各ルータ リストには、最大 8 台までのルータを含めることができます）が 1 つのクラスタをサービスすることができます。これにより、サービス グループ内で使用可能なルータが、クラスタ内の各 Content Engine にパケットをリダイレクトできます。

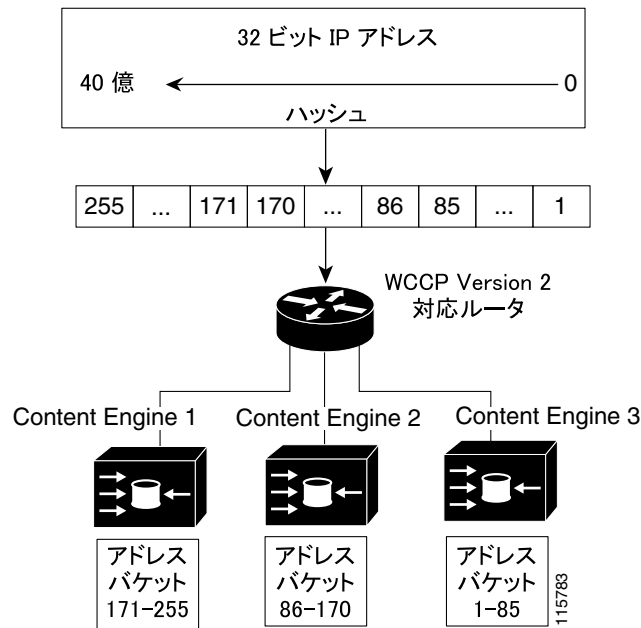
2. 各 Content Engine は、装置の存在をルータのリストの各ルータに告知します。ルータはサービス グループ内の Content Engine のビューを使用して応答します。
3. このビューがクラスタ内のすべての Content Engine 間で一致すると、1 台の Content Engine がリード Content Engine として指定され、WCCP 対応ルータがパケットのリダイレクトで配備する必要のあるポリシーを設定します。

## WCCP Version 2 を使用した動的負荷分散について

IP パケットが WCCP Version 2 対応ルータ上で受信された時、Content Engine にリダイレクトする必要があるかどうかを判断するために、IP パケットを検査します。これは、その要求と定義されたサービス基準を照合することにより行われます。これらのパケットはルータの処理ルーチンに渡され、どの Content Engine（ある場合）がリダイレクトされたパケットを受け取る必要があるかが判断されます。

どの Content Engine が代行受信されたパケットを受信する必要があるかの決定は、パケットが割り当てられたアドレス パケットを取得するために、宛先 IP アドレスのハッシュ関数を実行することで行われます。そして、これらのアドレス パケットは、存在する Content Engine の数とそれらの内の何台が動作中であるかによって、特定の Content Engine にマップされます。図 6-1 を参照してください。

図 6-1 IP アドレスのハッシュによる負荷分散



(注) Content Engine で処理されないパケットは、それらが受信された同じルータにトンネル伝送で戻されます。前にリダイレクトしたパケットを受信するときは、ルータはそのパケットを再度リダイレクトしません。

WCCP Version 2 は動的な負荷分散をサポートし、これによって、ルータはクラスタの個々の Content Engine に転送される負荷を調整できるようになります。WCCP Version 2 は、このタスクを実行するために 2 つの技術を使用します。

- 負荷分散：この技術により、Content Engine に割り当てられるハッシュ アドレス バケットの組み合わせの調整が可能になり、負荷容量が超過した Content Engine から、十分な能力のある他の Content Engine に負荷を移すことができます。
- 負荷制限：この技術により、WCCP 対応ルータは、Content Engine の容量を超過しないように負荷を選択的にリダイレクトします。

## パケット転送方式の概要

WCCP 対応ルータは、次の 2 つのパケット転送方式を使用して代行受信した要求をスタンドアロン Content Engine へリダイレクトします。

- GRE (Generic Routing Encapsulation)：Content Engine へのパスにあるルータの数に関係なく、パケットが Content Engine に到達できます。
- レイヤ 2 リダイレクション：パケットがレイヤ 2 (MAC レイヤ) で切り替えられ、Content Engine に到達できるようにします。

表 6-1 では、これら 2 つの方式を説明しています。

表 6-1 パケット転送方式

パケット転送方式	負荷分散方式：ハッシュ	負荷分散方式：マスク
GRE (レイヤ3)	パケット リダイレクションはすべてルータ ソフトウェアによって処理されます。	パケット リダイレクションはルータ ソフトウェアによって処理されます。パケット転送方式として、GRE が使用されている場合、マスクの割り当てはお勧めできません。
レイヤ2 リダイレクション	最初にリダイレクトされるパケットは、ルータ ソフトウェアで処理され、リダイレクトされる後続のすべてのパケットはルータ ハードウェアで処理されます。	すべてのパケットがルータ ハードウェアで処理されます (特別なハードウェアが必要なため、現在、Catalyst 6000 シリーズでのみサポートされています)。



(注)

どちらのパケット転送方式でも、各種 WCCP サービス グループ内にある複数の Content Engine 間でリダイレクトされたトラフィックの負荷分散方法は、ハッシュ パラメータによって指定されます。

「アサイメント方式」という用語は、Content Engine 間で負荷分散を行うために、WCCP で使用される方式を示しています。使用可能な負荷分散に関するアサイメント方式には、次の2つがあります。それは、ハッシュとマスクです。マスク負荷分散方式が指定されていない場合には、ハッシュ負荷分散方式 (図 6-1 を参照) がデフォルトの方式として使用されます。

このリダイレクションモードは、Content Engine によって制御されます。WCCP グループに参加する最初の Content Engine が、転送方式 (GRE またはレイヤ2 リダイレクション) およびアサイメント方式 (ハッシュまたはマスク) を決定します。「マスクアサイメント」という用語は、WCCP レイヤ2 Policy Feature Card 2 (PFC2) 入力リダイレクションを示すために使用されます。

Content Engine は、無制限に Content Engine クラスタ外にとどまるのではなく、**assign-method-strict** オプションが使用 (たとえば、**wccp https-cache assign-method-strict** コマンドは HTTPS キャッシュサービスの **assign-method-strict** オプションを指定するために使用されます) されない限り、ハードウェアでサポートされるアサイメント方式にフォールバックします。マスクが WCCP 出力リダイレクションで選択される場合、Content Engine は、Multilayer Switch Feature Card (MSFC) および Policy Feature Card (PFC) で使用される元のハードウェア高速化にフォールバックします。

たとえば、WCCP Version 2 では、パケットをフィルタリングして、Content Engine から戻されたリダイレクトパケットと、戻されていないリダイレクトパケットを判別します。戻されたパケットはリダイレクトされません。これは、Content Engine が、そのパケットを処理しないことを判定済みであるからです。WCCP Version 2 は、Content Engine が処理しないパケットを、送信元である同じルータに戻します。

Content Engine がパケットを拒否し、パケットを戻す理由は、主に次のとおりです。

- Content Engine が過負荷になり、パケットを処理するリソースがない。
- Content Engine が、サーバエラーまたは認証の失敗により、自動バイパスをアクティブにした。この場合、クライアントはサーバに直接到達することができます。したがって、Content Engine はその障害の原因ではありません。
- Content Engine が、パケットの処理に逆効果を招く条件 (たとえば、IP 認証がすでにオンになっている場合) でフィルタリングしている。
- Content Engine 上にスタティックバイパスリストを設定している。



(注) パケットは、WCCP 対応ルータと Content Engine 間の接続の送信元にリダイレクトされます。そのアドレスは、使用される Cisco IOS ソフトウェアのバージョンに応じて、発信インターフェイスのアドレスか、ルータの IP アドレスのどちらかになります。元のアドレスがルータの IP アドレスである場合、そのルータ IP アドレスが Content Engine の WCCP 対応ルータ リストに保存されていることが重要です。ルータ リストの詳細は、「[スタンドアロン Content Engine のルータ リストの定義](#)」(P. 6-12) を参照してください。

Cisco Express Forwarding (CEF) は、WCCP Version 2 に統合され、パケットリダイレクト時に最適のパフォーマンスを実現します。さらに、WCCP Version 2 では複数のルータ (ルータ リスト) を設定して、特定の WCCP サービス (たとえば、RTSP リダイレクション) をサポートできます。これについては、「[WCCP 透過リダイレクションのスタンドアロン Content Engine の設定](#)」(P. 6-8) を参照してください。サポートされている WCCP Version 2 の機能とサービスについては、[表 6-3](#) を参照してください。

これらのパケット転送方式の詳細については、次を参照してください。

- [パケット転送方式としてレイヤ 3 GRE を使用する方法](#) (P. 6-6)
- [パケット転送方式としてレイヤ 2 リダイレクションを使用する方法](#) (P. 6-7)

## パケット転送方式としてレイヤ 3 GRE を使用する方法

GRE は、レイヤ 3 の技術であり、データグラムを WCCP 対応ルータ上で IP パケットにカプセル化した後、Content Engine へリダイレクトします (透過プロキシサーバ)。この中間の宛先では、データグラムはカプセル化が解除され、キャッシュミスの場合に要求が満たされるように、オリジンサーバヘルディングされます。この過程で、オリジンサーバへのトリップは 1 ホップの内部データグラムとして扱われます。通常、GRE を使用して行われるリダイレクトトラフィックは、GRE トンネルトラフィックと呼ばれています。GRE を使用して、すべてのリダイレクションはルータソフトウェアによって処理されます。

WCCP リダイレクションの場合、Cisco のルータは TCP SYN パケットを宛先に転送しません。それは、ルータにはその接続の宛先ポートで有効な WCCP があるためです。その代わりに、WCCP 対応ルータは、GRE トンネリングを使用してパケットをカプセル化し、そしてそれを WCCP 対応ルータからリダイレクトされるパケットを受信するように設定されたスタンドアロン Content Engine に送信します。

リダイレクトされたパケットを受信すると、Content Engine は次の動作を行います。

1. GRE レイヤをパケットから除去する。
2. このリダイレクトされたパケットを受け入れ、コンテンツの要求を処理する必要があるかを決定する。
  - a. Content Engine がその要求を受け入れる場合、TCP SYN ACK パケットをクライアントに送信します。この応答パケットでは、Content Engine はソース アドレスとして指定されているオリジナルの宛先 (オリジンサーバ) の IP アドレスを使用します。これは、Content Engine がクライアントからは見えない (透過的) ようにします。そしてクライアントの TCP SYN パケットが到達しようとしている宛先のふりをします。
  - b. Content Engine は、その要求を受け入れないという決定をする場合、GRE の TCP SYN パケットを再度カプセル化し WCCP 対応ルータに送り返します。ルータは、この場合、Content Engine が接続しないことを認識し、そのパケットをオリジナルの宛先 (つまり、オリジンサーバ) に転送します。

たとえば、スタンドアロン Content Engine は、一連の特定のクライアントからの要求、または一連の特定のサーバ宛ての要求をバイパスするように設定されているので、その要求を受け入れないということを決定します。

## パケット転送方式としてレイヤ 2 リダイレクションを使用する方法

レイヤ 2 リダイレクションとは、ルータまたはスイッチ上の WCCP が、レイヤ 2 のルータ ハードウェアの WCCP のトラフィック代行受信およびリダイレクション機能を部分的にまたはすべてを実行する、スイッチング ハードウェアを利用できる状況を表す用語です。このリダイレクションタイプは、現在、Cisco Catalyst 6000 ファミリー、および 6500 ファミリーのスイッチ製品のみがサポートしています。レイヤ 2 リダイレクションでは、最初にリダイレクトされるトラフィック パケットはルータ ソフトウェアにより処理されます。それ以降のトラフィックはルータ ハードウェアで処理されます。レイヤ 2 リダイレクションでは、Content Engine がルータまたはスイッチに対して特定パケットフィールドにビットマスクを適用するように指示します。このビットマスクはクラスタ内の Content Engine にマスクの結果、またはマスク インデックス アドレス テーブルの形にマップされたインデックスを渡します。このリダイレクション プロセスはスイッチング ハードウェアで加速されるので、レイヤ 2 リダイレクションはレイヤ 3 GRE よりも効率的です。



(注) WCCP は Content Engine に対してのみライセンスされており、リダイレクトするルータにはライセンスされていません。WCCP は、ルータまたはスイッチの通常の動作に干渉することはありません。

レイヤ 2 リダイレクションの設定については、「[WCCP レイヤ 2 のサポートの設定](#)」(P. 6-37) を参照してください。

## WCCP 透過リダイレクションのスタンドアロン Content Engine の設定

スタンドアロン Content Engine と WCCP 対応ルータによりサポートされる WCCP サービスのタイプは、表 B-3 で示しているように、WCCP Version 1 または Version 2 のどちらが使用されるかで異なります。標準 Web キャッシュ サービス（サービス 0）を除くすべてのサービスでは、サポートされる特定の WCCP サービスのために（WCCP Version 1 ではなく）WCCP Version 2 がルータおよびスタンドアロン Content Engine で実行されていることが必要です。

表 6-2 サポートされる WCCP 透過リダイレクション サービス

WCCP 透過リダイレクション サービス	WCCP サービス名	説明	詳細
サービス 80	rtsp	RealMedia クライアントから Content Engine に RTSP 要求をリダイレクトするために使用される RTSP リダイレクション。RealMedia 要求を透過的にリダイレクトするには、サービス 80 のみを設定する必要があります。WMT RTSP 透過リダイレクション（Windows Media 9 Player からの RTSP 要求の透過リダイレクション）をサポートするには、サービス 83 だけでなく、サービス 80 を設定する必要があります。	クライアントが RealMedia プレーヤの場合、バックエンドの RTSP サーバは、RealProxy サーバです。クライアントが Windows Media 9 Player の場合、バックエンドの RTSP サーバは Content Engine 上で稼働している Windows Media 9 Server です。
サービス 81	mmstu	WMT クライアントから Content Engine に MMS 要求（MMS 要求および MMS-over-HTTP 要求）をリダイレクトするために使用される MMSTU リダイレクション サービス。	クライアントは WMT クライアント（Windows Media Player Version 6、7、9 など）で、バックエンドの MMS サーバは、WMT サーバ（mms_server プロセス）です。
サービス 82	mmsu	WMT クライアントから Content Engine に MMS 要求（MMS 要求および MMS-over-HTTP 要求）をリダイレクトするために使用される MMSTU リダイレクション サービス。WMT 要求を MMS にリダイレクトするには、サービス 81 とサービス 82 をルータ上で設定する必要があります。	クライアントは WMT クライアント（Windows Media Player Version 6、7、9 など）で、バックエンドの MMS サーバは、WMT サーバ（mms_server プロセス）です。
サービス 83	wmt-rtspu	WMT クライアント（Windows Media 9 Player）から Content Engine（Windows Media 9 Server）に RTSP 要求をリダイレクトするために使用される WMT RTSP リダイレクション サービス	クライアントとサーバは、WMS 9（たとえば、Windows Media 9 Player および Content Engine 上で動作し、WMT RTSP 要求を処理するバックエンドの RTSP サーバとして機能している Windows Media 9 Server）です。



スタンドアロン Content Engine 上で設定可能な WCCP オプションおよびサービスのリストを表示するには、**wccp EXEC** コマンドとそれに続けて疑問符（「?」）を入力してください。WCCP Version 2 が有効になっている Content Engine からの出力例を次に示します。WCCP Version 1 を使用している場合、1 台のルータ（ホーム ルータ）と 1 つの WCCP サービス（標準 Web キャッシュ サービス）だけがサポートされています。

```
ContentEngine(config)# wccp ?
  access-list      Configure an IP access-list for inbound WCCP encapsulated traffic
  custom-web-cache Custom web caching service
  dns              Caching Domain Name Service
  flow-redirect    Redirect moved flows
  ftp-native       Transparent FTP proxy caching service
  home-router      WCCP Version 1 Home Router Ip address
  https-cache      HTTPS caching service
  port-list        Port list for use in WCCP service
  reverse-proxy    Reverse Proxy web caching service
  router-list      Router List for use in WCCP services
  rtsp            RTSP protocol transparent interception
  service-number   WCCPv2 service number
  shutdown         Wccp Shutdown parameters
  slow-start       accept load in slow-start mode
  spoof-client-ip  Use client IP while connecting to the origin server
  version          WCCP Version Number
  web-cache        Standard web caching service
  wmt             Windows media caching service
  wmt-rtspu       Windows media RTSPU (port 5005) transparent interception
```

WCCP Version 1 を使用した標準 Web キャッシュ サービス（サービス 0）については、「例 1 : WCCP Version 1 を使用する web-cache サービスの設定」（P. 6-43）を参照してください。

これらの WCCP Version 2 のオプションおよびサービスについては、表 6-3 を参照してください。表 6-3 のアスタリスク（「\*」）は、各機能が WCCP オプションまたは WCCP サービスのどちらかであることを示しています。

表 6-3 WCCP Version 2 のオプションとサービス

WCCP オプション またはサービス名	WCCP オプション	WCCP サービス	詳細
access-list	*		スタンドアロン Content Engine での WCCP アクセス リストの設定
custom-web-cache		*	ルータ上での custom-web-cache サービス（サービス 98）の設定
dns		*	ルータ上での DNS キャッシング サービス（サービス 53）の設定
flow-redirect	*		スタンドアロン Content Engine の WCCP フロー リダイレクションの無効化および再有効化
ftp-native		*	ルータ上での ftp-native キャッシング（サービス 60）の設定
https-cache		*	ルータ上での https-cache サービス（サービス 70）の設定
port-list	*		スタンドアロン Content Engine のポートリストの定義
reverse-proxy		*	ルータ上での reverse-proxy サービス（サービス 99）の設定
rtsp		*	ルータ上での rtsp サービス（サービス 80）の設定
service-number	*		ルータ上でのユーザ定義 WCCP サービス（サービス 90～97）の設定
shutdown	*		スタンドアロン Content Engine のポートリストの定義
slow-start	*		WCCP スロー スタートの設定
spoof-client-ip	*		WCCP IP スプーフィングの設定
version	*		スタンドアロン Content Engine の WCCP の有効化
web-cache		*	例 2 : WCCP Version 2 を使用する web-cache サービスの設定

表 6-3 WCCP Version 2 のオプションとサービス (続き)

WCCP オプション またはサービス名	WCCP オプション	WCCP サービス	詳細
wmt		*	ルータ上での MMST サービス (サービス 81) の設定 ルータ上での MMSU サービス (サービス 82) の設定
wmt-rtspu		*	ルータ上での wmt-rtspu サービス (サービス 83) の設定



(注)

ACNS 5.2 ソフトウェアより前のリリースでは、最大 8 個の WCCP サービスが WCCP Version 2 対応ルータおよび Content Engine によってサポートされていました。ACNS 5.2.1 ソフトウェアまたはそれ以降では、最大 25 個のアクティブな WCCP Version 2 サービスをサポートします。ACNS 5.3.1 ソフトウェアリリースでは、wmt-rtspu (サービス 83) が追加されました。ACNS 5.3 ソフトウェアでは、現在設定可能なサービスが 18 個あります。

ACNS 5.2 ソフトウェアでは、別の代行受信モード (accept-all モード) が https-cache サービスのために追加されました。このモードは、HTTPS トラフィックのフィルタリングをサポートするために追加されました。このモードは、従来の WCCP サービスと同様に機能します (たとえば、デフォルトですべての Web トラフィックを代行受信する標準 Web キャッシュ サービス [サービス 0])。wccp https-cache accept-all 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いる場合は、HTTP キャッシュ (https-cache サービスが設定され、有効になっている Content Engine) は「accept-all」モードで動作します。それ以外の場合は、Content Engine (HTTPS キャッシュ) は、ACNS 5.1.x ソフトウェアの場合と同じように、「accept-only」モードで動作します。

透過リダイレクション用に WCCP を使用するには、Content Engine を適切に設定する必要があります。次の重要事項に注意してください。

- Content Engine は、1 台または複数台の WCCP 対応ルータからリダイレクトされたパケットを受け入れるように設定される必要があります。WCCP Version 1 では、単一のルータのみがサポートされます。WCCP Version 2 では、複数のルータ (ルータ リスト) がサポートされます。
- Content Engine 上のソフトウェアのバージョンは、WCCP 対応ルータ上にインストールされているバージョンとの互換性が重要です。
- Content Engine 上のパケットは、暗号化も圧縮もされていないことが必要で、また、「内部」ネットワーク アドレス変換 (NAT) がある場合は、Content Engine はその一部であることが必要です。
- Web キャッシュ リダイレクト対応インターフェイスを超えて、サーバへのルート上に Content Engine を配置すると、IP ルート キャッシュにエントリが読み込まれません。
- ルータ上で WCCP を有効にした後、そのルータおよび Content Engine を透過キャッシング サービス用に設定する必要があります。

WCCP 透過リダイレクション用にスタンドアロン Content Engine を設定する方法については、次を参照してください。

- [スタンドアロン Content Engine の WCCP の有効化 \(P. 6-11\)](#)
- [スタンドアロン Content Engine の ポート リスト の定義 \(P. 6-11\)](#)
- [スタンドアロン Content Engine の ルータ リスト の定義 \(P. 6-12\)](#)
- [スタンドアロン Content Engine の WCCP サービスの設定 \(P. 6-13\)](#)
- [スタンドアロン Content Engine の WCCP 設定情報の表示 \(P. 6-16\)](#)

スタンドアロン Content Engine で WCCP サービスを設定する方法のサンプル シナリオについては、「[スタンドアロン Content Engine の WCCP サービス設定例](#)」(P. 6-42) を参照してください。ルータ上で WCCP 透過代行受信を設定する方法については、「[WCCP 透過リダイレクション用のルータの設定](#)」(P. 6-19) を参照してください。

## スタンドアロン Content Engine の WCCP の有効化

スタンドアロン Content Engine で WCCP を有効にするには、**wccp version** グローバル設定コマンドを入力します。スタンドアロン Content Engine で実行する WCCP のバージョンを指定します。WCCP 環境で使用されるルータが実行しているソフトウェアの Version が、スタンドアロン Content Engine 上で設定した WCCP の Version をサポートしていることを確認します。

次の例では、スタンドアロン Content Engine 上で WCCP Version 2 を有効にする方法を示しています。

```
Content Engine (config)# wccp version 2
```

次の例では、スタンドアロン Content Engine 上で WCCP Version 1 を有効にする方法を示しています。

```
Content Engine (config)# wccp version 1
```

Content Engine で一度に有効にできるのは、WCCP の 1 つのバージョンだけです。WCCP Version 2 を実行することをお勧めします。これは、WCCP Version 2 の方が WCCP オプションを広範囲にサポートしていて、複数のルータ (ルータ リスト) をサポートできるからです。WCCP Version 2 でサポートされている機能およびサービスのリストについては、[表 6-3](#) を参照してください。

WCCP Version 2 を有効にするときは事前に WCCP Version 1 を無効にする必要はなく、その逆も同様です。しかし、Content Engine 上で WCCP を適切にシャットダウンするには、現在実行中のバージョンを無効にする必要があります。これについては、「[スタンドアロン Content Engine の WCCP フロー リダイレクションの無効化および再有効化](#)」(P. 6-17) を参照してください。

## スタンドアロン Content Engine の ポート リスト の定義

WCCP Version 1 の場合、TCP ポート 80 を宛先とする Web キャッシュ情報だけを Content Engine にリダイレクトできますが、多くのアプリケーションでは、他のポートを宛先とするバケットもリダイレクトする必要があります。たとえば、プロキシ Web キャッシュ処理、ポート 80 以外に対する Web キャッシング、RealAudio、およびビデオなどのアプリケーションです。ルータが WCCP Version 1 ではなく WCCP Version 2 用に設定されている場合には、WCCP 対応ルータのポート 80 以外の TCP ポートを設定して、トラフィックを Content Engine にリダイレクトできます。

最大 8 つのポート リストを設定できます (ポート リスト番号 1 ~ 8)。これらのポート リストで、WCCP がリダイレクトした着信トラフィックを Content Engine が待ち受けるポート番号を指定します。これらのポート リストによって、Content Engine が着信 WCCP 要求を複数のポートで待ち受けるように設定することができます。

デフォルトで、Content Engine はポート 80 で着信トラフィックを待ち受けます。作成する 8 つのユーザ定義 WCCP サービスのそれぞれに 1 つのポート リストを作成します (サービス 90 ~ 97)。ポート リストごとに最大 8 つのポートを定義できます。次の場合、各ポート リストには単一のポートがあります (たとえば、ポート リスト 1 にはポート 32 があります)。

```
ContentEngine(config)# wccp port-list 1 32
ContentEngine(config)# wccp port-list 2 33
ContentEngine(config)# wccp port-list 3 34
ContentEngine(config)# wccp port-list 4 35
ContentEngine(config)# wccp port-list 5 36
ContentEngine(config)# wccp port-list 6 37
ContentEngine(config)# wccp port-list 7 38
ContentEngine(config)# wccp port-list 8 39
```

## スタンドアロン Content Engine の ルータ リスト の定義

Content Engine 上で WCCP Version 2 サービスを設定する際には、Content Engine に対して特定の WCCP Version 2 サービス (rtsp サービスなど) をサポートする WCCP Version 2 対応ルータのリストを作成する必要があります。

スタンドアロン Content Engine でルータ リストを作成するには、**wccp router-list** グローバル設定コマンドを使用します。Content Engine のために特定の WCCP サービスをサポートする各 WCCP Version 2 対応ルータの IP アドレスを入力します。各種 WCCP サービスに対して複数の異なるルータを使用する場合、複数のルータ リストを作成する必要があります。各ルータ リストには、最大 8 台のルータを含めることができます。

次の例では、ルータ リスト番号 1 が作成され、これには 1 台のルータが含まれています (IP アドレス 10.10.10.1 の WCCP Version 2 対応ルータ)。

```
ContentEngine(config)# wccp router-list 1 10.10.10.1
```

次の例では、ルータ リスト (ルータ リスト 1) の作成方法と、ルータ リスト 1 の WCCP Version 2 対応ルータからリダイレクトされた WMT トラフィック (「wmt」という名前の WCCP サービス) を受け入れるように Content Engine を設定する方法を示しています。

```
ContentEngine(config)# wccp router-list 1 10.10.10.2
ContentEngine(config)# wccp wmt router-list 1
ContentEngine(config)# wccp version 2
```

WCCP Version 1 では、標準 Web キャッシュ サービス (サービス 0) をサポートする 1 台の WCCP 対応ルータだけを設定できます。Content Engine のクラスタがある場合でも、1 台のみの WCCP Version 1 対応ルータが Content Engine のクラスタと通信し、クラスタのデフォルト ホーム ルータになります。ルータを WCCP Version 1 を使用する標準 Web キャッシュ サービスのホーム ルータとして設定する方法については、「例 1: WCCP Version 1 を使用する web-cache サービスの設定」(P. 6-43) を参照してください。



(注)

ルータ リストに含まれる各ルータ上で WCCP を有効にするためには、**ip wccp** グローバル設定コマンドを使用する必要があります。

WCCP Version 2 用に Content Engine を設定する場合、Content Engine 上のルータのリストではなく IP マルチキャストアドレスを設定することができます。Content Engine 上のルータのリストを使用しても、IP マルチキャストを使用する必要はありませんが、各 Content Engine 上での設定がさらに必要になります。IP マルチキャストアドレスを使用すると、Content Engine 上の設定が軽減され、プロトコルのオーバーヘッドも削減されます。

IP マルチキャストでは、IP マルチキャスト アドレスが Content Engine で設定されます。WCCP Version 2 対応ルータは、IP マルチキャスト アドレスを 1 つまたは複数のインターフェイスで受信するように設定されます。そして、これらのルータはリダイレクトされた要求を Content Engine の指定された IP マルチキャスト アドレスに送信します。マルチキャスト アドレスは 224.0.0.0 ~ 239.255.255.255 でなければなりません。IP マルチキャストアドレスの割り当ては、Internet Assigned Numbers Authority (IANA) によって管理されています。IANA は、IP マルチキャスト用に IPv4 クラス D アドレス スペースを割り当てています。このため、すべての IP マルチキャスト グループ アドレスは、224.0.0.0 ~ 239.255.255.255 の範囲内にあります。ただし、ソースとグループアドレスのいくつかの組み合わせは、マルチキャストには使用できません。使用できないマルチキャストアドレス範囲、および使用できない理由については、「使用できないマルチキャストアドレスの割り当て」(P. B-16) を参照してください。

サービス グループのメンバーの WCCP Version 2 対応ルータの設定がさらに必要になるのは、IP マルチキャストが次のように使用されるとき、それらのルータがサービス グループのメンバーになることが予定されている場合です。

- サービス グループで使用される IP マルチキャスト アドレスを設定する必要がある。
- WCCP Version 2 対応ルータが IP マルチキャスト アドレスを受信するインターフェイスは、**ip wccp {web-cache | service-number} group-listen** コマンドで設定する必要がある。

ターゲットルータに到達するために別の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、次のような IP マルチキャストルーティングを行う必要があります。

- **ip multicast-routing** コマンドを使用し、ルータの IP マルチキャストルーティングを設定することにより、それを有効にする必要がある。
- **ip pim** コマンドを使用して、Content Engine の接続先のルータ インターフェイスでマルチキャストを受信するように設定する必要がある。

## スタンドアロン Content Engine の WCCP サービスの設定

WCCP 対応ルータと Content Engine がサポートできる WCCP サービスの中には、よく知られた一連の基準および事前定義サービス ID があります (たとえば、標準 web-cache サービス [サービス 0])。これらのサービスは、事前定義 WCCP サービスと呼ばれます。他の例には、reverse-proxy キャッシング サービス (サービス 99) https-caching サービス (サービス 70)、および rtsp サービス (サービス 80) があります。

あまり知られていない他の WCCP サービスは、基準のセットを指定し、これらのユーザ定義 WCCP Version 2 サービスをサービス ID に割り当てることで定義されます。WCCP Version 2 では、最大 8 個のユーザ定義 WCCP サービス (サービス 90 ~ 97) を定義できます。これらユーザ定義サービスのそれぞれは、最大 8 つのポートをサポートします。

ユーザ定義 WCCP サービスをサポートするスタンドアロン Content Engine の設定方法の詳細については、「[ユーザ定義 WCCP サービスをサポートするためのスタンドアロン Content Engine の設定](#)」(P. 6-14) を参照してください。



(注) サポートされる WCCP サービスについては、[表 B-3](#) を参照してください。

スタンドアロン Content Engine の WCCP サービスを設定するには、次の重要事項に注意してください。

- WCCP Version 1 は、1 つの WCCP サービス (標準 web-cache のサービス [サービス 0]) と 1 台のルータだけをサポートします。したがって、WCCP Version 2 の使用をお勧めします。これは、WCCP Version 2 の方が広範囲な機能やサービスに加え、複数のルータをサポートしているからです。
- スタンドアロン Content Engine で使用される、特定の WCCP サービスをサポートする WCCP Version 2 対応ルータのリストを作成する必要があります。各種 WCCP サービスに対して複数の異なるルータを使用する場合、複数のルータ リストを作成する必要があります。
- WCCP Version 2 もルータ リスト内の各ルータ上で有効にする必要があります。指定した WCCP サービスを、特定のルータ リストにリストされている、特定の WCCP サービスに関連付けられたルータのそれぞれで有効にすることも必要です。
- WCCP Version 2 をスタンドアロン Content Engine 上で有効にし、このサービスをサポートする WCCP Version 2 対応ルータのリストを定義した後、Content Engine で特定の WCCP サービスと、特定の WCCP サービスをサポートする WCCP 対応ルータを有効にする必要があります。

次の例では、WCCP Version 2 対応ルータ上でユーザ定義 WCCP サービス（サービス 91）を有効にする方法を示しています。

```
Router# configure terminal
Router(config)# ip wccp 91
Router(config)# interface ethernet 0
Router(config-if)# ip wccp 91 redirect out
```

- WCCP Version 2 対応ルータ上で **show ip wccp EXEC** コマンドを使用し、WCCP 変数に関連付けられた値を表示します。
- クラスタと通信するルータの TTL (Time To Live; 存続可能時間) 値は、15 秒以下でなければなりません。
- サービス グループには、最大 32 台の Content Engine と 32 台の WCCP 対応ルータを組み込むことができます。
- クラスタ内のすべての Content Engine に、そのクラスタと通信するすべての WCCP 対応ルータが設定されている必要があります。クラスタ内のある Content Engine にルータがまったく設定されていない場合、サービス グループは不整合を検出し、その Content Engine は、サービス グループ内で動作しません。



(注)

Content Engine と WCCP 対応ルータをファイアウォールで隔てることはできません。ファイアウォールでは、オリジン Web サーバ宛ての packets トラフィックだけを処理し、そのサーバに代わって Content Engine がクライアントに送信する packets トラフィックは処理しないからです。

また、多くの WCCP Version 2 サービスには、**wccp** グローバル設定コマンドの特定のオプションの設定も必要です。**wccp** グローバル設定コマンドの詳細は、『Cisco ACNS Software Command Reference, Release 5.3』を参照してください。ルータまたはスイッチの設定方法が不明な場合は、それらの装置に付属のソフトウェア資料を参照してください。WCCP Version 2 コマンドおよびルータ設定例の詳細は、Cisco IOS ソフトウェアのオンライン資料を参照してください。

## ユーザ定義 WCCP サービスをサポートするためのスタンドアロン Content Engine の設定

ユーザ定義 WCCP サービスは、トラフィックをスタンドアロン Content Engine にリダイレクトするようポート番号を設定できる WCCP Version 2 のサービスです。Content Engine は、透過的なフォワードプロキシサーバとして機能しています。

WCCP Version 2 では、複数のポートをサポート (WCCP サービスごとに最大 8 つのポート) する最大 8 つのユーザ定義 WCCP サービス (サービス 90 ~ 97) を設定できます。これらのサービスを設定するため、使用する各サービスに対して 1 つのポート リストを作成する必要があります (たとえば、サービス 90 に対してはポート リスト番号 1 を作成します)。ポート リストには、その特定のユーザ定義 WCCP サービスで WCCP Version 2 対応ルータが WCCP リダイレクションをサポートするポート番号が含まれています。これらのユーザ定義 WCCP サービスを設定する場合、そのトラフィックが Content Engine 上のキャッシング アプリケーション、HTTP キャッシング アプリケーション、またはストリーミング アプリケーションのいずれかにリダイレクトされるべきかを指定する必要があります。

複数のポートを使用して Web トラフィックをキャッシングするように Content Engine を設定するには、ユーザ定義 WCCP サービスを実行するように Content Engine と WCCP Version 2 対応ルータを設定します。これらのユーザ定義 Web サービスを使用して、通常は、単一ポートだけをサポートする標準 WCCP サービス (たとえば、所定の https-cache、rtsp、mmst、および reverse-proxy の各サービス) の複数のポート (サービスごとに最大 8 つのポート) で HTTP、MMS、HTTPS、および RTSP 要求の WCCP リダイレクションをサポートします。

Content Engine GUI または CLI コマンドを使用して、ユーザ定義 WCCP サービスを Content Engine 上で設定できます。Content Engine GUI では、**WCCP > Services** を選択します。表示された Services ウィンドウを使用して Content Engine を設定し、ユーザ定義 WCCP サービス（サービス 90 ~ 97）をサポートします。Services ウィンドウの使用の詳細については、ウィンドウの **HELP** ボタンをクリックしてください。

Content Engine CLI では、**wccp service-number** グローバル設定コマンドを使用して Content Engine を設定し、ユーザ定義 WCCP サービスをサポートします。次の例で示しているように、作成する各ユーザ定義 WCCP サービス（たとえば、サービス 95）のマスクとルータリストを指定できます。

```
ContentEngine(config)# wccp service-number 95 ?
mask                Specify mask used for CE assignment
router-list-num     Router list number
```

**router-list-num** オプションを使用して、Content Engine が指定した WCCP サービスからリダイレクトされた要求を受け入れる必要のある WCCP Version 2 対応ルータのリストを指定します。

```
ContentEngine(config)# wccp service-number 95 router-list-num 1
```

**port lists** オプションを使用して、Content Engine が指定した WCCP サービスからリダイレクトされたトラフィックを受信するポートを指定します。次の例は、ルータ リスト 1 の WCCP Version 2 対応ルータからリダイレクトされたサービス 95 のトラフィックを、ポートリスト番号 5 にリストされたポートで受信するよう Content Engine を設定する方法を示しています。

```
ContentEngine(config)# wccp service-number 95 router-list-num 1 port-list-num 5
```

**applications** オプションを使用して、リダイレクトされたトラフィックが Content Engine 上のキャッシングアプリケーション、HTTP キャッシングアプリケーション、またはストリーミングアプリケーションのいずれに宛てられるべきかを指定します。

```
ContentEngine(config)# wccp service-number 95 router-list-num 1 port-list-num 1
application ?
cache          Direct traffic to the caching application
https-cache    Direct traffic to the https caching application
streaming      Direct traffic to the streaming media application
```

Content Engine GUI を使用して、スタンドアロン Content Engine の WCCP の有効化および設定を行う場合には、次の Content Engine GUI ウィンドウの各サービスで、指定されたルータリストを指定する必要があります。Web Cache ウィンドウ (**WCCP > Web Cache**)、Reverse Proxy ウィンドウ (**WCCP > Reverse Proxy**)、Custom Web Cache ウィンドウ (**WCCP > Custom Web Cache**)、および WCCP Services ウィンドウ (**WCCP > Services**)。

スタンドアロン Content Engine でユーザ定義 WCCP サービス（サービス 90 ~ 97）を設定する方法の例については、「[例 4 : スタンドアロン Content Engine での複数の WCCP Version 2 サービスの設定](#)」(P. 6-49) を参照してください。

## スタンドアロン Content Engine の WCCP 設定情報の表示

いくつかの Content Engine CLI コマンドが、スタンドアロン Content Engine で WCCP 関連の設定情報（たとえば、現在設定されている WCCP サービスのリスト）を表示して使用できます。

スタンドアロン Content Engine 上で現在設定されている WCCP サービスのリストを表示するには、**show wccp services EXEC** コマンドを入力します。

```
ContentEngine# show wccp services
Services configured on this Content Engine
  Web-cache
  Reverse Proxy
  RTSP
  WMT
  MMSU
  DNS
  FTP
  RTSPU
  HTTPS Cache
  WCCPv2 Service 90
  WCCPv2 Service 91
  WCCPv2 Service 92
  WCCPv2 Service 93
  WCCPv2 Service 94
  WCCPv2 Service 95
  WCCPv2 Service 96
  WCCPv2 Service 97
```

サポートされる WCCP サービスのリストについては、[表 B-3](#) を参照してください。

現在設定されている WCCP サービスのスタンドアロン Content Engine のリストを表示するには、**show wccp content-engines EXEC** コマンドを入力します。

スタンドアロン Content Engine で設定された WCCP サービスのルータ関連情報を表示するには、**show wccp EXEC** コマンドを入力します。



## スタンドアロン Content Engine の WCCP フロー リダイレクションの無効化および再有効化

デフォルトで、WCCP フロー リダイレクションはスタンドアロン Content Engine 上で有効です。

スタンドアロン Content Engine で WCCP フロー リダイレクションを再度有効にするには、**wccp flow-redirect enable** グローバル設定コマンドを使用します。

```
ContentEngine(config)# wccp flow-redirect enable
```

WCCP フロー リダイレクションを無効にする場合は、このコマンドの **no** 形式を使用します。

```
ContentEngine(config)# no wccp flow-redirect enable
```

詳細は、「[WCCP フロー保護の設定](#)」(P. 15-10) を参照してください。

## スタンドアロン Content Engine における WCCP のシャットダウン

不完全な TCP 接続を防止するには、**reload** または **no wccp version** コマンドを入力してから、Content Engine による WCCP の適切なシャットダウンを行います。Content Engine は、すべての接続サービスが完了するか、あるいは WCCP Version 2 の最大待ち時間 (**wccp shutdown max-wait** コマンドで指定します [デフォルトでは、120 秒]) が経過するまでリブートしません。

WCCP が適切にシャットダウンしている間、Content Engine は扱っているフローの処理は続けますが、新しいフローはバイパスするようになります。フローの数が 0 になると、リード Content Engine によりバケットが他の Content Engine に再割り当てされ Content Engine は自身をクラスタから除外します。Content Engine がクラッシュするか、または WCCP を適切にシャットダウンしないでリブートすると、TCP 接続は、さらに不完全になる可能性があります。

Content Engine の特定のポートの個々の WCCP サービスをシャットダウンできないので (たとえば、ポート 80 のリバースプロキシサービスをシャットダウンできません)、Content Engine の WCCP をシャットダウンする必要があります。Content Engine の WCCP がシャットダウンした後も、Content Engine は WCCP 設定値を保持し、プロキシスタイル要求を処理します (たとえば、Content Engine がクライアントのブラウザから直接受信する HTTP 要求)。

スタンドアロン Content Engine で WCCP をシャットダウンするのに、Content Engine GUI または CLI を使用することができます。Content Engine GUI の場合、Content Engine GUI のメインウィンドウの **Clean WCCP shutdown** チェックボックスにチェックマークを付けて (図 4-19 を参照)、同じウィンドウの **REBOOT** ボタンをクリックします。

Content Engine CLI を使用して、スタンドアロン Content Engine 上で WCCP を適切にシャットダウンする手順は、次のとおりです。

### ステップ 1 適切なシャットダウンまでの待機時間を指定します。

```
Content Engine(config)# wccp shutdown max-wait seconds
```

*seconds* は、**no wccp version** コマンドを入力してから、Content Engine が WCCP を適切にシャットダウンするまで待機する秒単位の最長時間です (0 ~ 86400)。デフォルトは 120 秒です。このコマンドは、WCCP Version 2 のみでサポートされています。次の例では、1000 秒間待つように Content Engine を設定する方法を示しています。

```
ContentEngine(config)# wccp shutdown max-wait 1000
```

ステップ 2 Content Engine 上で WCCP Version 2 をシャットダウンします。

```
ContentEngine(config)# no wccp version 2
```

Content Engine は、WCCP Version 2 をシャットダウンするまで 1000 秒間待ちます。カウントダウンメッセージが表示され、Content Engine 上で WCCP をシャットダウンするまでに残されている秒数が示されます。

```
Waiting (999 seconds) for WCCP shutdown. Press ^C to skip shutdownn
```

カウントダウンメッセージが表示された後、**^C** を同時に押すと、進行中でもシャットダウンを中止することができます。

---

## WCCP 透過リダイレクション用のルータの設定

ここでは、ルータ上で次のタスクを行う方法を説明します。

- [WCCP Version 2 対応ルータのパスワードの設定 \(P. 6-19\)](#)
- [ルータにおける WCCP Version 2 の一般的な設定の実行 \(P. 6-19\)](#)
- [ルータ上での WCCP の有効化 \(P. 6-20\)](#)
- [WCCP サービス グループをサポートするための WCCP Version 2 ルータの有効化 \(P. 6-20\)](#)
- [WCCP を使用した送信インターフェイスまたは受信インターフェイスでのパケットのリダイレクトの有効化 \(P. 6-24\)](#)
- [ルータ アクセス リストを使用した Content Engine のバイパス \(P. 6-25\)](#)



(注)

**ip wccp** コマンドを WCCP Version 2 対応ルータ上で使用し、ルータに実行させたい WCCP サービスを指定します。WCCP サービスはそのサービス番号または名前で指定されます。サポートされる WCCP サービス、サービス番号、および名前全リストについては、[表 B-3](#) を参照してください。ルータ上で WCCP サービスを設定する方法については、「[ルータ上での WCCP サービスの設定 \(P. 6-27\)](#)」を参照してください。

### WCCP Version 2 対応ルータのパスワードの設定

スタンドアロン Content Engine がアクセスする WCCP Version 2 対応ルータのパスワードを、次のように設定する必要があります。

```
Router(config)# ip wccp web-cache password [0-7] password
```

ここで各パラメータの意味は、次のとおりです。

- **password** は、指定されたサービス グループから受信されるメッセージに MD5 認証を適用するように、WCCP Version 2 対応ルータに指示する文字列です。この認証によって受け入れられないメッセージは、廃棄されます。
- **0-7** は、パスワードの暗号化に使用される HMAC MD5 アルゴリズムを示すオプション値です。暗号化されたパスワードが Content Engine に対して作成されるときに、この値が生成されます。
- **password** は、ルータと Content Engine 間の接続に対するセキュリティを確立するために、HMAC MD5 値と組み合わせるオプションのパスワード名です。

### ルータにおける WCCP Version 2 の一般的な設定の実行

次の例では、ルータ上での WCCP Version 2 の一般的な設定セッションを示します。



(注)

WCCP Version 2 を使用したリダイレクションを有効にするには、すべての WCCP Version 2 のルータ設定で **ip wccp version 2** コマンドを入力する必要があります。

```
Router# configure terminal
Router(config)# ip wccp version 2
Router(config)# interface ethernet0
Router(config-if)# ip wccp web-cache redirect out
```

## ルータ上での WCCP の有効化

ルータ上で WCCP を有効にするには、**ip wccp version** グローバル設定コマンドを入力します。たとえば、次のコマンドでルータ上の WCCP Version 2 を有効にします。

```
Router(config)# ip wccp version 2
```



(注)

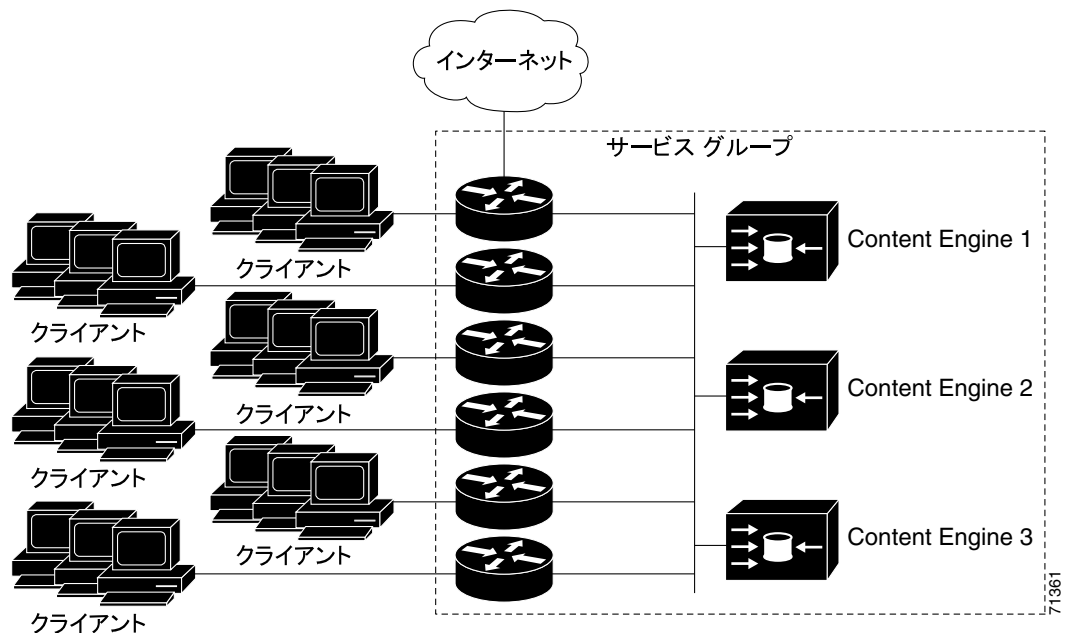
ルータ リストに含まれている各ルータ上で WCCP を有効にするには、**ip wccp** グローバル設定コマンドを使用する必要があります。

## WCCP サービス グループをサポートするための WCCP Version 2 ルータの有効化

WCCP Version 2 では、Content Engine クラスタの一連の Content Engine を有効にして、複数のルータに接続します。同じサービスを実行しているクラスタ内の Content Engine および Content Engine クラスタに接続されている WCCP Version 2 対応ルータは、「サービス グループ」として知られています。スタンドアロン Content Engine (Content Distribution Manager に登録されていない Content Engine) は、Content Engine クラスタの一部になります。

WCCP Version 2 対応ルータは、Content Engine と常に通信していて、利用可能な Content Engine を認識しています。ルータと Content Engine は互いを認識し、WCCP Version 2 を使用してサービス グループを構築します。図 6-2 を参照してください。

図 6-2 WCCP Version 2 のサービス グループ



サービス グループが構築された後、いずれかの Content Engine が、Content Engine クラスタ内の Content Engine 間の負荷の割り当てを決定するように指定されます。サポートされる WCCP サービスのタイプは、WCCP Version 1 または Version 2 のいずれが使用されるかによって異なります。標準 **web-cache** サービス (サービス 0) を除き、表 B-3 にリストされたすべての WCCP サービスでは、WCCP Version 2 が必要とされます。

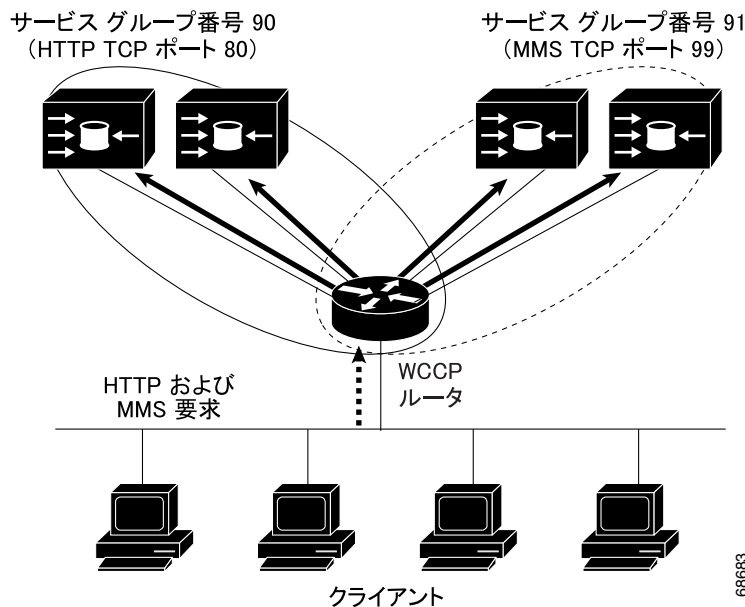
WCCP は、サービス グループの概念を取り入れ、WCCP 対応のルータおよび Content Engine に対するキャッシング関連サービスを 1 つのクラスタ内に定義します。また WCCP は、それらのキャッシング関連サービスを要求するクライアントからのユーザ要求を、キャッシングクラスタにリアルタイムでリダイレクトします。WCCP を経由した透過キャッシングでは、WCCP Version 2 対応ルータを設定して、透過キャッシング エンジンとして機能している Content Engine に要求をリダイレクトできます。

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

- **wccp service-number mask** グローバル設定コマンドを使用して設定された同じハッシュ パラメータまたはマスク パラメータをもつ。
- 個々のポート上の WCCP Version 2 サービスは、個別に停止または開始できない (WCCP Version 2 の制約事項)。

図 6-3 では、左側の 2 つの Content Engine は、ポート 80 で HTTP トラフィックのみを処理し、サービス グループ 90 のメンバーとして定義されています。右側の 2 つの Content Engine は、ポート 99 で Microsoft Media Server (MMS) 要求のみを処理し、サービス グループ 91 のメンバーとして定義されています。

図 6-3 WCCP Version 2 サービス グループ



custom-web-cache サービスおよび reverse-proxy サービス (サービス 98 と 99) は、それぞれ 1 ポートだけを使用して設定できます。したがって、従来のサービスを 1 つだけ設定している場合、透過リダイレクション ポートの最大合計数は 57 になります。これらの両方の従来型サービスが設定される場合、最大合計ポート数は 50 になります。

8 つのユーザ定義サービスがそれぞれ最大ポート数の 8 ポートを使用すると、透過リダイレクションで指定可能なポートの最大数は 64 になります。

WCCP は、非対称パケットフローも処理できます。また WCCP は、WCCP サービス グループで使用されるスイッチまたはルータの数 (最高 32 台のルータまたはスイッチが、クラスタ内で最高 32 個の Content Engine と通信します) に関係なく、Web サーバとキャッシュとの一貫したマッピングを常に保持します。

WCCP のサービス グループに対するサポートの有効化または無効化を WCCP Version 2 対応ルータに指示するには、この **ip wccp** グローバル設定コマンドを使用します。WCCP のサービス グループに対するサポートを制御するルータの機能を除去する場合には、このコマンドの **no** 形式を使用します。

**ip wccp** {web-cache | service-number} [group-address groupaddress] [redirect-list access-list] [group-list access-list] [password [0-7] password]

表 6-4 ip wccp コマンドのパラメータ

<b>web-cache</b>	Web キャッシュ サービスを有効にします。
<i>service-number</i>	WCCP Version 2 対応ルータが制御する WCCP サービスの識別番号。サービス番号は 0 ~ 99 です。WCCP のサービス番号のリストについては、表 B-3 を参照してください。
<b>group-address</b>	(オプション) WCCP サービス グループとの通信に、指定されたマルチキャスト IP アドレスを使用するように、WCCP Version 2 対応ルータに指示します。
<i>groupaddress</i>	(オプション) リダイレクトされたメッセージを受信する Content Engine を判別するために、WCCP Version 2 対応ルータが使用するマルチキャスト アドレス。
<b>redirect-list</b>	(オプション) アクセス リストを使用して、この WCCP サービス グループにリダイレクトされるトラフィックを制御するように、WCCP Version 2 対応ルータに指示します。
<i>access-list</i>	(オプション) Content Engine にリダイレクトされるトラフィックを判別するアクセス リストの名前 (64 文字以下の文字列)。
<b>group-list</b>	(オプション) アクセス リストを使用して、WCCP サービス グループへの参加が許可されている Content Engine を判別するように、WCCP Version 2 対応ルータに指示します。
<i>access-list</i>	(オプション) WCCP サービス グループへの参加が許可されている Content Engine を判別するアクセス リストの名前 (64 文字以下の文字列)。
<b>password</b>	(オプション) 指定されたサービス グループから受信されるメッセージに MD5 認証を適用するように、WCCP Version 2 対応ルータに指示する文字列。この認証によって受け入れられないメッセージは、廃棄されます。
<i>0-7</i>	(オプション) パスワードの暗号化に使用される HMAC MD5 アルゴリズムを示す値。暗号化されたパスワードが Content Engine に対して作成されるときに、この値が生成されます。
<i>password</i>	(オプション) WCCP Version 2 対応ルータと Content Engine 間の接続に対するセキュリティを確立するために、HMAC MD5 値と組み合わせるパスワード名。

次の例では、マルチキャストアドレス 172.31.0.0 を使用 (待ち受け) して、WCCP リバース プロキシ サービス (サービス 99) を実行するよう WCCP Version 2 対応ルータを設定する方法を示しています。

```
Router(config)# ip wccp 99 group-address 172.31.0.0
```



(注) **ip wccp group-listen** コマンドを使用して、WCCP 機能用の IP マルチキャスト パケットの受信を有効または無効にするように、WCCP Version 2 対応ルータ上のインターフェイスを設定します。

WCCP Version 2 は認証機能を備えています。この認証機能を使用すると、WCCP サービス グループにどの WCCP Version 2 対応ルータと Content Engine を含めるかを管理できます。サービス グループのメンバーシップを管理するには、`ip wccp password [0-7] password` コマンドで設定するパスワードと HMAC MD5 アルゴリズムを使用します。

## ルータ上での WCCP リダイレクションの有効化

WCCP Version 2 を使用する前に、インターネットに接続されているインターフェイス上の IP、および Content Engine に接続されているインターフェイス上の IP を設定する必要があります。Content Engine に接続されるインターフェイスは、イーサネット インターフェイス、またはファーストイーサネット インターフェイスです。

ルータ インターフェイスが WCCP Version 2 を使用できるようにし、Web トラフィックを ACNS 5.x ソフトウェア実行中のスタンドアロン Content Engine にリダイレクトする手順は次のとおりです。

**ステップ 1** ルータが WCCP を使用できるようにします。

```
Router# configure terminal  
Router(config)# ip wccp version 2
```

**ステップ 2** (オプション) リダイレクト アクセス リストを指定します。

このアクセス リストと一致するパケットだけが、Content Engine に転送されます。リダイレクト アクセス リストを指定しない場合、すべてのパケットが Content Engine にリダイレクトされます。

```
Router(config)# ip wccp redirect-list [number | name]
```

**ステップ 3** インターフェイス名および番号を指定することで、インターフェイス設定モードを入力します。

次の例では、イーサネット 0 インターフェイスを指定する方法を示しています。

```
Router(config)# interface ethernet 0
```

**ステップ 4** Web トラフィックをスタンドアロン Content Engine にリダイレクトするように、インターネットに接続されているルータ インターフェイスを設定します。

```
Router(config-if)# ip wccp web-cache redirect [in | out]
```



(注) すべての WCCP 対応ルータは out オプションをサポートしていますが、in オプションをサポートしているのは特定のルータだけです。可能な場合はいつも、out オプションを指定することをお勧めします。詳細情報については、次の [WCCP を使用した送信インターフェイスまたは受信インターフェイスでのパケットのリダイレクトの有効化](#) を参照してください。

**ステップ 5** (オプション) クライアントと Content Engine が同一ネットワーク上にある場合、インターフェイス上で高速スイッチング パスを使用するように、ルータを設定します。

```
Router(config-if)# ip route-cache same-interface
```

ステップ 6 設定モードを終了します。

```
Router(config-if)# end
```

ステップ 7 実行中の設定をスタートアップ設定に保存します。スタートアップ設定は、不揮発性メモリに格納されます。

```
Router# copy running-config startup-config
```

## WCCP を使用した送信インターフェイスまたは受信インターフェイスでのパケットのリダイレクトの有効化

送信インターフェイスまたは受信インターフェイスのいずれかに対して、リダイレクトを指定できます。受信トラフィックと、Cisco Express Forwarding (CEF)、分散 Cisco Express Forwarding (dCEF)、Fast Forwarding、または Process Forwarding を使用するように設定します。

インターフェイス上で受信トラフィックをリダイレクトする WCCP を設定すると、送信トラフィックの CEF 転送に関連するオーバーヘッドを回避できます。送信インターフェイス上でリダイレクションを有効にすると、インターフェイスに着信するすべてのパケットで、低速スイッチングパスを取ります。入力インターフェイス上でリダイレクションを有効にすると、そのインターフェイスに着信するパケットだけが設定された機能パスを使用し、他のインターフェイスに着信するパケットはより高速のデフォルトパスを使用します。しかし、必ずしもすべてのルータが入力インターフェイスのリダイレクションをサポートしているとはかぎりません。

受信トラフィックに対して WCCP を設定すると、ルーティング テーブルの検索前にパケットが分類されるので、パケットのリダイレクションは高速になります。

WCCP を使用して、送信インターフェイスまたは受信インターフェイス上でのパケットのリダイレクトを有効にするには、表 6-5 で説明されているように、この **ip wccp redirect** インターフェイス設定コマンドを使用します。WCCP リダイレクトを無効にする場合は、このコマンドの **no** 形式を使用します。

```
ip wccp {web-cache | service-number} redirect {out | in}
```

表 6-5 ip wccp redirect コマンドのパラメータ

パラメータ	説明
<b>web-cache</b>	Web キャッシュ サービスを有効にします。
<i>service-number</i>	WCCP Version 2 対応ルータが制御する WCCP サービス グループの識別番号。サービス番号は 0 から 99 です。サポートされているサービス番号のリストについては、表 B-3 を参照してください。
<b>redirect</b>	送信インターフェイスまたは受信インターフェイス上でのパケットのリダイレクトに対するチェックを有効にします。
<b>out</b>	送信インターフェイス上でのパケットのリダイレクトを指定します。
<b>in</b>	受信インターフェイス上でのパケットのリダイレクトを指定します。

**ip wccp redirect** インターフェイス コマンドは、**ip wccp redirect exclude in** コマンドに影響を与える可能性があります。あるインターフェイス上で **ip wccp redirect exclude in** を設定した後に、**ip wccp redirect in** コマンドを設定すると、**exclude in** コマンドが無効になります。その反対の場合もあります。すなわち、**exclude in** コマンドを設定すると、**redirect in** コマンドが無効になります。



特定のクライアントに対してキャッシングを無効にする手順は、次のとおりです。

**ステップ 1** リダイレクトを有効にするために使用されるアクセス リストを設定します。

```
Router# configure terminal
Router(config)# ip wccp web-cache redirect-list access-list number
```

**ステップ 2** Content Engine へのトラフィックのリダイレクトを有効または無効にするアクセス リストを作成します。

```
Router(config)# access-list access-list number deny host host-address
```

**ステップ 3** 任意のホストへのアクセスを有効にするアクセス リストを設定します。

```
Router(config)# access-list access-list number permit ip any
```

次の例では、イーサネット インターフェイス 0 上のリバース プロキシ パケットが、リダイレクト用にチェックされ、Content Engine にリダイレクトされる設定セッションを示しています。

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

次の例では、イーサネット インターフェイス 0/1 に着信する HTTP トラフィックが、Content Engine にリダイレクトされる設定セッションを示しています。

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

## ルータ アクセス リストを使用した Content Engine のバイパス

デフォルトでは、すべての HTTP パケットが Content Engine にリダイレクトされます。アクセス リストを使用して WCCP Version 2 対応ルータを設定すると、スタンドアロン Content Engine へのトラフィックのリダイレクトを許可したり、拒否したりできます。次の例では、ルータは、以下の条件に合うトラフィックを Content Engine にリダイレクトしません。

- ホスト 10.1.1.1 から発信され、他の任意のホストを宛先とするトラフィック
- 任意のホストから発信され、ホスト 10.255.1.1 を宛先とするトラフィック

```
Router# configure terminal
Router(config)# ip wccp web-cache redirect-list 120
Router(config)# access-list 120 deny ip host 10.1.1.1 any
Router(config)# access-list 120 deny ip any host 10.255.1.1
Router(config)# access-list 120 permit ip any
```

明示的に許可されていないトラフィックは、暗黙的にリダイレクションが拒否されます。**access-list 120 permit ip any** コマンドは、任意の送信元から任意の宛先に送信される、すべてのトラフィックが Content Engine にリダイレクトされることを明示的に許可します。条件の一致はコマンドが入力される順に行われるため、**permit** グローバル コマンドは最後に入力します。アクセス リストの詳細については、Cisco IOS ソフトウェアの資料を参照してください。

アクセスリストと一致するパケットだけをリダイレクトするには、**ip wccp redirect-list** グローバル設定コマンドを使用してください。Content Engine にリダイレクトするパケットを指定する場合に、このコマンドを使用します。

WCCP が有効であるときに、**ip wccp redirect-list** コマンドが使用されていない場合は、すべての Web 関連パケットが Content Engine にリダイレクトされます。**ip wccp redirect-list** コマンドを指定すると、アクセスリストに一致するパケットだけがリダイレクトされます。

WCCP を使用して Content Engine への要求のリダイレクトを開始するときに必要なコマンドは、**ip wccp** グローバル設定コマンドと **ip web-cache redirect** インターフェイス設定コマンドだけです。送信パケットをチェックし、適切なパケットを Content Engine にリダイレクトするよう WCCP 対応ルータインターフェイスに指示する場合、この **ip web-cache redirect** インターフェイス設定コマンドを使用します。**ip wccp** コマンドが有効であるにもかかわらず、**ip web-cache redirect** コマンドが無効の場合、WCCP 対応ルータは Content Engine を認識しますが、それを使用しません。

一部の Web サイトでは、認証にパケットの送信元 IP アドレスを使用します。Content Engine は、Web サイトへの要求の送信時に独自の IP アドレスを使用します。したがって、Content Engine からの要求は認証されないことがあります。このような場合、**ip wccp redirect-list** コマンドを使用して Content Engine をバイパスします。

**ip wccp redirect-list {number | name}**

ここで各パラメータの意味は、次のとおりです。

- *number* は、標準または拡張 IP アクセスリスト番号 (1 ~ 199)。
- *name* は、標準または拡張 IP アクセスリストの名前。この引数は Cisco IOS リリース 11.2 P のみ使用できます。

## ルータ上での WCCP サービスの設定

ここでは、WCCP Version 2 が実行中のルータ上で、次の WCCP サービスを設定する方法を説明します。

- ルータ上での標準 Web キャッシュ サービス (サービス 0) の設定 (P. 6-27)
- ルータ上での DNS キャッシング サービス (サービス 53) の設定 (P. 6-28)
- ルータ上での ftp-native キャッシング (サービス 60) の設定 (P. 6-29)
- ルータ上での https-cache サービス (サービス 70) の設定 (P. 6-29)
- ルータ上での rtsp サービス (サービス 80) の設定 (P. 6-30)
- ルータ上での MMST サービス (サービス 81) の設定 (P. 6-31)
- ルータ上での MMSU サービス (サービス 82) の設定 (P. 6-32)
- ルータ上での wmt-rtspu サービス (サービス 83) の設定 (P. 6-33)
- ルータ上でのユーザ定義 WCCP サービス (サービス 90 ~ 97) の設定 (P. 6-34)
- ルータ上での custom-web-cache サービス (サービス 98) の設定 (P. 6-34)
- ルータ上での reverse-proxy サービス (サービス 99) の設定 (P. 6-35)

ルータ上で WCCP サービスを設定した後、さらにリダイレクトされた要求を受け入れるよう Content Engine を設定する必要があることに注意してください。「WCCP 透過リダイレクションのスタンドアロン Content Engine の設定」(P. 6-8) を参照してください。

### ルータ上での標準 Web キャッシュ サービス (サービス 0) の設定

標準 Web キャッシュ サービス (サービス 0) は、事前定義 Web キャッシング サービスで、1 台の WCCP Version 1 対応ルータか、1 台または複数の WCCP Version 2 対応ルータが、HTTP トラフィックをスタンドアロン Content Engine にリダイレクトすることをポート 80 でのみ許可します。スタンドアロン Content Engine がポート 80 でリダイレクトされた HTTP 要求を受け入れるには、さらに、Content Engine でこのサービスを設定します (Content Engine は、透過 HTTP プロキシ転送キャッシュとして機能します)。

次の例では、ルータ上で WCCP Version 2 を有効にしてから、ルータ上で標準 Web キャッシュ サービス (サービス 0) を設定する方法を示しています。

**ステップ 1** ルータ上で WCCP Version 2 を有効にします。

```
Router# configure terminal
Router(config)# ip wccp version 2
```

**ステップ 2** ルータ上で標準 Web キャッシュ サービス (サービス 0) を有効にします。

```
Router(config)# ip wccp web-cache
```

**ステップ 3** 標準 Web キャッシュ サービスを実行するインターフェイスを指定します。通常、このインターフェイスがインターネットへ出力するトラフィックを搬送します。

```
Router(config)# interface type number
```

次の例では、ルータ上のイーサネット インターフェイス 0/1 が標準 Web キャッシュ サービスを実行するように設定されています。

```
Router(config)# interface ethernet 0/1
```

- ステップ 4** 標準 Web キャッシュ サービスが設定されているインターフェイス（たとえば、イーサネットインターフェイス 0/1）に着信する HTTP トラフィックを確認するようルータを設定します。ルータはこのトラフィックを確認して、パケットをスタンドアロン Content Engine にリダイレクトする必要があるかどうかを判定します。Content Engine は、透過プロキシ転送サーバとして機能しており、ポート 80 で、この WCCP Version 2 対応ルータからリダイレクトされた HTTP 要求を受け入れます。

```
Router(config-if)# ip wccp web-cache redirect out
```

Content Engine で標準 Web キャッシュ サービスを設定することにより（透過 HTTP プロキシ転送キャッシング）、ポート 80 でリダイレクトされた HTTP 要求を受け入れるように、スタンドアロン Content Engine を設定する必要があることにも注意してください。このトピックに関する詳細は、「[スタンドアロン Content Engine における標準 Web キャッシュ サービス（サービス 0）の設定](#)」（P. 7-18）を参照してください。

## ルータ上での DNS キャッシング サービス（サービス 53）の設定

DNS キャッシング サービス（サービス 53）は、事前定義 WCCP Version 2 キャッシング サービスです。このサービスは、WCCP Version 2 対応ルータがクライアント要求を透過的に Content Engine にリダイレクトすることを許可し、Content Engine が DNS の名前解決できるようにします。Content Engine が DNS の名前解決すると、Content Engine は DNS をローカルに保存して、今後の DNS 要求に対してこれら解決済みの名前を使用できるようにします。

ルータ上で DNS キャッシング サービス（サービス 53）を設定する手順は、次のとおりです。

- ステップ 1** ルータ上で WCCP Version 2 を有効にします。

```
Router# configure terminal
Router(config)# ip wccp version 2
```

- ステップ 2** ルータ上で DNS キャッシング サービス（サービス 53）を有効にします。

```
Router(config)# ip wccp 53
```

- ステップ 3** DNS キャッシング サービスを実行するルータ インターフェイスを指定します。

```
Router(config)# interface type number
```

- ステップ 4** DNS キャッシング サービスに送信インターフェイスを使用するように、ルータを設定します。

```
Router(config-if)# ip wccp 53 redirect out
```

Content Engine が WCCP Version 2 対応ルータからリダイレクトされた DNS 要求を受け入れるには、事前にスタンドアロン Content Engine で DNS キャッシング サービス（サービス 53）を設定する必要がありますことに注意してください。このトピックに関する詳細は、「[スタンドアロン Content Engine における DNS キャッシングの設定](#)」（P. 7-64）を参照してください。

## ルータ上での ftp-native キャッシング（サービス 60）の設定

ftp-native キャッシング サービス（サービス 60）は、事前定義 WCCP Version 2 キャッシング サービスです。このサービスは、WCCP Version 2 対応ルータが、ネイティブ FTP 要求を透過的に Content Engine 上の単一ポートにリダイレクトすることを許可します。Content Engine は、要求された FTP コンテンツを取得し、ローカルにコピーを保存し（ネイティブ FTP キャッシング）、要求されたコンテンツを FTP クライアントに配信します。



(注) ACNS 5.3.1 ソフトウェア リリースでは、FTP のネイティブ要求と FTP-over-HTTP 要求の違いを明確にするために、この WCCP サービスの名前は、「ftp から ftp-native」に変更されました。サービス 60 (ftp-native キャッシング サービス) は、FTP ネイティブ要求の透過リダイレクションにのみ適用され、FTP-over-HTTP 要求には適用されません。

ルータ上で ftp-native キャッシング サービス（サービス 60）を設定する手順は、次のとおりです。

**ステップ 1** ルータ上で WCCP Version 2 を有効にします。

```
Router# configure terminal
Router(config)# ip wccp version 2
```

**ステップ 2** ルータ上で ftp-native キャッシング サービス（サービス 60）を有効にします。

```
Router(config)# ip wccp 60
```

**ステップ 3** ftp-native キャッシング サービスを実行するインターフェイスを指定します。

```
Router(config)# interface type number
```

**ステップ 4** ftp-native キャッシング サービスに送信インターフェイスを使用するように、ルータを設定します。

```
Router(config-if)# ip wccp 60 redirect out
```

Content Engine が WCCP Version 2 対応ルータからリダイレクトされた FTP-native 要求を受け入れるには、事前にスタンドアロン Content Engine 上で ftp-native キャッシング サービスを設定する必要がありますことに注意してください。このトピックに関する詳細は、「[透過 FTP ネイティブ キャッシングの設定](#)」(P. 7-44) を参照してください。

## ルータ上での https-cache サービス（サービス 70）の設定

https-cache サービス（サービス 70）は、事前定義 WCCP Version 2 Web キャッシング サービスです。このサービスは、WCCP Version 2 対応ルータが、HTTPS トラフィックを透過的に、ポート 443 でスタンドアロン Content Engine にリダイレクトすることを許可します。

ルータ上で HTTPS キャッシュ サービス（サービス 70）を設定する手順は、次のとおりです。

ステップ 1 ルータ上で WCCP Version 2 を有効にします。

```
Router# configure terminal  
Router(config)# ip wccp version 2
```

ステップ 2 ルータ上で https-cache サービス（サービス 70）を有効にします。

```
Router(config)# ip wccp 70
```

ステップ 3 HTTPS キャッシュ サービスを実行するインターフェイスを指定します。

```
Router(config)# interface type number
```

次の例では、ルータのイーサネット 0 インターフェイスが HTTPS キャッシュ サービスを実行するように設定されています。

```
Router(config)# interface ethernet 0
```

ステップ 4 HTTPS キャッシュ サービスに対して送信インターフェイスを使用できるようにルータを設定します。

```
Router(config-if)# ip wccp 70 redirect out
```

スタンドアロン Content Engine が WCCP Version 2 対応ルータからリダイレクトされた HTTPS 要求を受け入れ可能にするには、事前に HTTPS 透過キャッシング用にスタンドアロン Content Engine を設定する必要があることにも注意してください。このトピックに関する詳細は、「[スタンドアロン Content Engine における HTTPS 透過キャッシングの設定](#)」(P. 7-29) を参照してください。

## ルータ上での rtsp サービス（サービス 80）の設定

rtsp サービス（サービス 80）は、事前定義 WCCP Version 2 メディア キャッシング サービスです。WCCP Version 2 対応ルータ上で、RTSP クライアント要求を透過的に Content Engine 上の単一ポートにリダイレクトさせるメディア キャッシング サービス（RealMedia 透過キャッシング）。

Content Engine は、標準 RTSP ポート（デフォルトポート 554）で転送された RTSP 要求を受信します。デフォルトポート（ポート 554）以外のポート上で RTSP トラフィックを代行受信するには、ユーザ定義 WCCP サービスを設定します（サービス 90～97）。RealMedia クライアントから RTSP 要求の透過代行受信を設定するには、WCCP Version 2 対応ルータ上で rtsp サービス（サービス 80）のみを設定する必要があります。

逆に、WMT RTSP 要求の透過代行受信を設定するには、WCCP Version 2 対応ルータ上で wmt-rtspu サービス（サービス 83）だけでなく、rtsp サービス（サービス 80）を設定する必要があります。ルータ上でサービス 83 を設定する方法については、「[ルータ上での wmt-rtspu サービス（サービス 83）の設定](#)」(P. 6-33) を参照してください。

ルータ上で RTSP サービス（サービス 80）を設定する手順は、次のとおりです。

ステップ 1 ルータ上で WCCP Version 2 を有効にします。

```
Router# configure terminal
Router(config)# ip wccp version 2
```

ステップ 2 ルータ上で rtsp サービス（サービス 80）を有効にします。

```
Router(config)# ip wccp 80
```

ステップ 3 rtsp サービスを実行するインターフェイスを指定します。

```
Router(config)# interface type number
```

ステップ 4 RTSP サービスに対して送信インターフェイスを使用できるようにルータを設定します。

```
Router(config-if)# ip wccp 80 redirect out
```

スタンドアロン Content Engine が WCCP Version 2 対応ルータからリダイレクトされた RealMedia RTSP 要求を受け入れ可能にするには、事前にスタンドアロン Content Engine で RealMedia 透過キャッシングを設定する必要があることに注意してください。このトピックに関する詳細は、[第 8 章「スタンドアロン Content Engine の RealMedia サービスの設定」](#)を参照してください。

## ルータ上での MMST サービス（サービス 81）の設定

MMST は、TCP を介して転送を行う Microsoft Media Server プロトコルです。MMST サービス（サービス 81）は、事前定義 WCCP Version 2 メディアキャッシングサービスです。このサービスは、WCCP Version 2 対応ルータが MMST リダイレクションを使用して、WMT クライアント要求を透過的に Content Engine の単一ポート（ポート 1755）にリダイレクトすることを許可します（Content Engine は、WMT 透過キャッシング用に設定された、透過プロキシサーバとして動作します）。

WMT RTSP 要求の透過代行受信を設定するには、WCCP Version 2 対応ルータ上で mmst サービス（サービス 81）だけでなく、mmsu サービス（サービス 82）を設定する必要があります。ルータ上でサービス 82 を設定する方法については、[ルータ上での MMSU サービス（サービス 82）の設定](#)を参照してください。

ルータ上で MMST サービス（サービス 81）を設定する手順は、次のとおりです。

ステップ 1 ルータ上で WCCP Version 2 を有効にします。

```
Router# configure terminal
Router(config)# ip wccp version 2
```

ステップ 2 ルータ上で mmst サービス（サービス 81）を有効にします。

```
Router(config)# ip wccp 81
```

ステップ 3 mmst サービスを実行するインターフェイスを指定します。

```
Router(config)# interface type number
```

ステップ 4 mmst サービスに対して送信インターフェイスを使用できるようにルータを設定します。

```
Router(config-if)# ip wccp 81 redirect out
```

---

スタンドアロン Content Engine が WCCP Version 2 対応ルータからリダイレクトされた WMT 要求を受け入れ可能にするには、事前にスタンドアロン Content Engine で WMT MMS 透過キャッシングを設定する必要があることに注意してください。このトピックに関する詳細は、「[WMT 要求の透過リダイレクションの設定](#)」(P. 9-40) を参照してください。

## ルータ上での MMSU サービス (サービス 82) の設定

MMSU は、UDP を介した転送を行う Microsoft Media Server プロトコルです。mmsu サービス (サービス 82) は、WCCP Version 2 メディア キャッシング サービスです。このサービスは、WCCP Version 2 ルータが MMSU リダイレクションを使用して、WMT クライアント要求を透過的に Content Engine の単一ポート (ポート 1755) にリダイレクトすることを許可します (Content Engine は、WMT MMS 透過キャッシング用に設定された、透過プロキシ サーバです)。

WMT RTSP 要求の透過代行受信を設定するには、WCCP Version 2 対応ルータ上で mmsu サービス (サービス 82) だけでなく、mmst サービス (サービス 81) を設定する必要があります。ルータ上でサービス 81 を設定する方法については、「[ルータ上での MMST サービス \(サービス 81\) の設定](#)」(P. 6-31) を参照してください。

ルータ上で MMSU サービス (サービス 82) を設定する手順は、次のとおりです。

ステップ 1 ルータ上で WCCP Version 2 を有効にします。

```
Router# configure terminal
Router(config)# ip wccp version 2
```

ステップ 2 ルータ上で mmsu サービス (サービス 82) を有効にします。

```
Router(config)# ip wccp 82
```

ステップ 3 MMSU サービスを実行するインターフェイスを指定します。

```
Router(config)# interface type number
```

ステップ 4 MMSU サービスに対して送信インターフェイスを使用できるようにルータを設定します。

```
Router(config-if)# ip wccp 82 redirect out
```



スタンドアロン Content Engine が WCCP Version 2 対応ルータからリダイレクトされた WMT MMS 要求を受け入れ可能にするには、事前にスタンドアロン Content Engine で WMT MMS 透過キャッシングを設定する必要があることに注意してください。このトピックに関する詳細は、「[WMT 要求の透過リダイレクションの設定](#)」(P. 9-40) を参照してください。

## ルータ上での wmt-rtspu サービス (サービス 83) の設定

wmt-rtspu サービス (サービス 83) は、事前定義 WCCP Version 2 メディア キャッシング サービスです。このサービスは、WCCP Version 2 対応ルータが RTSP クライアント要求を透過的に Windows Media 9 Player から Content Engine 上の単一ポートにリダイレクトすることを許可します (Content Engine は、WMT RTSP 透過キャッシング用に設定された、透過プロキシサーバとして動作します)。wmt-rtspu サービスは、ACNS 5.3.1 ソフトウェア リリースで追加されました。また、これは rtspu サービスとも呼ばれます。

Content Engine は、標準 RTSPU ポート (デフォルト ポート 5005) 上でリダイレクトされた RTSP 要求を待ち受けます。デフォルト ポート (ポート 5005) 以外で WMT RTSP トラフィックを代行受信するには、ユーザ定義 WCCP Version 2 サービスを設定します (サービス 90 ~ 97)。

ルータ上で wmt-rtspu サービス (サービス 83) を設定する手順は、次のとおりです。

**ステップ 1** ルータ上で WCCP Version 2 を有効にします。

```
Router# configure terminal  
Router(config)# ip wccp version 2
```

**ステップ 2** ルータ上で wmt-rtspu サービス (サービス 83) を有効にします。

```
Router(config)# ip wccp 83
```

**ステップ 3** wmt-rtspu サービスを実行するインターフェイスを指定します。

```
Router(config)# interface type number
```

**ステップ 4** wmt-rtspu サービスに対して送信インターフェイスを使用できるようにルータを設定します。

```
Router(config-if)# ip wccp 82 redirect out
```

また、WMT RTSP 要求の Content Engine への透過リダイレクションをサポートするために、WCCP ルータ上で rtsp サービス (サービス 80) を設定する必要があります。

また、スタンドアロン Content Engine が WCCP Version 2 対応ルータからリダイレクトされた WMT RTSP 要求を受け入れ可能にするには、事前にスタンドアロン Content Engine で WMT RTSP 透過キャッシングを設定する必要があることに注意してください。このトピックに関する詳細は、「[スタンドアロン Content Engine 上の WMT RTSP ストリーミングおよびキャッシング サービスの設定](#)」(P. 9-21) を参照してください。

## ルータ上でのユーザ定義 WCCP サービス（サービス 90 ～ 97）の設定

WCCP Version 2 を使用してユーザ定義 WCCP サービス（サービス 90 ～ 97）をサポートできるようにルータを設定する手順は、次のとおりです。

**ステップ 1** ルータ上で WCCP Version 2 を有効にします。

```
Router# configure terminal  
Router(config)# ip wccp version 2
```

**ステップ 2** ユーザ定義サービス（たとえば、サービス 90）用の WCCP 機能を有効にします。

```
Router(config)# ip wccp 90
```

**ステップ 3** ルータ上でサービス 90 を実行するインターフェイスを指定します。

```
Router(config)# interface type number
```

**ステップ 4** サービス 90 に対して送信インターフェイスを使用できるように Content Engine を設定します。

```
Router(config-if)# ip wccp 90 redirect out
```

また、Content Engine が WCCP Version 2 対応ルータからリダイレクトされたプロキシパケットを受け入れ可能にするには、事前にスタンドアロン Content Engine 上でユーザ定義 WCCP サービス（たとえば、サービス 90）を設定する必要もあることに注意してください。このトピックに関する詳細は、「[ユーザ定義 WCCP サービスをサポートするためのスタンドアロン Content Engine の設定](#)」（P. 6-14）を参照してください。

## ルータ上での custom-web-cache サービス（サービス 98）の設定

custom-web-cache サービス（サービス 98）は、事前定義 WCCP Version 2 web-caching サービスです。このサービスは、WCCP Version 2 対応ルータが HTTP トラフィックを Content Engine に、ポート 80 以外の複数のポートでリダイレクトすることを許可します。Content Engine は、透過プロキシ転送サーバとして機能します。この WCCP サービスにより、WCCP がリダイレクトした HTTP 要求を複数のポート（最大 8 つのポート）で待ち受けできるように Content Engine を設定することができ、ユーザ定義 WCCP サービス（サービス 90 ～ 97）を設定する必要はありません。

WCCP Version 2 を使用して custom-web-cache サービス（サービス 98）をサポートできるようにルータを設定する手順は、次のとおりです。

**ステップ 1** ルータ上で WCCP Version 2 を有効にします。

```
Router# configure terminal  
Router(config)# ip wccp version 2
```

**ステップ 2** ルータ上で custom-web-cache サービス（サービス 98）を有効にします。

```
Router(config)# ip wccp 98
```

ステップ 3 custom-web-cache サービスを実行するインターフェイスを指定します。

```
Router(config)# interface type number
```

次の例では、イーサネット 0 インターフェイスが custom-web-cache サービスを実行するように設定されています。

```
Router(config)# interface ethernet 0
```

ステップ 4 custom-web-cache サービスに送信インターフェイスを使用するように、ルータを設定します。

```
Router(config-if)# ip wccp 98 redirect out
```

---

また、Content Engine が複数のポートで WCCP Version 2 対応ルータからリダイレクトされた Web キャッシュ プロキシ パケットを受け入れ可能にするには、事前にスタンドアロン Content Engine 上で custom-web-cache サービスを設定する必要もあることに注意してください。このトピックに関する詳細は、「[スタンドアロン Content Engine に対するカスタム Web キャッシュ サービス \(サービス 98\) の設定](#)」(P. 7-21) を参照してください。

## ルータ上での reverse-proxy サービス (サービス 99) の設定

reverse-proxy サービス (サービス 99) は、事前定義 WCCP Version 2 サービスです。このサービスは、WCCP Version 2 対応ルータが、リバース プロキシ パケットを、透過リバース プロキシ サーバとして機能しているスタンドアロン Content Engine にリダイレクトすることを許可します。

WCCP Version 2 を使用して reverse-proxy サービス (サービス 99) をサポートするようにルータを設定する手順は、次のとおりです。

ステップ 1 ルータ上で WCCP Version 2 を有効にします。

```
Router# configure terminal
Router(config)# ip wccp version 2
```

ステップ 2 ルータ上で reverse-proxy サービス (サービス 99) を有効にします。

```
Router(config)# ip wccp 99
```

ステップ 3 reverse-proxy サービスを実行するインターフェイスを指定します。

```
Router(config)# interface type number
```

次の例では、イーサネット 0 インターフェイスが reverse-proxy サービスを実行するように設定されています。

```
Router(config)# interface ethernet 0
```

- ステップ 4** reverse-proxy サービスに送信インターフェイスを使用するように、ルータを設定します。ルータは、イーサネット インターフェイス 0 でリバース プロキシ パケットを確認して、それらのパケットを透過的に Content Engine にリダイレクトする必要があるかを判定します (Content Engine は、透過リバース プロキシ サーバとして動作します)。

```
Router(config-if)# ip wccp 99 redirect out
```

---

また、Content Engine が WCCP Version 2 ルータからリダイレクトされた リバース プロキシ パケットを受け入れ可能にするには、事前にスタンドアロン Content Engine で reverse-proxy サービス (サービス 99) を設定する必要もあることに注意してください。このトピックに関する詳細は、「[スタンドアロン Content Engine における HTTP リバース プロキシ キャッシングの設定](#)」(P. 7-24) を参照してください。

## ルータ上での WCCP 統計情報の削除

特定のサービス、またはすべてのサービスに対して、WCCP Version 2 ルータ上の WCCP 統計情報を削除するには、**clear ip wccp EXEC** コマンドを使用します。

```
clear ip wccp {web-cache | service-number}
```

ここで各パラメータの意味は、次のとおりです。

- **web-cache** で、ルータが Web キャッシュ サービスの統計情報を削除する必要があることが指定されます。
- **service-number** で、ルータが指定されたサービスの統計情報を削除する必要があることが指定されます。サービス グループ番号は、0 ~ 99 です。

たとえば、ルータに reverse-proxy サービス (サービス 99) の統計情報を削除するように指示するには、WCCP Version 2 対応ルータ上で次のコマンドを入力します。

```
Router# clear ip wccp web-cache 99
```

## WCCP レイヤ 2 のサポートの設定

ルータまたはスイッチ上の WCCP は、ハードウェアでレイヤ 2 の WCCP のトラフィック代行受信機能、および宛先変更機能を部分的または完全に提供する、スイッチング ハードウェアを利用できます。これによって、Content Engine は、互換 Cisco スイッチに直接接続されている場合、レイヤ 2 または MAC アドレス リライト リダイレクション方式を実行できます。このリダイレクト プロセスはスイッチング ハードウェア内で処理が加速されるため、この方式は GRE を使用したレイヤ 3 リダイレクションよりも効率的に実行されます。

Content Engine には、スイッチとのレイヤ 2 接続が必要です。GRE トンネルでは、スイッチと Content Engine 間のスイッチは、CLI から **l2-redirect** オプションを指定して、カプセル化パケットを転送するカットスルー方式です。

レイヤ 2 転送を選択する場合、WCCP Version 2 対応ルータまたはスイッチと Content Engines 間の負荷分散には次の 2 つの方式があります。

- ハッシュ アサイメント

Catalyst 6000 および 6500 シリーズ スイッチの場合、この負荷分散方式は、WCCP レイヤ 2 Policy Feature Card (PFC) リダイレクションと呼ばれます。この方式は、Supervisor Engine 1A と Multilayer Switch Feature Card 2 (MSFC2) を組み合わせて使用し、最高 3 ギガビット / 秒の転送パフォーマンスを実現します。

- マスク アサイメント

この負荷分散方式は、WCCP レイヤ 2 Policy Feature Card 2 (PFC2) リダイレクションと呼ばれています。この方式では、Supervisor Engine 2 と MSFC2 を組み合わせて使用しています。

Content Engine GUI または CLI コマンドを使用して、特定の WCCP サービスの負分散方式を Content Engine 上で設定できます。Content Engine がサポートしているすべての WCCP サービスは、次の CLI コマンドを使用し、ハッシュ アサイメントまたはマスク アサイメントの負分散方式をレイヤ 2 転送と連携してサポートします。使用するコマンドは、**wccp custom-web-cache**、**wccp media-cache**、**wccp reverse-proxy**、**wccp service-number**、**wccp web-cache**、**wccp wmt**、および **wccp rtsp** です。Content Engine クラスタの WCCP サービスごとに 1 つの負分散方式 (ハッシュとマスク) を指定することができます。たとえば、Content Engine クラスタ A に、3 つの WCCP サービスを定義する場合、クラスタ A 内のサービスのうち 2 つは、ハッシュ負分散方式を使用します。クラスタ A 内の 3 番目のサービスは、マスク負分散方式を使用します。



(注) レイヤ 2 リダイレクションは、Content Engine CLI を使用するマスク アサイメント負荷分散方式でのみ有効にすることができます（これは、Content Engine GUI ではサポートされません）。

ハッシュ負荷分散方式の設定方法については、次の[ハッシュ負荷分散方式を使用するレイヤ 2 転送の設定](#)を参照してください。マスク負荷分散方式の設定方法については、「[マスク負荷分散方式を使用するレイヤ 2 転送の設定](#)」(P. 6-39) を参照してください。

## ハッシュ負荷分散方式を使用するレイヤ 2 転送の設定

2 つのタイプのパケット転送方式でも（レイヤ GRE およびレイヤ 3 リダイレクション）、負荷分散方式としてハッシュをサポートしています。ハッシュでは、リダイレクトされたトラフィックが Content Engine クラスターの複数の Content Engine で負荷分散する方法を指定できます。

Content Engine 上でユーザ定義 WCCP Version 2 サービスを設定する場合、特定のユーザ定義 WCCP Version 2 サービスに対してハッシュパラメータ（たとえば、発信元 IP アドレスでハッシュ）を設定できます。ユーザ定義 WCCP サービス（サービス 90 ~ 97）のデフォルトのハッシュアサイメントは、宛先 IP アドレスでのハッシュです。任意のユーザ定義 WCCP サービスに対するデフォルトのハッシュアサイメントを変更するには、**wccp service-number** グローバル設定コマンドを使用します。

次の例では、**wccp service-number** コマンドを使用して、ユーザ定義 WCCP サービス（この場合、サービス 90）を、宛先 IP アドレスでのハッシュではなく、発信元 IP アドレスでのハッシュに設定しています。

```
ContentEngine(config)# wccp service-number 90 router-list-num 1 port-list-num 1
application cache hash-source-ip
```

表 6-6 では、デフォルトのハッシュアサイメントをリストしています。事前定義 WCCP サービスのデフォルトのハッシュアサイメントは、変更できないことに注意してください。

表 6-6 WCCP Version 2 シリーズのデフォルトのハッシュアサイメント

WCCP サービス タイプ	サービス番号 (ID)	サービスのデフォルトのハッシュアサイメント
ユーザ定義 WCCP サービス	90 ~ 97	デフォルトのハッシュアサイメントは宛先 IP アドレスでのハッシュ
事前定義 WCCP サービス		
web-cache	0	宛先 IP アドレスでハッシュ
dns caching	53	発信元ポートでハッシュ
ftp-native	60	宛先 IP アドレスでハッシュ
https-cache	70	発信元 IP アドレスでハッシュ
rtsp	80	宛先 IP アドレスでハッシュ
mmst	81	宛先 IP アドレスでハッシュ
mmsu	82	宛先 IP アドレスでハッシュ
wmt-rtspu	83	宛先 IP アドレスでハッシュ
custom-web-cache	98	宛先 IP アドレスでハッシュ
reverse-proxy	99	発信元 IP アドレスと発信元ポートでのハッシュ

次の例では、負荷分散方式にハッシュ アサイメントを使用して、Multilayer Switch Feature Card (MSFC) と Supervisory Engine 1A (SUP 1A) を実装している Catalyst 6500 シリーズ スイッチからレイヤ 2 リダイレクトトラフィックを受信する Content Engine を設定する方法を示しています。

**ステップ 1** Content Engine 上で WCCP Version 2 を有効にします。

```
ContentEngine# configure terminal
ContentEngine(config)# wccp version 2
```

**ステップ 2** Content Engine でルータ リストを作成します。次の例では、ルータ リスト 1 が作成され、1 台の WCCP Version 2 対応ルータが含まれています (IP アドレス 172.16.55.1 のルータ)。

```
ContentEngine(config)# wccp router-list 1 172.16.55.1
```

**ステップ 3** Content Engine 上で標準 Web キャッシュ サービス (サービス 0) を設定します。

ステップ 2 で作成したルータ リストを使用してこの WCCP サービスを設定します。**l2-redirect** オプションを入力して、このサービスのパケット転送方式として (GRE とは反対の) レイヤ 2 リダイレクションを指定します。マスク アサイメント方式は指定されていないため、デフォルトのハッシュ アサイメント方式を使用してリダイレクトされた要求の負荷分散が行われます。

```
ContentEngine(config)# wccp web-cache router-list-num 1 l2-redirect
```

**ステップ 4** **show wccp services detail** EXEC コマンドを使用して、確認できるように設定を表示します。

```
ContentEngine# show wccp services detail
```

**ステップ 5** 実行設定を不揮発性メモリに書き込みます。

```
ContentEngine# copy running-config startup-config
```

## マスク負荷分散方式を使用するレイヤ 2 転送の設定

どちらのタイプのパケット転送方式でも (GRE およびレイヤ 2 リダイレクション)、負荷分散方式としてマスクをサポートしています。Content Engine で異なるマスク (たとえば、宛先 IP マスク) を指定するには、**wccp service-name mask** グローバル設定コマンドを使用します。

特定の WCCP Version 2 サービスのデフォルト マスクを変更するには、**wccp service-name mask** 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。たとえば、透過的にリダイレクトされた HTTPS 要求 (HTTP キャッシュ サービス) のマスクを設定するには、**wccp https-cache mask** 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。

```
ContentEngine(config)# wccp https-cache mask ?
dst-ip-mask       Specify sub-mask used in packet destination-IP address
dst-port-mask     Specify sub-mask used in packet destination-port number
src-ip-mask       Specify sub-mask used in packet source-IP address
src-port-mask     Specify sub-mask used in packet source-port number
```

```
wccp https-cache {mask {[dst-ip-mask hex_num] [dst-port-mask port_hex_num]
[src-ip-mask hex_num] [src-port-mask port_hex_num]}}
```

表 6-7 では、コマンドのパラメータを説明しています。

表 6-7 wccp https-cache CLI コマンドのパラメータ

パラメータ	説明
<b>mask</b>	Content Engine の配置に使用されるマスクを設定します。少なくとも 1 つのマスクを設定。最大 4 つのマスクを設定できます。
<b>dst-ip-mask</b>	(オプション) リダイレクトされたパケットの宛先 IP アドレスとの照合に使用されるマスクを設定。
<i>hex_num</i>	16 進数で定義される IP アドレス (たとえば、0xFC000000)。その範囲は、0x00000000 から FC000000 です。
<b>dst-port-mask</b>	(オプション) リダイレクトされたパケットの宛先ポート番号との照合に使用されるマスクを設定。
<i>port_hex_num</i>	16 進数で定義されたソース ポート マスク (たとえば、0xFC00)。ポート範囲は 0 から 65535 です。
<b>src-ip-mask</b>	(オプション) リダイレクトされたパケットの発信元 IP アドレスとの照合に使用されるマスクを設定。
<i>hex_num</i>	16 進数で定義される IP アドレス (たとえば、0xFC000000)。その範囲は、0x00000000 から FC000000 です。
<b>src-port-mask</b>	(オプション) リダイレクトされたパケットの発信元ポート番号との照合に使用されるマスクを設定。
<i>port_hex_num</i>	16 進数で定義されたソース ポート マスク (たとえば、0xFC00)。ポート範囲は 0 から 65535 です。

**show wccp masks service-name** EXEC コマンドを使用して、特定の WCCP Version 2 サービスのマスク設定を表示します。

```
ContentEngine(config)# show wccp masks ?
  custom-web-cache  Custom web caching service
  dns                DNS caching service
  ftp-native        Native FTP caching service
  https-cache       HTTPS caching service
  reverse-proxy     Reverse Proxy web caching service
  rtsp              Media caching service
  service-number    Custom-service number
  web-cache         Standard web caching service
  wmt                WMT service
  wmt-rtspu         WMT RTSPU service
```

次の例では、Multilayer Switch Feature Card 2 と Supervisory Engine 2 (MSFC2/SUP 2) を実装している Catalyst 6500 シリーズ スイッチから、リダイレクトされたレイヤ 2 トラフィックを受信するように、Content Engine を設定する方法を示しています。

**ステップ 1** Content Engine 上で WCCP Version 2 を有効にします。

```
ContentEngine# configure terminal
ContentEngine(config)# wccp version 2
```

**ステップ 2** Content Engine でルータ リストを作成します。次の例では、ルータ リスト 1 が作成され、これには WCCP Version 2 対応ルータが 1 台のみ含まれています (IP アドレス 172.16.55.1 のルータ)。

```
ContentEngine(config)# wccp router-list 1 172.16.55.1
```



- ステップ 3** Content Engine 上で Web キャッシュ サービスを設定します。手順 2 で作成されたルータ リストを使用してこの WCCP サービスを設定します。**l2-redirect** オプションを入力して、パケット転送方式として (GRE とは反対の) レイヤ 2 リダイレクションを指定します。**mask-assign** オプションを入力して、この WCCP サービスの負荷分散方式として (デフォルトのハッシュ アサイメント方式とは反対の) マスク アサイメントを指定します。

```
ContentEngine(config)# wccp web-cache router-list-num 1 l2-redirect mask-assign
```

- ステップ 4** 設定内容を検証できるように、その内容を表示します。

```
ContentEngine# show wccp services detail
```

- ステップ 5** 実行設定を不揮発性メモリに書き込みます。

```
ContentEngine# copy running-config startup-config
```

---

## スタンドアロン Content Engine の WCCP サービス設定例

ここでは、WCCP Version 2 を使用するスタンドアロン Content Engine の WCCP サービスを設定する簡単な例を示します。

- 例 1 : WCCP Version 1 を使用する web-cache サービスの設定 (P. 6-43)
- 例 2 : WCCP Version 2 を使用する web-cache サービスの設定 (P. 6-46)
- 例 3 : WCCP Version 2 を使用した HTTPS 透過キャッシング サービスの設定 (P. 6-48)
- 例 4 : スタンドアロン Content Engine での複数の WCCP Version 2 サービスの設定 (P. 6-49)

WCCP Version 1 または WCCP Version 2 のどちらかを使用して、標準 Web キャッシュ サービス (サービス 0) を設定する場合、次の重要事項に注意してください。

- Content Engine 上のパケットは、暗号化も圧縮もされていないことが必要で、また、「内部」ネットワークアドレス変換 (NAT) がある場合は、Content Engine はその一部であることが必要です。
- Content Engine と WCCP 対応ルータをファイアウォールで隔てることはできません。ファイアウォールでは、オリジン Web サーバ宛てのパケット トラフィックだけを処理し、そのサーバに代わって Content Engine がクライアントに送信するパケット トラフィックは処理しないからです。
- Web キャッシュ リダイレクト対応インターフェイスを超えて、サーバへのルート上に Content Engine を配置すると、IP ルート キャッシュにエントリが読み込まれません。
- Content Engine で標準 Web キャッシュ サービスを設定するには、Content Engine GUI も使用できます。しかし、ルータ上では、常時 CLI を使用して、標準 Web キャッシュ サービスを設定する必要があります。
- Web キャッシュ サービスをサポートするために WCCP 対応ルータを使用するには、インターネットに接続されているインターフェイス (ブラウザ) 上に IP アドレスを設定して、そのインターフェイスを Content Engine に接続する必要があります。ルータ上で **show ip interface EXEC** コマンドを使用して、IP 用に設定された、ルータのインターフェイスが、現在、使用可能かどうかを確認します。

インターフェイスが使用可能である場合、Cisco IOS ソフトウェアは、ルーティング テーブルに直接接続ルートを自動的に入力します。使用可能なインターフェイスとは、Cisco IOS ソフトウェアがパケットの送受信時に使用できるインターフェイスです。Cisco IOS ソフトウェアは、インターフェイスが使用不可である場合、直接接続されているルーティングのエントリをルーティング テーブルから削除します。Cisco IOS ソフトウェアは、このエントリを削除すると、動的ルーティング プロトコルを使用して、ネットワークへのバックアップルート (ある場合) を判別できます。

インターフェイスで双方向通信が可能である場合は、回線プロトコルに「up」のマークが付きます。インターフェイス ハードウェアが使用可能である場合は、インターフェイスに「up」のマークが付きます。

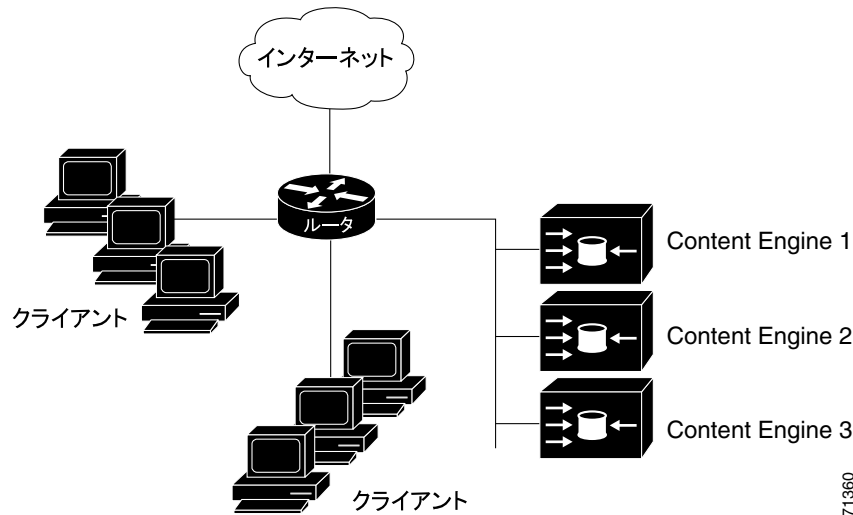
- オプションのインターフェイスのタイプを指定すると、特定のインターフェイスだけについての情報が表示されます。
- オプションの引数を指定しない場合は、すべてのインターフェイスについての情報が表示されます。

非同期インターフェイスがポイントツーポイント プロトコル (PPP)、またはシリアル ライン インターネット プロトコル (SLIP) を使用してカプセル化されている場合、IP ファースト スイッチングが有効になります。PPP または SLIP を使用してカプセル化された非同期インターフェイスに対して **show ip interface** コマンドを入力すると、IP 高速スイッチングが有効になっていることを示すメッセージが表示されます。

## 例 1 : WCCP Version 1 を使用する web-cache サービスの設定

WCCP Version 1 を使用する場合、標準 web-cache サービス（サービス 0）を実行する 1 台の WCCP 対応ルータと 1 台または複数の Content Engine を設定します。図 6-4 では、1 台の WCCP Version 1 対応ルータと通信している 3 台の Content Engine のクラスタから構成された、WCCP Version 1 ネットワーク構成例を示しています。

図 6-4 WCCP Version 1 を使用した Content Engine のネットワーク構成



71360



(注)

WCCP Version 1 では、1 台の WCCP 対応ルータが 1 つの Content Engine のクラスタを処理し、そのルータがクラスタのデフォルト ホームルータになります。WCCP Version 1 では、クラスタを処理しているこの 1 台のルータが、すべての IP パケットリダイレクションを行うデバイスです。

WCCP Version 1 が使用される場合、Content Engine とこれらの Content Engine と通信する 1 つの WCCP 対応ルータ（ホームルータ）の間で、次の順序でイベントが発生します。

1. 各 Content Engine は、Content Engine クラスタと通信する WCCP 対応ルータの IP アドレスを記録します。
2. Content Engine は自身の IP アドレスを WCCP 対応ルータに送信し、クラスタ内の Content Engine 相互に存在を通知します。
3. WCCP 対応ルータは Content Engine に応答し、各 Content Engine がクラスタ内の他の Content Engine に接続できるようにし、クラスタ内の Content Engine のアドレスのビュー（リスト）を提供して、すべての Content Engine が互いに認識できることを示します。
4. このビューが確立された後、1 台の Content Engine がリードエンジンとして指定され、IP パケットのリダイレクト方法を WCCP 対応ルータに指示します。

リード Content Engine は、クラスタで番号が最小の IP アドレスを持つものとして定義され、クラスタをサービスする WCCP Version 1 対応ルータ（ホームルータ）から参照されます。

次の例では、Content Engine CLI を使用して、WCCP Version 1 を使用する標準 Web キャッシュ サービス（サービス 0）の有効化および設定を行う方法を説明します。WCCP Version 1 では、1 つのサービス（標準 Web キャッシュ サービス）と 1 台の WCCP 対応ルータ（ホームルータ）だけを設定することができます。Content Engine のクラスタがある場合でも、1 台のみの WCCP Version 1 対応ルータが Content Engine のクラスタと通信し、クラスタのデフォルト ホームルータになります。

この例では、IP アクセス リストは、スタンドアロン Content Engine にリダイレクトされる Web 関連パケットを制御するために使用します。また、この例では、単一ルータおよびスタンドアロン Content Engine 上に設定した後に、web-cache サービスが適切に動作していることを確認する方法も示しています。

**ステップ 1** 標準 Web キャッシュ サービスに対して WCCP 対応ルータを使用するには、インターネットに接続されているインターフェイス（ブラウザ）上に IP アドレスを設定して、そのインターフェイスをスタンドアロン Content Engine に接続します。

ルータ上で **show ip interface EXEC** コマンドを使用して、IP 用に設定されたルータのインターフェイスが使用可能かどうかを確認します。

**ステップ 2** **show ip wccp EXEC** コマンドを入力して、WCCP がルータ上で現在有効になっているかどうかを確認します。

**ステップ 3** WCCP Version 1 を使用するようにルータを有効にし、WCCP Version 1 を使用してルータを設定し、192.168.196.51 の宛先をもたない Web 関連のパケットをスタンドアロン Content Engine にリダイレクトします。

```
Router# configure terminal
Router(config)# ip wccp version 1
Router(config)# access-list 100 deny ip any host 192.168.196.51
Router(config)# access-list 100 permit ip any any
Router(config)# ip wccp web-cache redirect-list 100
Router(config)# interface Ethernet 0
Router(config)# ip wccp web-cache redirect out
Router(config-if)# end
Router#
%SYS-5-CONFIG_I: Configured from console by console.
```

**ステップ 4** スタンドアロン Content Engine 上で WCCP Version 1 を有効にします。

```
ContentEngine# configure terminal
ContentEngine(config)# wccp version 1
```

**ステップ 5** **wccp home-router ip-address** グローバル コンフィギュレーション コマンドを入力して、スタンドアロン Content Engine がホーム ルータを指すようにします。これは、IP のデフォルト ゲートウェイの IP アドレスである場合もあります。

次の例では、ホーム ルータの IP アドレスは 192.168.51.102 です。

```
ContentEngine(config)# wccp home-router 192.168.51.102
```



(注) また、スタンドアロン Content Engine で WCCP Version 1 Web キャッシュ サービスを設定するには、Content Engine GUI も使用できます (**WCCP > Enable WCCP** の順に選択します)。Enable WCCP ウィンドウの詳細については、ウィンドウの **HELP** ボタンをクリックしてください。

**ステップ 6** 「スタンドアロン Content Engine における標準 Web キャッシュ サービス（サービス 0）の設定」(P. 7-18) で説明されているように、Content Engine 上で標準 Web キャッシュ サービスを設定します。

**ステップ 7** `show wccp EXEC` コマンドを入力して、標準 `web-cache` サービスがこれで有効になったことを確認します。

```
ContentEngine# show wccp services
Services configured on this Content Engine
  Web-cache
ContentEngine#
```

Content Engine で `show wccp EXEC` コマンドの他のオプションを使用すると、スタンドアロン Content Engine で他の WCCP 情報を表示できます。たとえば、Content Engine の GRE (General Routing Encapsulation) パケット関連情報を表示するには、`show wccp` コマンドの `gre` オプションを指定します。

**ステップ 8** WCCP 対応ルータ上で、`show ip wccp web-cache` コマンドを入力し、WCCP がルータ上で有効になっていること、およびルータが Web キャッシュとして設定したスタンドアロン Content Engine を認識していることを確認します。

次の例では、ホーム ルータの設定直後に `show ip wccp web-caches` コマンドが入力されています。数秒後、2 番目の出力にあるように、IP アドレス 192.168.25.3 のスタンドアロン Content Engine の状態が「NOT Usable」から「Usable」に変化します。

```
Router# show ip wccp web-cache

WCCP Web-Cache information:
  IP Address:          192.168.25.3
  Protocol Version:   1.0
  State:              NOT Usable
  Initial Hash Info:  FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
                    FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
  Assigned Hash Info: 00000000000000000000000000000000
                    00000000000000000000000000000000
  Hash Allotment:    0 (0.00%)
  Packets Redirected: 0
  Connect Time:      00:00:06
```

```
Router# show ip wccp web-cache

WCCP Web-Cache information:
  IP Address          192.168.25.3
  Protocol Version:  0.3
  State:            Usable
  Initial Hash Info: FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
                    FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
  Assigned Hash Info: FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
                    FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
  Hash Allotment:   256 (100.00%)
  Packets Redirected: 0
  Connect Time:    00:00:31
```

**ステップ 9** WCCP Version 1 対応ルータ上で、`debug ip wccp events EXEC` コマンドを入力して、重要な WCCP イベントについての情報を表示します。

次の例では、この WCCP Version 1 対応ルータ上で使用可能な Web キャッシュのリストに 1 台の Content Engine が追加された場合の `debug ip wccp events EXEC` コマンドの出力を示しています。

```
Router# debug ip wccp events

WCCP-EVNT: Built I_See_You msg body w/1 usable web caches, change # 0000000A
WCCP-EVNT: Web Cache 192.168.25.3 added
WCCP-EVNT: Built I_See_You msg body w/2 usable web caches, change # 0000000B
WCCP-EVNT: Built I_See_You msg body w/2 usable web caches, change # 0000000C
```

**ステップ 10** WCCP Version 1 対応ルータ上で、**debug ip wccp packets** コマンドを入力し、このルータ上で送信または受信された各 WCCP パケットについての情報を表示します。

次の例では、**debug ip wccp packets** コマンドの出力を示しています。このルータは、192.168.25.3 に存在する Content Engine にキープアライブ パケットを送信しています。各キープアライブ パケットには、ID 番号が関連付けられています。Content Engine がルータからキープアライブ パケットを受信すると、ID 番号を付けて応答をルータに戻します。

```
Router# debug ip wccp packets
WCCP-PKT: Received valid Here_I_Am packet from 192.168.25.3 w/rcvd_id 00003532
WCCP-PKT: Sending I_See_You packet to 192.168.25.3 w/ rcvd_id 00003534
WCCP-PKT: Received valid Here_I_Am packet from 192.168.25.3 w/rcvd_id 00003533
WCCP-PKT: Sending I_See_You packet to 192.168.25.3 w/ rcvd_id 00003535
WCCP-PKT: Received valid Here_I_Am packet from 192.168.25.3 w/rcvd_id 00003534
WCCP-PKT: Sending I_See_You packet to 192.168.25.3 w/ rcvd_id 00003536
WCCP-PKT: Received valid Here_I_Am packet from 192.168.25.3 w/rcvd_id 00003535
WCCP-PKT: Sending I_See_You packet to 192.168.25.3 w/ rcvd_id 00003537
WCCP-PKT: Received valid Here_I_Am packet from 192.168.25.3 w/rcvd_id 00003536
WCCP-PKT: Sending I_See_You packet to 192.168.25.3 w/ rcvd_id 00003538
WCCP-PKT: Received valid Here_I_Am packet from 192.168.25.3 w/rcvd_id 00003537
WCCP-PKT: Sending I_See_You packet to 192.168.25.3 w/ rcvd_id 00003539
```



**ヒント** WCCP によってリダイレクトされたパケットのルータのカウンタをクリアするには、WCCP 対応ルータ上で、**clear ip wccp EXEC** コマンドを使用します。

## 例 2 : WCCP Version 2 を使用する web-cache サービスの設定

次の例では、クライアントとスタンドアロン Content Engine が同一サブネット上にあり、WCCP Version 1 ではなく WCCP Version 2 が使用されている場合に、Content Engine CLI を使用して標準 web-cache サービス（サービス 0）を設定する方法を示しています。

**ステップ 1** ステップ 3 のルータ リストに追加される各ルータ上で、WCCP Version 2 が有効になっていることを確認します。

```
Router(config)# ip wccp version 2
```

**ステップ 2** **ip wccp web-cache password** グローバル設定コマンドを入力して、WCCP 対応ルータ上で標準 Web キャッシュ サービスを設定し、このルータのパスワードも設定します。

```
Router(config)# ip wccp web-cache [password [0-7] [password]]
```

ここで各パラメータの意味は、次のとおりです。

- **password** は、指定されたサービス グループから受信されるメッセージに MD5 認証を適用するように、WCCP 対応ルータに指示する文字列です。この認証によって受け入れられないメッセージは、廃棄されます。
- 0 ~ 7 は、パスワードの暗号化に使用される HMAC MD5 アルゴリズムを示すオプション値です。暗号化されたパスワードが Content Engine に対して作成されるときに、この値が生成されます。

- *password* は、WCCP 対応ルータと Content Engine 間の接続に対するセキュリティを確立するために、HMAC MD5 値と組み合わせるオプションのパスワード名です。

**ステップ 3** 標準 web-cache サービス (WCCP Version 2 を使用した HTTP 透過キャッシング) 用に設定するスタンドアロン Content Engine で、ルータ リストを作成します (たとえば、ルータ リスト 1)。

```
ContentEngine(config)# wccp router-list 1 10.10.10.1
```

**ステップ 4** Content Engine で標準 Web キャッシュ サービスを有効にし、この Content Engine のこの特定のサービスをサポートする WCCP Version 2 対応ルータ (ルータ リスト) を指定します (つまり、これは HTTP 要求をポート 80 で、この Content Engine にリダイレクトします)。

この WCCP サービスと作成したルータ リストを関連付けます。レイヤ 2 リダイレクション オプションを割り当てます。マスク アサイメント方式が指定されていない場合、負荷分散方式のデフォルトはハッシュ アサイメントです。

```
ContentEngine(config)# wccp web-cache router-list-num 1 12-redirect
```



**ヒント** スタンドアロン Content Engine で WCCP Version 2 Web キャッシュ サービスを設定するには、Content Engine GUI も使用できます (Content Engine GUI から **WCCP > Web Cache** を選択します)。Content Engine GUI を使用し、Content Engine で WCCP Version 2 設定する場合には、Content Engine GUI ウィンドウのそれぞれの各サービスで、示されたルータ リストを指定する必要があります。Web Cache ウィンドウ (**WCCP > Web Cache**)、Reverse Proxy ウィンドウ (**WCCP > Reverse Proxy**)、Custom Web Cache ウィンドウ (**WCCP > Custom Web Cache**)、および WCCP Services ウィンドウ (**WCCP > Services**)。

**ステップ 5** Content Engine 上で WCCP Version 2 を有効にします。

```
ContentEngine(config)# wccp version 2
```

**ステップ 6** グローバル設定モードを終了します。

```
ContentEngine(config)# exit
```

**ステップ 7** 実行コンフィギュレーションを Content Engine の不揮発性メモリに書き込みます。

```
ContentEngine# write memory
```

**ステップ 8** ルータは WCCP Version 2 を実行するように設定されているため、ルータ上で WCCP をモニタします。

```
Router# show ip wccp
```

または

```
Router# show ip wccp {web-cache | 90-99}
```

**ステップ 9** WCCP 対応ルータが特定のサービス グループ内で検出した Content Engine に関する情報を、ルータに照会します。この情報は、90 から 99 の範囲の WCCP サービスに対して表示できます。

```
Router# show ip wccp {web-cache | 90-99} detail
```

**ステップ 10** `ip wccp direct` コマンドがインターフェイス上で設定されているかどうかを判別します。

```
Router# show ip interface
```

**ステップ 11** 特定の WCCP サービス グループ内のどの装置が検出されたか、また現在のルータが接続されている他のルータすべてが認識できないのは、どの Content Engine かを表示します。この情報は、90 から 99 のサービス グループに対して表示できます。

```
Router# show ip wccp {web-cache | 90-99} view
```

### 例 3 : WCCP Version 2 を使用した HTTPS 透過キャッシング サービスの設定

次の例では、スタンドアロン Content Engine 上で、ユーザ定義 WCCP Version 2 サービスおよび HTTPS 透過キャッシングを設定するための、Content Engine CLI の使用方法を示しています。この例では、サービス番号 95 がユーザ定義サービスです。

**ステップ 1** デフォルトのポート以外のポートで、複数の WCCP Version 2 対応ルータにより、透過的に代行受信およびリダイレクトされている HTTPS 要求を Content Engine が受け入れるようにサービス 95 を設定します。

最初に、サービス 95 で使用する ルータ リストおよびポート リストを作成する必要があります (たとえば、サービス 95 用にポート リスト 1 を作成します)。ポート リストには、WCCP Version 2 対応ルータがサービス 95 の WCCP リダイレクションをサポートするポート番号が含まれています。

```
ContentEngine# configure terminal
ContentEngine(config)# wccp service-number 95 router-list-num 1
ContentEngine(config)# wccp service-number 95 router-list-num 1 port-list-num 1
```

**ステップ 2** サービス 95 を設定する場合、そのトラフィックが Content Engine 上のキャッシングアプリケーション、HTTP キャッシングアプリケーション、またはストリーミングアプリケーションのどれにリダイレクトされるかを指定する必要があります。

```
ContentEngine(config)# wccp service-number 95 router-list-num 1 port-list-num 1
application ?
  cache           Direct traffic to the caching application
  https-cache     Direct traffic to the HTTPS caching application
  streaming       Direct traffic to the streaming media application
```



- ステップ 3** Content Engine が、その HTTPS アプリケーションにリダイレクトされたトラフィックを受け入れることを指定します。ルータ リスト番号 1 の WCCP Version 2 対応ルータは、HTTPS トラフィックを Content Engine の HTTPS キャッシング アプリケーションにリダイレクトします。Content Engine は、ポート リスト 1 で指定されているポートで、そのような WCCP がリダイレクトした要求を待ち受けます。

```
ContentEngine(config)# wccp service-number 95 router-list-num 1 port-list-num 1
https-cache
```

ACNS 5.2.1 ソフトウェアまたはそれ以降では、accept-all モードは https-cache でサポートされています。accept-all モードは、HTTPS トラフィックのフィルタリングをサポートします。このモードは、従来の WCCP サービスと同様に機能します（たとえば、デフォルトですべての Web トラフィックを代行受信する web-cache キャッシュ サービス）。

デフォルトでは、Content Engine はすべての HTTPS トラフィックを受け入れます。

```
ContentEngine(config)# wccp https-cache ?
accept-all      Accept all HTTPS traffic by default
mask            Specify mask used for CE assignment
router-list-num Router list number
```



(注) **wccp https-cache accept-all** グローバル設定コマンドが使用される場合、HTTPS キャッシュ (HTTPS 透過キャッシング用に設定されている Content Engine) は、「すべてを受け入れる」モード (すべての HTTPS トラフィックが代行受信される) で機能します。それ以外の場合、HTTPS キャッシュは ACNS 5.1.x ソフトウェアにある「受け入れ限定」モードで機能します。

- ステップ 4** Content Engine 上で WCCP Version 2 を有効にします。

```
ContentEngine(config)# wccp version 2
```

## 例 4 : スタンドアロン Content Engine での複数の WCCP Version 2 サービスの設定

次の例では、スタンドアロン Content Engine 上で、16 個の WCCP Version 2 サービスを設定するための Content Engine CLI の使用方法を示しています。

- ステップ 1** 16 個の WCCP Version 2 サービス (8 個のユーザ定義サービスと 8 個の事前定義サービス) をサポートする WCCP Version 2 対応ルータを含むルータ リストを設定します。この場合、ルータ リスト 1 にはルータが 1 台含まれています (IP アドレス 10.1.202.1 の WCCP Version 2 対応ルータ)。

```
ContentEngine(config)# wccp router-list 1 10.1.202.1
```

- ステップ 2** 8 つのポート リストを設定します (ポート リスト、番号 1 ~ 8)。

これらのポート リストで、特定の WCCP Version 2 対応ルータから着信するトラフィックを Content Engine が待ち受けるポート番号を指定します。これらのポート リストによって、Content Engine が着信する WCCP 要求を複数のポートで待ち受けるように設定することができます。デフォルトでは、Content Engine はポート 80 で着信トラフィックを受信します。作成する 8 個のユーザ定義 WCCP

Version 2 サービスのそれぞれに1つのポートリストを作成します (サービス 90 ~ 97)。ポートリストごとに最大8つのポートを定義できます。次の場合、各ポートリストには単一のポートがあります (たとえば、ポートリスト1にはポート32が含まれます)。

```
ContentEngine(config)# wccp port-list 1 32
ContentEngine(config)# wccp port-list 2 33
ContentEngine(config)# wccp port-list 3 34
ContentEngine(config)# wccp port-list 4 35
ContentEngine(config)# wccp port-list 5 36
ContentEngine(config)# wccp port-list 6 37
ContentEngine(config)# wccp port-list 7 38
ContentEngine(config)# wccp port-list 8 39
```

- ステップ 3** Content Engine で標準 Web キャッシュ サービス (サービス 0) を有効にして、ルータ リスト 1 と、この最初の事前定義 WCCP サービスとを関連付けます。

```
ContentEngine(config)# wccp web-cache router-list-num 1
```

これにより Content Engine は、ルータ リスト 1 のルータからリダイレクトされた HTTP 要求を、ポート 80 で待ち受けするように設定されます。



(注) 「HTTP 要求」という用語は、HTTP、FTP-over-HTTP、および HTTPS-over-HTTP の各要求をまとめて指すために使用されています。

- ステップ 4** Content Engine 上で reverse-proxy キャッシング サービス (サービス 99) を有効にして、ルータ リスト 1 と、この2番目の事前定義 WCCP Version 2 サービスとを関連付けます。

```
ContentEngine(config)# wccp reverse-proxy router-list-num 1
```

Content Engine は、ルータ リスト 1 のルータからリダイレクトされた リバース プロキシ要求を、ポート 80 で待ち受けます。

- ステップ 5** Content Engine 上で custom-web-cache サービス (サービス 98) を有効にして、ルータ リスト 1 およびポート 31 と、この3番目の事前定義 WCCP Version 2 サービスとを関連付けます。

```
ContentEngine(config)# wccp custom-web-cache router-list-num 1 port 31
```

Content Engine は、ルータ リスト 1 の WCCP Version 2 対応ルータからリダイレクトされた HTTP 要求を、ポート 31 で待ち受けます。

- ステップ 6** Content Engine 上で RTSP サービス (サービス 80) を有効にして、ルータ リスト 1 と、この4番目の事前定義 WCCP Version 2 サービスとを関連付けます。

```
ContentEngine(config)# wccp rtsp router-list-num 1
```

Content Engine は、ルータ リスト 1 の WCCP Version 2 対応ルータからリダイレクトされた RTSP 要求を、標準 RTSP ポート (デフォルトポート 554) で待ち受けます。

- ステップ 7** Content Engine 上で WMT サービス（サービス 81 および 82）を有効にして、ルータ リスト 1 と、この 5 番目の事前定義 WCCP Version 2 サービスとを関連付けます。

```
ContentEngine(config)# wccp wmt router-list-num 1
```

このコマンドを使用後に、Content Engine は、ルータ リスト 1 の WCCP Version 2 対応ルータからリダイレクトされた WMT 要求を、デフォルト ポート（ポート 1755）で待ち受けます。

- ステップ 8** Content Engine 上で DNS キャッシング サービス（サービス 53）を有効にして、ルータ リスト 1 と、この 6 番目の事前定義 WCCP Version 2 サービスとを関連付けます。

```
ContentEngine(config)# wccp dns router-list-num 1
```

Content Engine は、ルータ リスト 1 の WCCP Version 2 対応ルータからリダイレクトされた DNS 要求を、ポート 80 で待ち受けます。

- ステップ 9** Content Engine 上で ftp-native キャッシング サービス（サービス 60）を有効にして、ルータ リスト 1 と、この 7 番目の事前定義 WCCP Version 2 サービスとを関連付けます。

```
ContentEngine(config)# wccp ftp-native router-list-num 1
```

Content Engine は、ルータ リスト 1 の WCCP Version 2 対応ルータからリダイレクトされた FTP ネイティブ要求を、ポート 80 で待ち受けます。これは、FTP ネイティブ キャッシング用です（Content Engine が FTP-over-HTTP 要求を直接クライアントのブラウザから受信し、要求されたコンテンツをキャッシュする場合に必要な FTP-over-HTTP キャッシングとは反対のものです）。

- ステップ 10** Content Engine で https-caching サービス（サービス 70）を有効にして、ルータ リスト 1 と、この 8 番目の事前定義 WCCP Version 2 サービスとを関連付けます。

```
ContentEngine(config)# wccp https-cache router-list-num 1
```

ACNS 5.1 ソフトウェアでは、HTTPS 要求は、WCCP モードの Content Engine 上でのみ SSL ターミネーションを行うことができます。ACNS 5.1 ソフトウェアでは、特定のサイト（Content Engine がサポートするように設定されていた HTTPS オリジン サーバ）への HTTPS 要求だけが WCCP モードで SSL ターミネーションが行われました。ACNS 5.1 ソフトウェアでは、Content Engine は、サポートするように明示的に設定されていない HTTPS サーバに送信された HTTPS 要求をバイパスします。SSL ターミネーションの詳細は、「[HTTPS クライアント要求の SSL 終了について](#)」(P. 7-26) を参照してください。

ACNS 5.1.x ソフトウェアでは、https-cache サービスに対して、1 種類の代行受信モード（accept-only モード）しかサポートされませんでした。accept-only モードでは、特定の HTTPS サーバ宛でのリダイレクトされた要求だけを受け入れるように、次のように Content Engine を設定する必要がありました。

```
ContentEngine(config)# wccp https-cache router-list-num 1
```

または

```
ContentEngine(config)# wccp service-number 95 router-list-num 1 port-list 1  
https-cache
```

前の例では両方とも、HTTPS サーバが Content Engine で設定されている場合 (**https server** グローバル設定コマンドを使用)、Content Engine はリダイレクトされた HTTPS トラフィックだけを受け入れます。

ACNS 5.2.1 ソフトウェアまたはそれ以降では、要求された HTTPS サーバが Content Engine 上で設定されている場合、Content Engine SSL は、WCCP モードと手動プロキシモードの HTTPS 要求を終了し、残りの HTTPS トラフィックをトンネルさせます。HTTPS 要求のトンネリングの詳細は、「[HTTPS クライアント要求のトンネリングについて](#)」(P. 7-27) を参照してください。特定の要求したコンテンツをキャッシュする場合、HTTPS サーバに適した証明書と鍵を Content Engine にインポートし、Content Engine にこれらのサーバをキャッシュするように設定します。スタンドアロン Content Engine の場合は、Content Engine CLI を使用してこれを実行します（「[HTTPS キャッシングに使用する証明書と秘密鍵の設定](#)」(P. 7-34) を参照）。

- ステップ 11** Content Engine 上で最初のユーザ定義 WCCP サービス（サービス 90）を有効にして、ルータ リスト 1 およびポート リスト 1 と、このサービスとを関連付けます。 **application cache** オプションを入力することにより、トラフィックが Content Engine のキャッシングアプリケーションにリダイレクトされるよう指定します。

```
ContentEngine(config)# wccp service-number 90 router-list-num 1 port-list-num 1
application cache
```

Content Engine は、ルータ リスト 1 のルータからリダイレクトされた要求を、ポート リスト 1（ポート 32）で待ち受けます。



**ヒント** この例で作成されたユーザ定義 WCCP サービス（サービス 90 ~ 97）のそれぞれに対して、**application cache** オプションを指定する必要があります。これは、WCCP ルータに、トラフィックを Content Engine のキャッシングアプリケーション（ストリーミングアプリケーションとは反対）にリダイレクトさせるためです。

- ステップ 12** Content Engine で 2 番目のユーザ定義 WCCP サービス（サービス 91）を有効にして、ルータ リスト 1 およびポート リスト 2 と、このサービスとを関連付けます。

```
ContentEngine(config)# wccp service-number 91 router-list-num 1 port-list-num 2
application cache
```

Content Engine は、ルータ リスト 1 の WCCP Version 2 対応ルータからリダイレクトされた要求を、ポート リスト 2（ポート 33）で待ち受けるように設定されます。

- ステップ 13** Content Engine で 3 番目のユーザ定義 WCCP サービス（サービス 92）を有効にして、ルータ リスト 1 およびポート リスト 3 と、このサービスとを関連付けます。

```
ContentEngine(config)# wccp service-number 92 router-list-num 1 port-list-num 3
application cache
```

Content Engine は、ルータ リスト 3 のルータからリダイレクトされた要求を、ポート リスト 1（ポート 34）で待ち受けます。

**ステップ 14** Content Engine で 4 番目のユーザ定義 WCCP サービス (サービス 93) を有効にして、ルータ リスト 1 およびポート リスト 4 と、このサービスとを関連付けます。

```
ContentEngine(config)# wccp service-number 93 router-list-num 1 port-list-num 4
application cache
```

Content Engine は、ルータ リスト 1 のルータからリダイレクトされた要求を、ポート リスト 4 (ポート 35) で待ち受けます。

**ステップ 15** Content Engine で 5 番目のユーザ定義 WCCP サービス (サービス 94) を有効にして、ルータ リスト 1 およびポート リスト 5 と、このサービスとを関連付けます。

```
ContentEngine(config)# wccp service-number 94 router-list-num 1 port-list-num 5
application cache
```

Content Engine は、ルータ リスト 5 のルータからリダイレクトされた要求を、ポート リスト 1 (ポート 36) で待ち受けます。

**ステップ 16** Content Engine で 6 番目のユーザ定義 WCCP サービス (サービス 95) を有効にして、ルータ リスト 1 およびポート リスト 6 と、このサービスとを関連付けます。

```
ContentEngine(config)# wccp service-number 95 router-list-num 1 port-list-num 6
application cache
```

Content Engine は、ルータ リスト 6 のルータからリダイレクトされた要求を、ポート リスト 1 (ポート 37) で待ち受けます。

**ステップ 17** Content Engine で 7 番目のユーザ定義 WCCP サービス (サービス 96) を有効にして、ルータ リスト 1 およびポート リスト 7 と、このサービスとを関連付けます。

```
ContentEngine(config)# wccp service-number 96 router-list-num 1 port-list-num 7
application cache
```

Content Engine は、ルータ リスト 7 のルータからリダイレクトされた要求を、ポート リスト 1 (ポート 38) で待ち受けます。

**ステップ 18** Content Engine で 8 番目のユーザ定義 WCCP サービス (サービス 97) を有効にして、ルータ リスト 1 およびポート リスト 8 と、このサービスとを関連付けます。

```
ContentEngine(config)# wccp service-number 97 router-list-num 1 port-list-num 8
application cache
```

Content Engine は、ルータ リスト 8 のルータからリダイレクトされた要求を、ポート リスト 1 (ポート 39) で待ち受けます。

**ステップ 19** Content Engine 上で WCCP Version 2 を有効にします。

```
ContentEngine(config)# wccp version 2
```

**ステップ 20** Content Engine 上で WCCP スロー スタート機能を無効にします。

```
ContentEngine(config)# no wccp slow-start enable
```

## ■ スタンドアロン Content Engine の WCCP サービス設定例

WCCP スロー スタート機能については、「[WCCP スロー スタートの設定](#)」(P. 15-11) を参照してください。

---

## リダイレクション方式としてのレイヤ 4 スwitチングの設定

レイヤ 4 スwitチング (Content Services Switch[CSS] スwitチ) が、要求を透過的にスタンドアロン Content Engine にリダイレクトするため使用されている場合に、透過リダイレクションを設定するには、次の重要事項に注意してください。

- CSS スwitチは、透過プロキシキャッシングのほか、リバースプロキシキャッシングもサポートします。CSS スwitチは、複数の Content Engine 上にデータを配分する方法 (たとえば、URL 全体、URL ストリング、ドメイン名全体、またはドメイン ストリング) に応じて、複数の負荷分散方式を備えています。また CSS スwitチは、既知のキャッシュ可能オブジェクトのリストも作成します。このリストは変更されることがありますが、変更作業の大部分は、Content Engine のキャッシング機能によって軽減されます。
- ユーザは CSS スwitチを設定して、スwitチがコンテンツを動的に分析し、そのコンテンツがキャッシング可能かどうかを判別します。コンテンツがキャッシング可能である場合、CSS スwitチはそのコンテンツをキャッシュ サービスに送信します。キャッシングできない場合、CSS スwitチは直接、オリジン Web サーバにそのコンテンツを送信します。
- キャッシュ サービスで透過キャッシングが使用できない場合、CSS スwitチは、クライアント要求をオリジン Web サーバに送信します。

CSS スwitチを経由した透過キャッシングを設定するには、次の作業が必要です。

1. CSS スwitチ上で透過キャッシングを有効にします。
2. スタンドアロン Content Engine 上で、CSS スwitチから転送されたトラフィックを受け入れ可能にします。
3. スタンドアロン Content Engine 上で透過キャッシングを有効にします。

次のワークフローのサンプルでは、CLI コマンドを使用して、CSS スwitチとスタンドアロン Content Engine を使用する透過キャッシングを設定する方法を示しています。この例では、serv1 が CS150 という名前の CSS スwitチおよび CE100 という名前のスタンドアロン Content Engine を使用する透過キャッシング サービスとして設定されています。CSS スwitチを使用したキャッシングを設定する前に、インターフェイス、サービス、所有者、VLAN、およびコンテンツ ルールが設定済であることを確認してください。



(注) CSS スwitチ上でこれらの属性を設定する方法の詳細は、『Content Services Switch Basic Configuration Guide』を参照してください。各コマンドの詳細については、『Content Services Switch Command Reference』を参照してください。

### レイヤ 4 スwitチングを使用した透過キャッシングの設定例

次の例では、レイヤ 4 CSS スwitチ (WCCP 対応ルータとは対照的) とスタンドアロン Content Engine を使用する、透過キャッシングを有効にする方法を示しています。

**ステップ 1** CSS スwitチ上で、透過キャッシング用に予約されているサービス serv1 を追加します。

```
CS150(config)# add service serv1
CS150(config-service[serv1])#
```

**ステップ 2** serv1 のサービス タイプとして透過キャッシングを指定します。

```
CS150(config-service[serv1])# type transparent cache
```

## ■ リダイレクション方式としてのレイヤ4スイッチングの設定

- ステップ 3** CSS スイッチがキャッシングを行うコンテンツのタイプを指定する、EQL (Extension Qualifier List) を作成します。

```
CS150(config)# eql graphics
CS150(config-eql[graphics])#
```

- ステップ 4** 引用符で囲んだ最長 64 文字以内のテキストで、EQL の説明を入力します。

```
CS150(config-eql[graphics])# description "This EQL specifies cacheable graphic files"
```

- ステップ 5** CSS スイッチにキャッシングするコンテンツの拡張子を指定します。1～8 文字のテキスト文字列を入力します。

```
CS150(config-eql[graphics])# extension jpeg
```

拡張子のタイプについてもここで記述できます。引用符で囲まれたテキスト文字列を入力します。最大長は 64 文字です。

```
CS150(config-eql[graphics])# extension jpeg "This is a graphics file"
CS150(config-eql[graphics])# exit
CS150(config)#
```

- ステップ 6** コンテンツ ルールに EQL を指定して、すべてのコンテンツ要求が所定の拡張子と一致するようにします。

```
CS150(config-owner-content[cisco.com-rule1])# url "/*" eql graphics
```

- ステップ 7** キャッシュ コンテンツ ルールに対して負荷分散方式を設定します。デフォルトは、ラウンドロビンです。

```
CS150(config-owner-content[cisco.com-rule1])# balance domain
```

- ステップ 8** フェールオーバー タイプ (**bypass**、**linear**、**next**) を指定して、サービスに障害が起きた場合、CSS スイッチがコンテンツ要求を処理する方式を指定します。デフォルトはリニアです。

```
CS150(config-owner-content[cisco.com-rule1])# failover bypass
```

- ステップ 9** EQL 設定を表示します。

```
CS150(config-owner-content[cisco.com-rule1])# show eql
```

- ステップ 10** キャッシュ設定を示すコンテンツ ルールを表示します。

```
CS150(config-owner-content[cisco.com-rule1])# show rule
```

- ステップ 11** CSS スイッチで設定モードを終了します。

```
CS150(config-owner-content[cisco.com-rule1])# end
```



**ステップ 12** 設定を保存します。これで、透過キャッシング サービス用に CSS スイッチが設定されます。

```
CS150(config-owner-content[cisco.com-rule1])# copy running-config startup-config
```

**ステップ 13** スタンドアロン Content Engine を設定して、CSS スイッチなどのレイヤ 4 対応スイッチから転送されたレイヤ 4 トラフィックを透過的に受信します。

```
CE100(config)# http 14-switch enable
```

**ステップ 14** スタンドアロン Content Engine 上で設定モードを終了します。

```
CE100(config)# exit
```

**ステップ 15** 実行設定を不揮発性メモリに書き込みます。

```
CE100# write memory
```

---

■ リダイレクション方式としてのレイヤ 4 スwitチングの設定