

# WCCP反向透明快取故障排除

## 目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[慣例](#)

[組態](#)

[相關資訊](#)

## 簡介

本檔案將說明Web快取通訊協定(WCCP)用於實作反向透明快取時，如何進行疑難排解。

## [必要條件](#)

### [需求](#)

本文件沒有特定需求。

### [採用元件](#)

本文中的資訊係根據以下軟體和硬體版本：

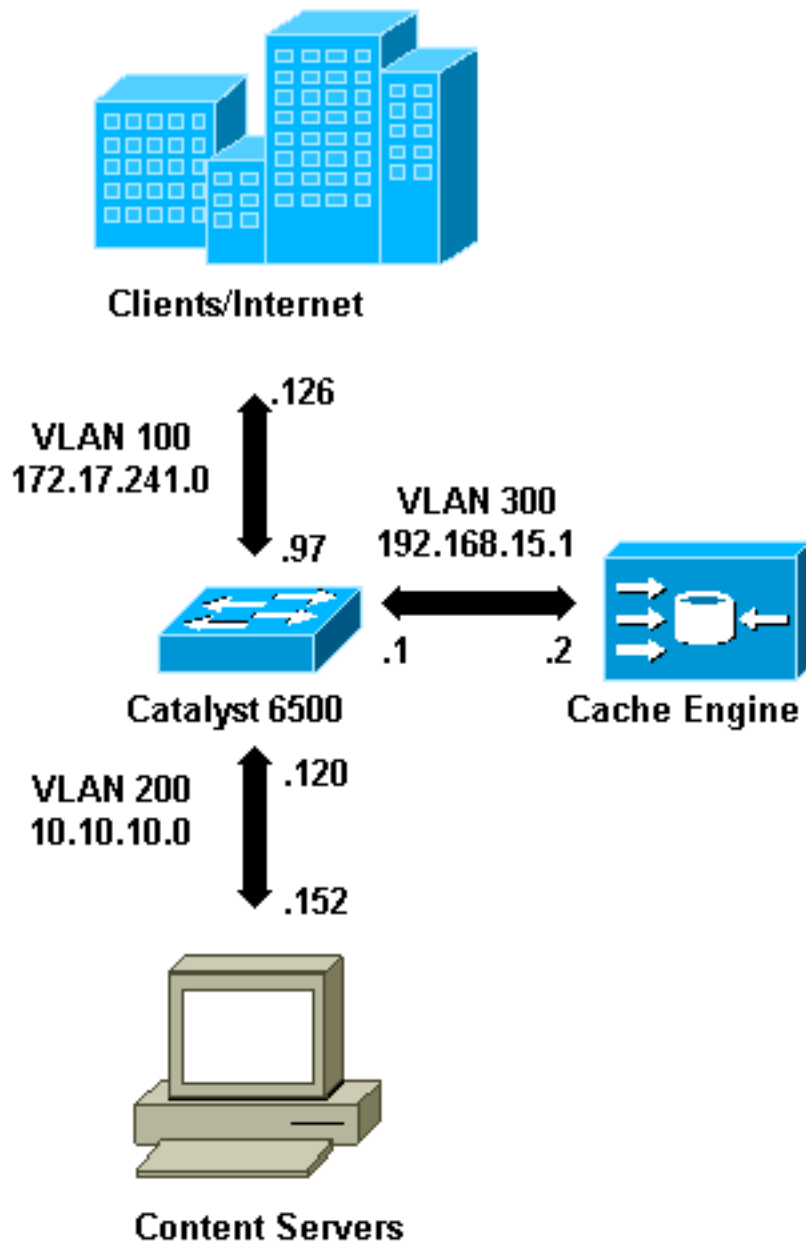
- 在原生模式下設定Supervisor 1和MSFC 1的Catalyst 6500
- Cisco IOS®軟體版本12.1(8a)EX(c6sup11-jsv-mz.121-8a.EX.bin)
- 快取引擎550 ( 版本2.51 )

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除 ( 預設 ) 的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

### [慣例](#)

如需檔案慣例的相關資訊，請參閱[思科技術提示慣例](#)。

## [組態](#)



安裝快取引擎時，思科建議您僅配置實施WCCP所需的命令。您可以稍後再新增其他功能，例如對路由器和使用者端重新導向清單進行驗證。

在快取引擎上，必須指定路由器的IP地址和要使用的WCCP版本。

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

配置IP地址和版本的WCCP後，您可能會看到一條消息，警告應在路由器中啟用服務99，以便實施反向透明快取。服務99是用於反向透明快取的WCCP服務識別符號。普通透明快取的識別符號是Cisco IOS中的「web-cache」一詞。若要在路由器上啟用服務99（反向透明快取）並指定將執行重新導向的連線埠，請在全域組態模式下新增以下命令：

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

配置反向透明快取時，運行WCCP服務99的路由器會攔截定向到Web伺服器的請求。命令**ip wccp 99 redirect out**應用於您要在其指向Web伺服器的路徑中攔截客戶端HTTP資料包的介面。通常是Web伺服器VLAN。這通常不是安裝快取引擎的VLAN。

WCCP處於活動狀態後，路由器會在配置了WCCP重定向的所有埠上偵聽。為了發出其存在訊號，快取引擎會持續將WCCP **Here I am** packets傳送到路由器清單中配置的IP地址。

在路由器和快取之間形成WCCP連線。要檢視連線資訊，請發出**show ip wccp**命令。

路由器識別符號是快取引擎所看到的路由器的IP地址。此識別符號不一定是重定向流量到達快取所使用的路由器介面。本示例中的路由器識別符號為192.168.15.1。

```
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**命令會提供有關快取的詳細資訊。

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

**Redirection**欄位表示用於將封包從路由器重新導向到快取引擎的方法。此方法可以是通用路由封裝(GRE)或第2層。使用GRE時，封包將封裝在GRE封包中。使用第2層時，封包會直接傳送到快取，但快取引擎和交換器或路由器必須鄰近第2層才能進行第2層重新導向。

**Initial Hash Info**和**Assigned Hash Info**欄位中以十六進位制表示的**Hash Allocation**是分配給此快取的

雜湊桶數。所有可能的源Internet地址都劃分為64個大小相等的範圍，每個範圍有一個儲存段，並且每個快取都分配了來自這些儲存段源地址範圍的數個的流量。此數量由WCCP根據快取的負載和負載加權動態管理。如果只安裝了一個快取，則可能將此快取分配給所有儲存桶。

當路由器開始將封包重新導向到快取引擎時，Total Packets Redirected欄位中的數目會增加。

Total Packets Unassigned欄位是未重新導向的封包數，因為封包未指派給任何快取。在此示例中，資料包數為5。在初始發現快取期間可能未分配資料包，或在刪除快取時以較小的間隔未分配資料包。

```
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
```

如果路由器沒有獲取快取，則調試WCCP活動可能很有用。每當路由器從快取收到Here I am packet時，都會以I see you packet作為回應，此情況在調試中報告。可用的debug命令是debug ip wccp events和debug ip wccp packets。

**附註：**使用 debug 指令之前，請先參閱[有關 Debug 指令的重要資訊](#)。

以下輸出提供一般WCCP偵錯訊息的範例：

```
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

```

為了提高偵錯等級，您可能希望追蹤IP封包流量，以便檢查路由器是否收到來自快取引擎的封包。為了避免在生產環境中使路由器超載並僅顯示感興趣的流量，可以使用ACL將調試限制到以快取的IP地址作為源的資料包。示例ACL是**access-list 130 permit ip host 192.168.15.2 host 192.168.15.1**。

```

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

```

如果路由器未看到任何快取且未看到WCCP活動，請檢查基本連通性。嘗試從路由器ping快取，或從快取ping路由器。如果ping操作成功，配置中可能會出現錯誤。

如果擷取了快取，但沒有重新導向封包，請確認路由器是否收到流量，以及流量是否已轉送到應用 `ip wccp 99 redirect out` 指令的介面。請記住，攔截和重定向的流量只是導向到TCP埠80的流量。

如果流量仍然未被重定向，並且Web內容直接來自伺服器，請驗證快取是否正確傳遞了擷取內容的指令。您必須擁有一些有關WCCP的背景資訊才能完成此操作。

WCCP識別兩種不同型別的服務：標準和動態。路由器隱式知道標準服務。也就是說，不需要通知路由器使用埠80，因為它已經知道這樣做。普通透明快取（Web快取 — 標準服務0）是一種標準服務。

在所有其他情況下（包括透明快取），路由器會被告知要攔截哪個連線埠。此資訊在 `Here I am packet` 中傳輸。

您可以發出 `debug ip packet dump` 命令以檢查封包本身。使用建立的ACL僅對快取引擎傳送的資料包進行調試。

```

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

```

使用此命令，可以確定是否通告埠，而無需檢視整個請求註解(RFC)。如果未通告埠，則問題很可能出在快取的配置中。

有關詳細資訊，請參閱 [Web快取協調協定V2.0](#)。

如果已經獲取快取並已重定向資料包，但Internet客戶端無法瀏覽伺服器，請檢查快取是否連線到Internet和伺服器。從快取ping Internet上的各種IP地址以及您的某些內部伺服器。如果對完全限定的域(URL)而不是IP地址執行ping，請確保指定要在快取配置中使用的DNS伺服器。

如果您不確定快取是否處理請求，可以調試快取中的HTTP活動。為了調試快取中的HTTP活動，必須限制流量以避免超載快取。在路由器上，使用Internet中一台客戶機的源IP地址建立一個ACL，您

可以將該地址用作測試裝置，然後使用全域性命令ip wccp 99的redirect-list選項進行測試。

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

建立並套用ACL後，請完成以下步驟：

1. 使用debug http all ( Cisco Cache Engine版本2.x ) 或debug http all ( Cisco Cache Engine版本3和ACNS版本4、5 ) 指令，啟用快取中的HTTP調試。
2. 啟用終端監控(發出term mon命令)。
3. 嘗試從ACL中配置的客戶端中瀏覽其中一台伺服器。

以下是輸出範例：

```
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
```

可在調試中找到的相關資訊以粗體突出顯示出來。

以下是網頁事務處理的不同階段：

1. 從客戶端接收的HTTP請求標頭。
2. 傳送到伺服器的HTTP請求標頭。
3. 從伺服器接收的HTTP響應標頭。
4. 傳送到客戶端的HTTP響應報頭。

如果瀏覽的網頁包含多個對象，則存在此事件序列的多個例項。使用最簡單的請求來減少調試輸出。

在Catalyst 6500或Cisco 7600路由器上，功能管理器處理Cisco IOS中配置的所有功能，以提供額外的故障排除層。當在這些裝置中配置第3層功能時，定義如何處理接收幀的資訊會傳遞到交換機或路由器的第2層控制功能（功能管理器）。對於WCCP，此控制資訊定義哪些資料包被IOS和WCCP攔截並定向到透明快取。

**show fm features**命令會顯示在Cisco IOS中啟用的功能。您可以使用此命令檢查快取引擎是否正確通告要攔截的埠。

```
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
```

**show fm int vlan 200** 命令會顯示三元內容可定址記憶體(TCAM)的確切內容。

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:線路定義來自快取引擎的幀上的偵聽旁路。否則將會產生重新導向回圈。vmr IP# 2:線路定義攔截將連線埠80作為目的地的所有封包。如果埠80未顯示在第二行中，但WCCP處於活動狀態，且路由器可以使用快取，則快取配置中可能會出現問題。收集Here I am packet的轉儲，以確定快取是否傳送埠。

如果在進行疑難排解後無法解決問題，請將該問題報告給思科[技術協助中心\(TAC\)](#)。

以下是您必須提供給Cisco TAC的一些基本資訊。在路由器上收集以下資訊：

- **show tech**命令的輸出。如果**show tech**輸出的大小有困難，則可替換**show running-config**和**show version output**命令的輸出。
- **show ip wccp**命令的輸出。
- **show ip wccp web-cache detail**命令的輸出。
- 如果路由器和Web快取之間的通訊似乎存在問題，請在出現問題時提供**debug ip wccp events**和**debug ip wccp packets**命令的輸出。

在Cache Engine ( 僅限Cisco Cache Engine ) 上，收集**show tech**命令的輸出。

聯絡TAC時，請完成以下步驟：

1. 提供問題的清晰描述。您應該包括以下問題的答案：症狀是什麼？是經常發生還是很少發生？更改配置後問題是否開始？是否使用思科或第三方快取？
2. 提供拓撲的清晰說明。包括一個圖表，這樣會使它更清晰。
3. 提供您認為對解決問題有用的任何其他資訊。

以下是組態範例的輸出：

```

***** 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
```

## **相關資訊**

- [Cisco Cache軟體](#)
- [Cisco 500系列快取引擎](#)
- [網路快取通訊協定 \(WCCP\)](#)
- [Cisco Cache Engine 2.0軟體下載頁面\(僅限註冊客戶\)](#)
- [Cisco Cache Engine 3.0軟體下載頁面\(僅限註冊客戶\)](#)
- [技術支援與文件 - Cisco Systems](#)