WCCP のリバース透過キャッシングのトラブルシューティング

内容

概要

このドキュメントでは、Web Cache Communication Protocol（WCCP）を使用してリバース透過キャッシングを実装するときに WCCP をトラブルシューティングする方法について説明します。

前提条件

要件

このドキュメントに特有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

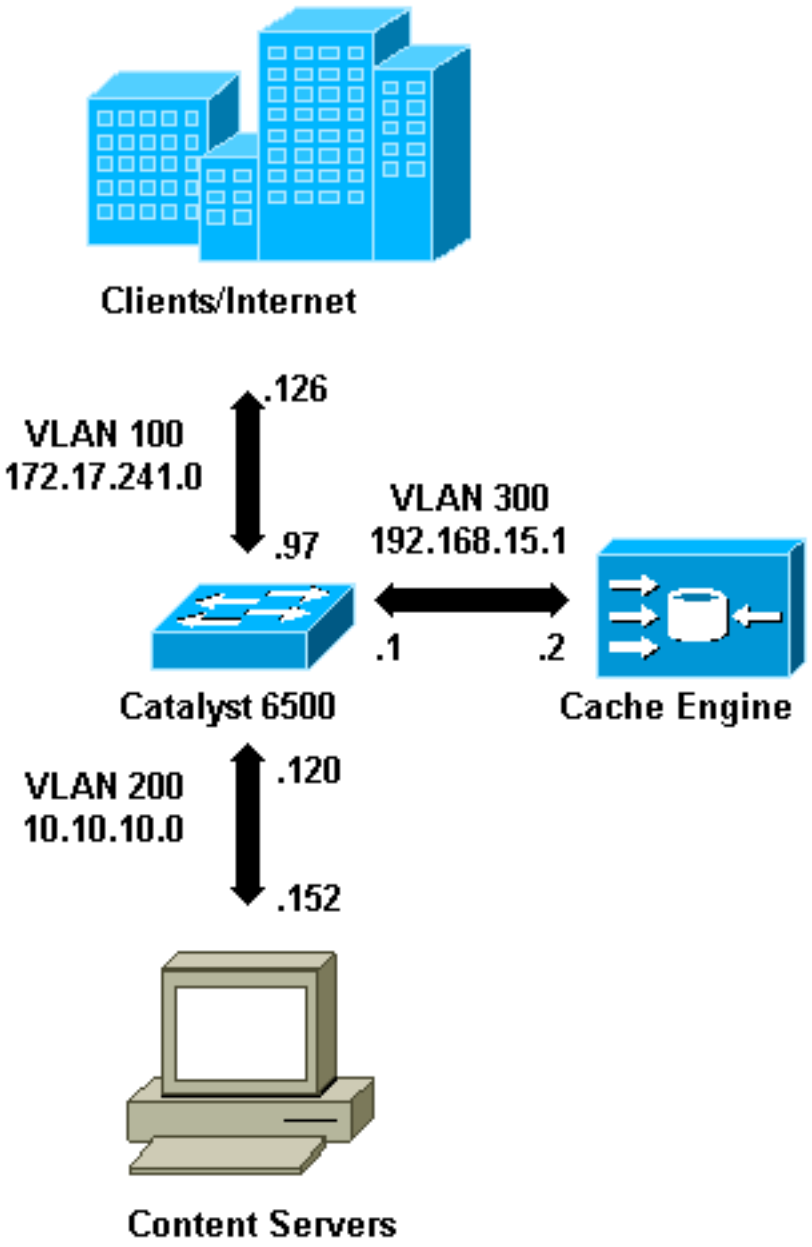
- Supervisor 1およびMSFC 1がネイティブモードで設定されたCatalyst 6500
- Cisco IOS®ソフトウェアリリース12.1(8a)EX(c6sup11-jsv-mz.121-8a.EX.bin)
- バージョン2.51のCache Engine 550

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

コンフィギュレーション



Cache Engineをインストールする場合は、WCCPの実装に必要なコマンドだけを設定することを推奨します。ルータやクライアントのリダイレクトリストに認証などの他の機能を後で追加できます。

キャッシュエンジンで、ルータのIPアドレスと使用するWCCPのバージョンを指定する必要があります。

```
wccp router-list 1 192.168.15.1
   wccp reverse-proxy router-list-num 1
   wccp version 2
```

WCCPのIPアドレスとバージョンを設定すると、リバース透過キャッシングを実装するためにルータでサービス99をアクティブにする必要があることを警告するメッセージが表示されることが

あります。サービス99は、リバース透過キャッシングのWCCPサービスIDです。通常の透過キャッシングの識別子は、Cisco IOSの「web-cache」という語です。ルータでサービス99 (リバース透過キャッシング) をアクティブにし、リダイレクションを実行するポートを指定するには、グローバルコンフィギュレーションモードで次のコマンドを追加します。

```
ip wccp 99
interface Vlan200
    ip address 10.10.10.120 255.255.255.0
    ip wccp 99 redirect out
```

Reverse Transparent Cachingを設定すると、WCCPサービス99を実行するルータがWebサーバに向けられた要求を代行受信します。ip wccp 99 redirect outコマンドは、Webサーバへのパス内のクライアントHTTPパケットをインターセプトするインターフェイスに適用されます。通常、これはWebサーバVLANです。これは通常、キャッシュエンジンがインストールされているVLANではありません。

WCCPがアクティブになると、ルータはWCCPリダイレクトが設定されているすべてのポートでリッスンします。Cache Engineは、WCCP Here I amパケットをルータリストに設定されているIPアドレスに送信して、その存在を示します。

ルータとキャッシュ間のWCCP接続が形成されます。接続情報を表示するには、show ip wccpコマンドを発行します。

ルータIDは、キャッシュエンジンで認識されるルータのIPアドレスです。この識別子は、リダイレクトされたトラフィックがキャッシュに到達するために使用するルータインターフェイスとは限りません。この例のルータIDは192.168.15.1です。

```
Router#show ip wccp
   Global WCCP information:
       Router information:
           Router Identifier:                  192.168.15.1
           Protocol Version:                   2.0
    Service Identifier: 99
           Number of Cache Engines:            1
           Number of routers:                  1
           Total Packets Redirected:           0
           Redirect access-list:               -none-
           Total Packets Denied Redirect:      0
           Total Packets Unassigned:           0
           Group access-list:                  -none-
           Total Messages Denied to Group:     0
           Total Authentication failures:      0
```

show ip wccp 99 detailコマンドは、キャッシュに関する詳細情報を提供します。

```
Router#show ip wccp 99 detail
   WCCP Cache-Engine information:
           IP Address:               192.168.15.2
           Protocol Version:         2.0
           State:                    Usable
           Redirection:              GRE
```

```
        Initial Hash Info:        FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
                                  FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
        Assigned Hash Info:       FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
                                  FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
        Hash Allotment:           256 (100.00%)
        Packets Redirected:       0
        Connect Time:             00:00:39
```

Redirectionフィールドは、ルータからキャッシュエンジンにパケットをリダイレクトするために使用する方法を表します。この方法は、総称ルーティングカプセル化(GRE)またはレイヤ2のいずれかです。GREでは、パケットはGREパケットにカプセル化されます。レイヤ2では、パケットはキャッシュに直接送信されますが、レイヤ2リダイレクションでは、キャッシュエンジンとスイッチまたはルータがレイヤ2隣接関係である必要があります。

ハッシュ割り当て[情報(Initial Hash Info)][報(Assigned Hash Info)]フィールドで16進数で表されます。これは、このキャッシュに割り当てられているハッシュバケットの数です。すべての可能な送信元インターネットアドレスは、64の等しいサイズの範囲（範囲ごとに1つのバケット）に分割され、各キャッシュには、これらのバケットの送信元アドレス範囲の数からトラフィックが割り当てられます。この量は、キャッシュの負荷と負荷の重み付けに応じてWCCPによって動的に管理されます。キャッシュが1つだけインストールされている場合、このキャッシュはすべてのバケットに割り当てられます。

ルータがキャッシュエンジンへのパケットのリダイレクトを開始すると、[リダイレクトされたパケットの合計]が増加します。

Total Packets Unassignedフィールドは、どのキャッシュにも割り当てられていなかったためリダイレクトされなかったパケットの数です。この例では、パケットの数は5です。キャッシュの初期検出時またはキャッシュが削除された場合に、パケットが割り当てられていない場合があります。

```
Router#show ip wccp
   Global WCCP information:
       Router information:
           Router Identifier:                    192.168.15.1
           Protocol Version:                     2.0
    Service Identifier: 99
           Number of Cache Engines:              1
           Number of routers:                    1
           Total Packets Redirected:             28
           Redirect access-list:                 -none-
           Total Packets Denied Redirect:        0
           Total Packets Unassigned:             5
           Group access-list:                    -none-
           Total Messages Denied to Group:       0
           Total Authentication failures:        0
```

キャッシュがルータによって取得されない場合は、WCCPアクティビティをデバッグすると便利です。ルータがキャッシュから**Here I am**パケットを受け取ると、「**I see you**」パケットで応答して、デバッグで報告されます。使用できるデバッグ コマンドは **debug ip wccp events** および **debug ip wccp packets** です。

注：debug コマンドを使用する前に、『**debug コマンドの重要な情報**』を参照してください。

次の出力は、通常のWCCPデバッグメッセージの例を示しています。

```
Router#debug ip wccp event
   WCCP events debugging is on
  Router#debug ip wccp packet
   WCCP packet info debugging is on
   Router#
   2d18h: WCCP-EVNT:S00: Built new router view: 0 routers,
          0 usable web caches, change # 00000001
   2d18h: WCCP-PKT:S00: Sending I_See_You packet to
          192.168.15.2 w/ rcv_id 00000001
   2d18h: WCCP-EVNT:S00: Redirect_Assignment packet from
          192.168.15.2 fails source check
   2d18h: %WCCP-5-SERVICEFOUND: Service web-cache
          acquired on Web Cache 192.168.15.2
   2d18h: WCCP-PKT:S00: Received valid Here_I_Am packet
          from 192.168.15.2 w/rcv_id 00000001
   2d18h: WCCP-EVNT:S00: Built new router view: 1
          routers, 1 usable web caches, change # 00000002
   2d18h: WCCP-PKT:S00: Sending I_See_You packet to 192.168.15.2
          w/ rcv_id 00000002
   2d18h: WCCP-EVNT:S00: Built new router view: 1 routers,
          1 usable web caches, change # 00000002
   2d18h: WCCP-PKT:S00: Received valid Redirect_Assignment
          packet from 192.168.15.2 w/rcv_id 00000002
   2d18h: WCCP-PKT:S00: Sending I_See_You packet to 192.168.15.2
          w/ rcv_id 00000003
   2d18h: WCCP-EVNT:S00: Built new router view: 1 routers,
          1 usable web caches, change # 00000002
   2d18h: WCCP-PKT:S00: Received valid Redirect_Assignment
          packet from 192.168.15.2 w/rcv_id 00000003
   2d18h: WCCP-PKT:S00: Sending I_See_You packet to 192.168.15.2
          w/ rcv_id 00000004
   2d18h: WCCP-PKT:S00: Sending I_See_You packet to 192.168.15.2
          w/ rcv_id 00000005
   2d18h: WCCP-PKT:S00: Sending I_See_You packet to 192.168.15.2
          w/ rcv_id 00000006
   2d18h: WCCP-EVNT:S00: Built new router view: 1 routers,
          1 usable web caches, change # 00000002
   2d18h: WCCP-PKT:S00: Received valid Redirect_Assignment
          packet from 192.168.15.2 w/rcv_id 00000006
```

デバッグレベルを上げるには、IPパケットトラフィックをトレースして、ルータがキャッシュエンジンからパケットを受信しているかどうかを確認します。実稼働環境でルータの過負荷を回避し、対象トラフィックのみを表示するために、ACLを使用して、デバッグを送信元としてキャッシュのIPアドレスを持つパケットだけに制限できます。ACLの例は、**access-list 130 permit ip host 192.168.15.2 host 192.168.15.1**です。

```
Router#debug ip wccp event
   WCCP events debugging is on
  Router#debug ip wccp packet
   WCCP packet info debugging is on
  Router#debug ip packet 130
   IP packet debugging is on for access list 130
   2d19h: WCCP-EVNT:S00: Built new router view: 1 routers,  1 usable web caches,
          change # 00000002
   2d19h: WCCP-PKT:S00: Received valid Redirect_Assignment  packet from 192.168.15.2
          w/rcv_id 0000001B
   2d19h: datagramsize=174, IP 18390: s=192.168.15.2  (Vlan300), d=192.168.15.1
          (Vlan300), totlen 160, fragment 0, fo 0, rcvd 3
   2d19h: WCCP-PKT:S00: Sending I_See_You packet to 192.168.15.2  w/ rcv_id 0000001C
```

```
2d19h: datagramsize=174, IP 18392: s=192.168.15.2  (Vlan300), d=192.168.15.1
       (Vlan300), totlen 160, fragment 0, fo 0, rcvd 3
2d19h: WCCP-PKT:S00: Sending I_See_You packet to 192.168.15.2  w/ rcv_id 0000001D
2d19h: datagramsize=174, IP 18394: s=192.168.15.2  (Vlan300), d=192.168.15.1
       (Vlan300), totlen 160, fragment 0, fo 0, rcvd 3
2d19h: WCCP-PKT:S00: Sending I_See_You packet to 192.168.15.2  w/ rcv_id 0000001E
2d19h: datagramsize=378, IP 18398: s=192.168.15.2  (Vlan300), d=192.168.15.1
       (Vlan300), totlen 364, fragment 0, fo 0, rcvd 3
2d19h: WCCP-EVNT:S00: Built new router view: 1 routers,  1 usable web caches,
       change # 00000002
2d19h: WCCP-PKT:S00: Received valid Redirect_Assignment  packet from 192.168.15.2
       w/rcv_id 0000001E
2d19h: datagramsize=174, IP 18402: s=192.168.15.2  (Vlan300), d=192.168.15.1
       (Vlan300), totlen 160, fragment 0, fo 0, rcvd 3
2d19h: WCCP-PKT:S00: Sending I_See_You packet to 192.168.15.2  w/ rcv_id 0000001F
2d19h: datagramsize=174, IP 18404: s=192.168.15.2  (Vlan300), d=192.168.15.1
       (Vlan300), totlen 160, fragment 0, fo 0, rcvd 3
2d19h: WCCP-PKT:S00: Sending I_See_You packet to 192.168.15.2  w/ rcv_id 00000020
2d19h: datagramsize=174, IP 18406: s=192.168.15.2  (Vlan300), d=192.168.15.1
       (Vlan300), totlen 160, fragment 0, fo 0, rcvd 3
2d19h: WCCP-PKT:S00: Sending I_See_You packet to 192.168.15.2  w/ rcv_id 00000021
2d19h: datagramsize=378, IP 18410: s=192.168.15.2  (Vlan300), d=192.168.15.1
       (Vlan300), totlen 364, fragment 0, fo 0, rcvd 3
2d19h: WCCP-EVNT:S00: Built new router view: 1 routers,  1 usable web caches,
       change # 00000002
2d19h: WCCP-PKT:S00: Received valid Redirect_Assignment  packet from 192.168.15.2
       w/rcv_id 00000021
2d19h: datagramsize=174, IP 18414: s=192.168.15.2  (Vlan300), d=192.168.15.1
       (Vlan300), totlen 160, fragment 0, fo 0, rcvd 3
2d19h: WCCP-PKT:S00: Sending I_See_You packet to 192.168.15.2  w/ rcv_id 00000022
2d19h: datagramsize=174, IP 18416: s=192.168.15.2  (Vlan300), d=192.168.15.1
       (Vlan300), totlen 160, fragment 0, fo 0, rcvd 3
```

ルータによってキャッシュが見えず、WCCPアクティビティが見られない場合は、基本的な接続を確認します。ルータからキャッシュへ、またはキャッシュからルータへ、ping を送信してみてください。pingが成功すると、設定に**エラー**が存在する可能性があります。

キャッシュが取得されてもパケットがリダイレクトされない場合は、ルータがトラフィックを受信し、**ip wccp 99 redirect outコマンドが適用されるインターフェイスにトラフィックが転送されることを確認**します。インターセプトされてリダイレクトされるトラフィックは、TCPポート80宛てのトラフィックだけであることに注意してください。

トラフィックがまだリダイレクトされておらず、Webコンテンツがサーバから直接送信されている場合は、キャッシュが代行受信の命令を正しく渡していることを確認します。この操作を完了するには、WCCPの背景情報が必要です。

WCCPは、次の2種類のサービスを認識します。*標準および動的な機能*。ルータは、標準サービスを暗黙的に認識しています。つまり、ポート80を使用するようにルータに指示する必要はありません。これは、ルータがすでにポート80を使用することを認識しているためです。通常の透過キャッシュ(Web-cache - standard service 0)は標準サービスです。

その他のケース (透過キャッシングを含む) では、ルータにインターセプトするポートが指示されます。この情報はHere I amパケット**に渡されます**。

debug ip packet dumpコマンドを発行すると、パケット自体を調べることができます。作成したACLを使用して、キャッシュエンジンから送信されたパケットのみをデバッグします。

```
Router#debug ip packet 130 dump
   2d19h: datagramsize=174, IP 19576: s=192.168.15.2 (Vlan300), d=192.168.15.1
      (Vlan300), totlen 160, fragment 0, fo 0,
   rcvd 3
   072C5120:                         0004 9B294800            ...)H.
!--- Start IP header. 072C5130: 00500F0D 25360800 450000A0 4C780000 .P..%6..E.. Lx.. 072C5140:
3F118F81 C0A80F02 C0A80F01 08000800 ?...@(..@(..... 072C5150: 008CF09E 0000000A 0200007C
00000004  ..p........|....
!--- Start WCCP header. 072C5160: 00000000 00010018 0163E606 00000515 .........cf..... 072C5170:
00500000 00000000 00000000 00000000  .P..............
!--- Port to intercept (0x50=80). 072C5180: 0003002C C0A80F02 00000000 FFFFFFFF
...,@(..........
!--- Hash allotment (FFFF...). 072C5190: FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF  ................
   072C51A0: FFFFFFFF FFFFFFFF FFFF0000 00000000  ................
   072C51B0: 00050018 00000002 00000001 C0A80F01  ............@(..
   072C51C0: 0000000C 00000001 C0A80F02 00080008  ........@(......
   072C51D0: 00010004 00000001 30                 ........0
```

このコマンドを使用すると、Request For Comments(RFC)全体を表示しなくても、ポートがアドバタイズされているかどうかを確認できます。 ポートがアドバタイズされていない場合は、おそらくキャッシュの設定に問題があります。

詳細はWeb Cache Coordination Protocol V2.0を参照 。

キャッシュが取得され、パケットがリダイレクトされても、インターネットクライアントがサーバーを参照できない場合は、キャッシュがインターネットとサーバーに接続できるかどうかを確認してください。キャッシュから、インターネット上のさまざまなIPアドレスと内部サーバの一部にpingを実行します。IPアドレスではなく完全修飾ドメイン(URL)にpingを実行する場合は、キャッシュ設定で使用するDNSサーバを指定してください。

キャッシュが要求を処理しているかどうかがわからない場合は、キャッシュ内のHTTPアクティビティをデバッグできます。キャッシュ内のHTTPアクティビティをデバッグするには、キャッシュの過負荷を回避するようにトラフィックを制限する必要があります。ルータで、インターネット上の1つのクライアントの送信元IPアドレスを使用してACLを作成し、テスト用のデバイスとして使用し、グローバルコマンド**ip wccp 99のオプションredirect-listを使用します**。

```
Router(config)#access-list 50 permit 172.17.241.126
Router(config)#ip wccp 99 redirect-list 50
```

ACLを作成して適用したら、次の手順を実行します。

1. コマンド**debug http all all**（Cisco Cache Engineバージョン2.x）または**debug http all**（Cisco Cache Engineバージョン3およびACNSバージョン4、5）を使用して、キャッシュ内のHTTPデバッグをアクティブにします。
2. ターミナル監視をアクティブにします(**term monコマンドを**発行します)。
3. ACLで設定したクライアントから、いずれかのサーバを参照してみます。

次に出力例を示します。

```
irq0#conf tcework_readfirstdata() Start the recv: 0xb820800 len 4096 timeout
   0x3a98 ms ctx 0xb87d800
   cework_recvurl() Start the request: 0xb20c800 0xb20c838 0xb20c8e0
   Http Request headers received from client:
   GET / HTTP/1.1
```

```
   Host: 10.10.10.152
   User-Agent: Links (0.92; Linux 2.2.16-22 i686)
   Accept: */*
   Accept-Charset: us-ascii, ISO-8859-1, ISO-8859-2, ISO-8859-4, ISO-8895-5,
      ISO-8859-13, windows-1250, windws-1251, windows-1257, cp437, cp850, cp852,
       cp866, x-cp866-u, x-mac-ce, x-kam-cs, x-koi8-r, x-koi8-u, utf8
   Connection: Keep-Alive

Protocol dispatch: mode=1 proto=2
   ValidateCode() Begin: pRequest=0xb20c800
   Proxy: CACHE_MISS: HealProcessUserRequest
   cework_teefile() 0xb20c800: Try to connect to server: CheckProxyServerOut():
      Outgoing proxy is not enable: 0xb20c800 (F)
   GetServerSocket(): Forwarding to server: pHost = 10.10.10.152, Port = 80
   HttpServerConnectCallBack : Connect call back socket = 267982944, error    = 0
   Http request headers sent to server:

   GET / HTTP/1.1
   Host: 10.10.10.152
   User-Agent: Links (0.92; Linux 2.2.16-22 i686)
   Accept: */*
   Accept-Charset: us-ascii, ISO-8859-1, ISO-8859-2, ISO-8859-4, ISO-8895-5,
      ISO-8859-13, windows-1250, windws-1251, windows-1257, cp437, cp850, cp852,
      cp866, x-cp866-u, x-mac-ce, x-kam-cs, x-koi8-r, x-koi8-u, utf8
   Connection: keep-alive
   Via: 1.1 irq0
   X-Forwarded-For: 172.17.241.126

cework_sendrequest: lBytesRemote = 386, nLength = 386 (0xb20c800)
   ReadResCharRecvCallback():  lBytesRemote = 1818, nLength = 1432 0xb20c800)
   IsResponseCacheable() OBJECTSIZE_IS_UNLIMITED, lContentLength = 3194
   cework_processresponse() : 0xb20c800 is cacheable
   Http response headers received from server:
   HTTP/1.1 200 OK
   Date: Tue, 20 Nov 2001 10:46:14 GMT
   Server: Apache/1.3.12 (Unix)  (Red Hat/Linux) mod_ssl/2.6.6 OpenSSL/0.9.5a
      mod_perl/1.24
   Last-Modified: Fri, 12 Oct 2001 12:55:23 GMT
   ETag: "5e23-c7a-3bc6e83b"
   Accept-Ranges: bytes
   Content-Length: 3194
   Keep-Alive: timeout=15, max=100
   Connection: Keep-Alive
   Content-Type: text/html

GetUpdateCode(): GET request from client, GET request to server.
   GetUpdateCode(): nRequestType = -1
   SetTChain() 0xb20c800: CACHE_OBJECT_CLIENT_OBJECT sendobj_and_cache
   Http response headers sent to client:
   HTTP/1.1 200 OK
   Date: Tue, 20 Nov 2001 10:46:14 GMT
   Server: Apache/1.3.12 (Unix)  (Red Hat/Linux) mod_ssl/2.6.6 OpenSSL/0.9.5a
      mod_perl/1.24
   Last-Modified: Fri, 12 Oct 2001 12:55:23 GMT
   ETag: "5e23-c7a-3bc6e83b"
   Content-Length: 3194
   Keep-Alive: timeout=15, max=100
   Content-Type: text/html
   Connection: keep-alive

cework_tee_sendheaders() 0xb20c800: sent 323 bytes to client
   cework_tee_send_zbuf() 0xb20c800: Send 1087 bytes to client (1087)
   UseContentLength(): Valid Content-Length (T)
   cework_tee_recv_zbuf() 0xb20c800: Register to recv 2107 bytes timeout 120 sec
```

```
   HttpServerRecvCallBack(): Recv Call Back socket 267982944, err 0, length  2107
   HttpServerRecvCallBack(): lBytesRemote = 3925, nLength = 2107 (186697728)
   cework_tee_send_zbuf() 0xb20c800: Send 2107 bytes to client (2107)
   UseContentLength(): Valid Content-Length (T)
   cework_setstats(): lBytesLocal = 0, lBytesRemote = 3925 (0xb20c800)
   cework_readfirstdata() Start the recv: 0xb84a080 len 4096 timeout 0x3a98
      ms ctx 0xb87d800
   cework_cleanup_final() End the request: 0xb20c800 0xb20c838 0xb20c8e0
```

デバッグで見つかった関連情報は、太字で強調表示されます。

Webページトランザクションの異なるフェーズは次のとおりです。

1. クライアントから受信したHTTP要求ヘッダー。
2. HTTP要求ヘッダーがサーバーに送信されました。
3. HTTP応答ヘッダーをサーバーから受信しました。
4. クライアントに送信されるHTTP応答ヘッダー。

参照するWebページに複数のオブジェクトが含まれている場合、この一連のイベントの複数のインスタンスが存在します。最も簡単な要求を使用して、デバッグ出力を減らします。

Catalyst 6500またはCisco 7600ルータでは、Feature ManagerがCisco IOSで設定されたすべての機能を処理して、トラブルシューティングの追加レイヤを提供します。これらのデバイスでレイヤ3機能を設定すると、受信したフレームの処理方法を定義する情報が、スイッチまたはルータのレイヤ2制御機能（機能マネージャ）に渡されます。 WCCPの場合、この制御情報は、IOSおよびWCCPによって代行受信され、トランスペアレントキャッシュに転送されるパケットを定義します。

show fm featuresコマンドは、Cisco IOSで有効になっている機能を表示します。このコマンドを使用すると、インターセプトするポートがキャッシュエンジンによって正しくアドバタイズされているかどうかを確認できます。

```
Router#show fm features
   Redundancy Status: stand-alone
   Interface: Vlan200 IP is enabled
     hw[EGRESS] = 1, hw[INGRESS] = 1
     hw_force_default[EGRESS] = 0, hw_force_default[INGRESS] = 0
     mcast = 0
     priority = 2
     reflexive = 0
     vacc_map :
     outbound label: 5
           merge_err: 0
           protocol: ip
             feature #: 1
             feature id: FM_IP_WCCP
             Service ID: 99
             Service Type: 1

The following are the used labels
     label 5:
           swidb: Vlan200
           Vlous:

The following are the features configured
     IP WCCP: service_id = 99, service_type = 1, state = ACTIVE
           outbound users:
```

```
            user_idb: Vlan200
          WC list:
            address: 192.168.15.2
          Service    ports:
            ports[0]:    80

The following is the ip ACLs port expansion information
     FM_EXP knob configured: yes

FM mode for WCCP: GRE (flowmask: destination-only)

FM redirect index base: 0x7E00

The following are internal statistics
     Number of pending tcam inserts: 0
     Number of merge queue elements: 0
```

コマンド**show fm int vlan 200**は、Ternary Content Addressable Memory(TCAM)の正確な内容を表示します。

```
Router#show fm int vlan 200
 Interface: Vlan200 IP is enabled
  hw[EGRESS] = 1, hw[INGRESS] = 1
  hw_force_default[EGRESS] = 0, hw_force_default[INGRESS] = 0
  mcast = 0
  priority = 2
  reflexive = 0
  vacc_map :
  outbound label: 5
   merge_err: 0
   protocol: ip
    feature #: 1
    feature id: FM_IP_WCCP
    Service ID: 99
    Service Type: 1
     (only for IP_PROT) DestAddr SrcAddr           Dpt   Spt  L4OP TOS Est  prot  Rslt
     vmr IP value #1:   0.0.0.0  192.168.15.2     0     0    0    0   0    6     permit
     vmr IP mask  #1:   0.0.0.0  255.255.255.255  0     0    0    0   0    FF
     vmr IP value #2:   0.0.0.0  0.0.0.0          80    0    0    0   0    6     bridge
     vmr IP mask  #2:   0.0.0.0  0.0.0.0          FFFF  0    0    0   0    FF
     vmr IP value #3:   0.0.0.0  0.0.0.0          0     0    0    0   0    0     permit
     vmr IP mask  #3:   0.0.0.0  0.0.0.0          0     0    0    0   0    0
```

`vmr IP# 1:`lineは、キャッシュエンジンから送信されるフレームのインターセプションバイパスを定義します。これを行わないと、リダイレクションループが発生します。`vmr IP# 2:`lineは、宛先としてポート80を持つすべてのパケットの代行受信を定義します。2行目にポート80が表示されていないが、WCCPがアクティブで、キャッシュがルータで使用可能な場合、キャッシュ設定に問題がある可能性があります。ポートがキャッシュによって送信さ**れているかどうかを判断**するために、「Here I am packet」のダンプを収集します。

トラブルシューティング後に問題を解決できない場合は、Cisco [Technical Assistance Center(TAC)に問題を報告してください](#)。

Cisco TACに提供する必要がある基本情報を次に示します。ルータから、次の情報を収集します。

- **show tech**コマンドの出力。**show running-config**コマンドと**show version output**コマンドの出

力は、show tech出力のサイズに問題がある場合に置き換えることができます。
- show ip wccpコマンドの出力。
- show ip wccp web-cache detailコマンドの出力。
- ルータとWebキャッシュの間の通信に問題がある場合は、問題が発生している間にdebug ip wccp eventsコマンドとdebug ip wccp packetsコマンドの出力を提供します。

キャッシュエンジン（Cisco Cache Engineのみ）で、show techコマンドの出力を収集します。

TACに連絡する際は、次の手順を実行します。

1. 問題の明確な説明を入力します。次の質問に対する回答を含める必要があります。どのような現象ですか。常に発生するか、まれに発生するか。設定を変更した後に問題が発生しましたか。シスコまたはサードパーティのキャッシュは使用されますか。
2. トポロジの明確な説明を入力します。より明確になる場合は、図を含めます。
3. 問題の解決に役立つと思われる他の情報を提供します。

設定例の出力を次に示します。

```
********************************** Router Configuration ****************************
Router#show running
   Building configuration...
Current configuration : 4231 bytes
   !
   version 12.1
   service timestamps debug uptime
   service timestamps log uptime
   no service password-encryption
   !
   hostname Router
   !
   boot buffersize 126968
   boot bootldr bootflash:c6msfc-boot-mz.120-7.XE1
   !
   redundancy
    main-cpu
     auto-sync standard
   ip subnet-zero
   ip wccp 99
   !
   !
   !
   interface FastEthernet3/1
    no ip address
    switchport
    switchport access vlan 100
    switchport mode access
   !
   interface FastEthernet3/2
    no ip address
    switchport
    switchport access vlan 200
    switchport mode access
   !
   interface FastEthernet3/3
    no ip address
    switchport
    switchport access vlan 300
    switchport mode access
```

```
   !
   interface FastEthernet3/4
    no ip address
   !
!
   interface Vlan100
    ip address 172.17.241.97 255.255.255.0
   !
   interface Vlan200
    ip address 10.10.10.120 255.255.255.0
    ip wccp 99 redirect out
   !
   interface Vlan300
    ip address 192.168.15.1 255.255.255.0
   !
   ip classless
   ip route 0.0.0.0 0.0.0.0 172.17.241.1
   no ip http server
   !
   access-list 30 permit 192.168.15.2
   !
   !
   line con 0
    exec-timeout 0 0
   line vty 0 4
    login
    transport input lat pad mop telnet rlogin udptn    nasi
   !
   end
********************************** Cache Configuration ******************************
Cache#show running
Building configuration...
   Current configuration:
   !
   !
   logging disk /local/syslog.txt debug
   !
   user add admin uid 0  capability admin-access
   !
   !
   !
   hostname Cache
   !
   interface ethernet 0
    ip address 192.168.15.2 255.255.255.0
    ip broadcast-address 192.168.15.255
    exit
   !
   interface ethernet 1
    exit
   !
   ip default-gateway 192.168.15.1
   ip name-server 172.17.247.195
   ip domain-name cisco.com
   ip route 0.0.0.0 0.0.0.0 192.168.15.1
   cron file /local/etc/crontab
   !
   wccp router-list 1 192.168.15.1
   wccp reverse-proxy router-list-num 1
   wccp version 2
   !
   authentication login local enable
   authentication configuration local enable
   rule no-cache url-regex .*cgi-bin.*
```

```
rule no-cache url-regex .*aw-cgi.*
!
!
end
```

関連情報

- Cisco キャッシュ ソフトウェア
- Cisco 500 シリーズ キャッシュ エンジン
- Web Cache Communications Protocol (WCCP; Web キャッシュ通信プロトコル)
- Cisco Cache Engine 2.0ソフトウェアダウンロードページ(登録ユーザ専用)
- Cisco Cache Engine 3.0ソフトウェアダウンロードページ(登録ユーザ専用)
- テクニカル サポートとドキュメント – Cisco Systems