

# Pesquisando defeitos o cache transparente reverso para o WCCP

## Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenções](#)

[Configuração](#)

[Informações Relacionadas](#)

## [Introdução](#)

Este documento descreve como resolver problemas relativos ao Web Cache Communication Protocol (WCCP) quando usado para implantar o cache transparente reverso.

## [Pré-requisitos](#)

### [Requisitos](#)

Não existem requisitos específicos para este documento.

### [Componentes Utilizados](#)

As informações neste documento são baseadas nestas versões de software e hardware:

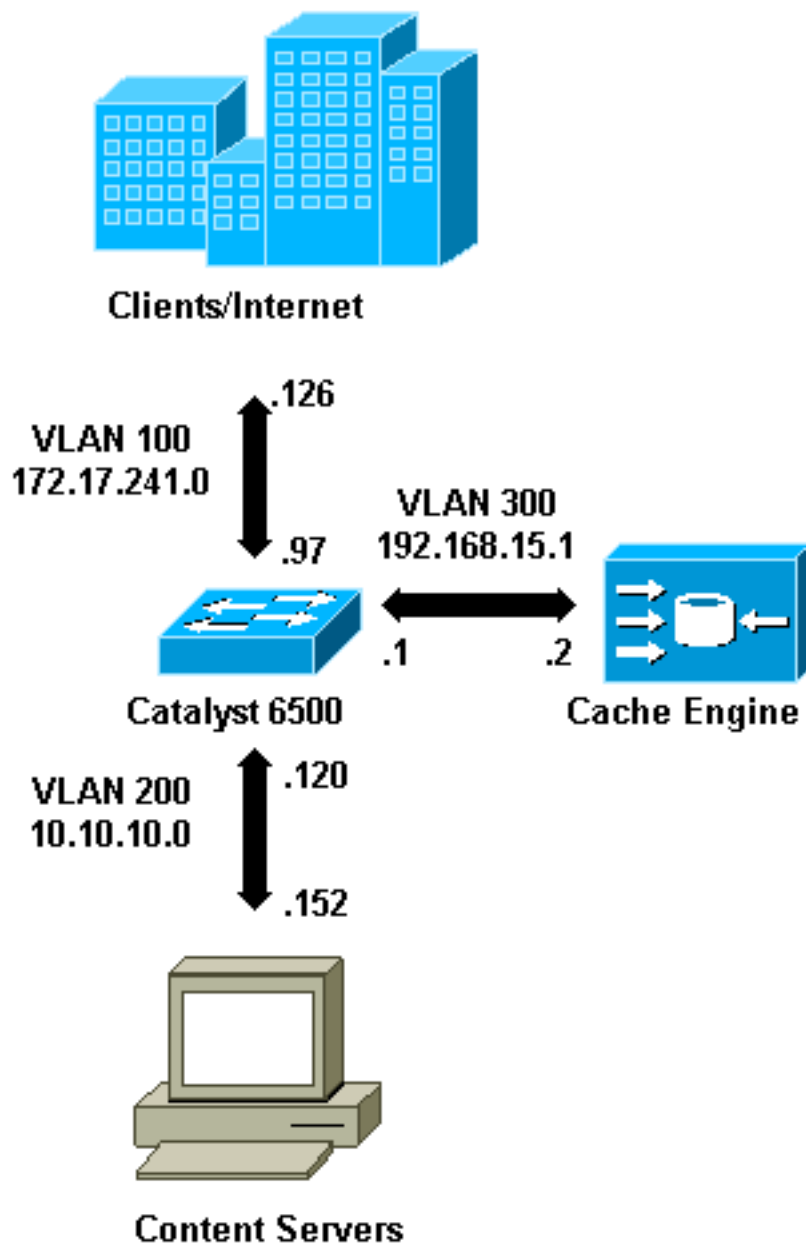
- Catalyst 6500 com Supervisor 1 e MSFC1 configurado no modo nativo
- Software Release 12.1(8a)EX de Cisco IOS® (c6sup11-jsv-mz.121-8a.EX.bin)
- Motor 550 do esconderijo com versão 2.51

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

### [Convenções](#)

Consulte as [Convenções de Dicas Técnicas da Cisco](#) para obter informações sobre convenções de documentos.

## Configuração



Quando você instala um motor do esconderijo, Cisco recomenda que você configura somente os comandos necessários executar o WCCP. Você pode adicionar outros recursos, tais como a autenticação ao roteador e às lista da reorientação dos clientes, em um outro dia.

No motor do esconderijo, você deve especificar o endereço IP de Um ou Mais Servidores Cisco ICM NT do roteador e a versão do WCCP que você quer se usar.

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

Uma vez que o endereço IP de Um ou Mais Servidores Cisco ICM NT e a versão do WCCP são configurados, você pôde ver que uma mensagem que advertisse o serviço 99 deve ser ativada no roteador a fim executar o cache transparente reverso. O serviço 99 é o identificador de serviço WCCP para o cache transparente reverso. O cache transparente do identificador para cache



```
Packets Redirected:      0
Connect Time:           00:00:39
```

O campo da `reorientação` representa o método usado para reorientar os pacotes do roteador ao motor do esconderijo. Este método é Generic Routing Encapsulation (GRE) ou camada 2. Com GRE, os pacotes são encapsulados em um pacote GRE. Com camada 2, os pacotes são enviados em linha reta ao esconderijo, mas o motor do esconderijo e o interruptor ou o roteador devem ser a camada 2 adjacente para a reorientação da camada 2.

A atribuição da mistura representada no hexadecimal na informação inicial da mistura e nos campos de informação atribuídos da mistura é o número de cubetas da mistura que são atribuídas a este esconderijo. Todos os endereços do Internet do origem possível são divididos no igual 64 - fez sob medida escalas, uma cubeta pela escala, e cada esconderijo é atribuído a tráfego de um número estas escalas de endereço de origem da cubeta. Esta quantidade é controlada dinamicamente pelo WCCP de acordo com a carga e a ponderação de carga do esconderijo. Se você tem somente um esconderijo instalado, este esconderijo pôde ser atribuído todas as cubetas.

Quando o roteador começa reorientar pacotes ao motor do esconderijo, o número nos `pacotes total reorientou` aumentos do campo.

O campo `Unassigned` dos `pacotes total` é o número de pacotes que não foram reorientados porque não foram atribuídos a nenhum esconderijo. Neste exemplo, o número de pacotes é 5. `pacotes` pôde ser `unassigned` durante a descoberta inicial dos esconderijos ou para um intervalo pequeno quando um esconderijo é removido.

```
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
```

Se o esconderijo não obtém adquirido pelo roteador, pôde ser útil debugar a atividade de WCCP. Sempre que o roteador me recebe **aqui é o pacote** do esconderijo, responde **comigo vê-o** pacote, e este é relatado no debuga. **Os comandos debug** disponíveis são **debugam eventos WCCP IP** e **debugam pacotes do wccp IP**.

**Nota:** Consulte [Informações Importantes sobre Comandos de Depuração](#) antes de usar comandos **debug**.

Esta saída fornece uma amostra de WCCP normal debuga mensagens:

```
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

```

A fim aumentar o nível de debug, você pôde querer seguir o tráfego do pacote IP a fim verificar se o roteador recebesse pacotes do motor do esconderijo. A fim evitar sobrecarregar um roteador em um ambiente de produção e a fim mostrar somente o tráfego interessante, você pode usar um ACL para restringir debuga somente aos pacotes que têm o endereço IP de Um ou Mais Servidores Cisco ICM NT do esconderijo como a fonte. Uma amostra ACL é host 192.168.15.1 de 192.168.15.2 do host da licença IP da lista de acesso 130.

```

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

```

Caso nenhum esconderijo estiver considerado pelo roteador e nenhuma atividade de WCCP estiver considerada, verifique a conectividade básica. Tente sibilhar o esconderijo do roteador ou do roteador do esconderijo. Se o sibilo trabalha, um erro pôde existir na configuração.

Se o esconderijo está adquirido, mas nenhum pacote está reorientado, verifique que o roteador receba o tráfego e que o tráfego está enviado à relação onde o **comando ip wccp 99 redirect out** é aplicado. Recorde que o tráfego que é interceptado e reorientado é somente o tráfego dirigido à porta TCP 80.

Se o tráfego não está sendo reorientado ainda e o conteúdo da Web está vindo em linha reta dos server, verifique que o esconderijo passa corretamente a instrução no que interceptar. Você deve ter alguma informações de fundo no WCCP a fim terminar esta ação.

O WCCP reconhece dois tipos de serviços diferentes: *padrão* e *dinâmico*. O roteador sabe implicitamente de um serviço padrão. Isto é, o roteador não precisa de ser dito para usar a porta 80, porque já sabe para fazer assim. O cache transparente normal (cache de web - serviço padrão 0) é um serviço padrão.

Em todos os casos restantes (que inclui o cache transparente), o roteador é dito que porta a interceptar. Esta informação é passada no **aqui mim é** pacote.

Você pode emitir o **comando debug ip packet dump** a fim examinar os pacotes eles mesmos. Use o ACL criado para debugar somente os pacotes enviados pelo motor do esconderijo.

```

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

```

Com este comando, você pode determinar mesmo se a porta está anunciada sem a necessidade de ver a solicitação para comentários (RFC) inteira. Se a porta não é anunciada, o problema é mais provável na configuração do esconderijo.

Refira o [protocolo web cache coordination V2.0](#) para mais informação.

Se o esconderijo está adquirido e os pacotes estão reorientados, mas seus clientes de Internet não podem consultar seus server, verifique se o esconderijo tenha a Conectividade ao Internet e a seus server. Sibila do esconderijo aos vários endereços IP de Um ou Mais Servidores Cisco ICM NT no Internet e a alguns de seus servidores internos. Se você sibila os domínios totalmente qualificados (URL) em vez dos endereços IP de Um ou Mais Servidores Cisco ICM NT, seja certo que você especifica o servidor DNS para se usar na configuração de cache.

Se você é incerto se o esconderijo processa os pedidos, você pode debugar a atividade de HTTP no esconderijo. A fim debugar a atividade de HTTP no esconderijo, você deve restringir o tráfego para evitar sobrecarregar o esconderijo. No roteador, crie um ACL com o endereço IP de origem de um cliente no Internet que você pode usar como um dispositivo para seus testes e use a reorientar-lista da opção do **wccp 99** do comando global **IP**.

```

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

```

Uma vez que você cria e aplica o ACL, termine estas etapas:

1. Ative o HTTP debugam no esconderijo com o comando `debug http all all` (versão 2.x do Cisco Cache Engine) ou `debugam HTTP todo` (versão 3 do Cisco Cache Engine e versão de ACNS 4, 5).
2. Ative o monitoramento de terminal (emita o **comando term mon**).
3. Tente consultar um de seus server do cliente que você configurou no ACL.

Está aqui um exemplo da saída:

```

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_rcv_zbuf() 0xb20c800: Register to rcv 2107 bytes timeout 120 sec
HttpServerRecvCallBack(): Rcv 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 rcv: 0xb84a080 len 4096 timeout 0x3a98
ms ctx 0xb87d800
cework_cleanup_final() End the request: 0xb20c800 0xb20c838 0xb20c8e0
```

A informação relevante que você pôde encontrar debugar é destacada em **corajoso**.

Estas são as fases diferentes de uma transação da página do página da web:



1. Encabeçamentos de pedido do HTTP recebidos do cliente.
2. Encabeçamentos de pedido do HTTP enviados ao server.
3. Encabeçamentos de resposta HTTP recebidos do server.
4. Encabeçamentos de resposta HTTP enviados ao cliente.

Se o página da web que você consulta contém objetos múltiplos, múltiplas instâncias desta sequência de evento existe. Use o pedido possível o mais simples reduzir o resultado do debug.

Em um Catalyst 6500 ou em um Cisco 7600 Router, um gerente da característica segura todas as características configuradas no Cisco IOS a fim fornecer uma camada adicionada de Troubleshooting. Quando uma característica da camada 3 é configurada nestes dispositivos, a informação que define como segurou os frames recebidos está passada às funções de controle da camada 2 do interruptor ou do roteador (gerente da característica). Para o WCCP, esta informação de controle define que pacotes são interceptados por IO e por WCCP e dirigidos ao cache transparente.

**O comando show fm features** indica as características que são permitidas no Cisco IOS. Você pode usar este comando a fim verificar se a porta interceptar esteja anunciada corretamente pelo motor do esconderijo.

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

O comando `show fm int vlan 200` indica o índice exato do Ternary Content Addressable Memory (TCAM).

```
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
```

O valor IP do vmr # 1: a linha define o desvio da interceptação nos quadros que vêm do motor do esconderijo. Sem isto, haveria um laço da reorientação. O valor IP do vmr # 2: a linha define a interceptação de todos os pacotes que têm a porta 80 como seu destino. Se a porta 80 não está indicada na segunda linha, mas o WCCP é ativo e o esconderijo é útil pelo roteador, a seguir pôde haver um problema na configuração de cache. Recolha uma descarga do [aquí mim são pacote](#) a fim determinar mesmo se a porta está enviada pelo esconderijo.

Se você é incapaz de resolver o problema depois que você pesquisa defeitos, relate o problema ao [centro de assistência técnica da Cisco \(TAC\)](#).

Está aqui alguma informação básica que você deve fornecer ao tac Cisco. Do roteador, recolha esta informação:

- A saída do **comando show tech**. A saída dos **comandos show running-config e show version output** pode ser substituída se há uma dificuldade com o tamanho da saída da **tecnologia da mostra**.
- A saída do **comando show ip wccp**.
- A saída do **comando show ip wccp web-cache detail**.
- Se parece haver um problema com uma comunicação entre o roteador e o cache de web, forneça a saída dos **comandos debug ip wccp events e debug ip wccp packets** quando o problema ocorrer.

No motor do esconderijo (motores do Cisco Cache somente), recolha a saída do **comando show tech**.

Quando você contacta o TAC, termine estas etapas:

1. Forneça uma descrição clara do problema. Você deve incluir respostas a estas perguntas: Que são os sintomas? Ocorre todo o tempo ou raramente? O problema começou

- após uma mudança na configuração? Cisco ou os esconderijos da 3ª parte são usados?
2. Forneça uma descrição clara da topologia. Inclua um diagrama se isso o fará mais claro.
  3. Forneça toda a outra informação que você pensar é útil em resolver o problema.

Está aqui a saída de uma configuração de exemplo:

```
***** 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

```

## [Informações Relacionadas](#)

- [Cisco Cache Software](#)
- [Cisco 500 Series Cache Engines](#)
- [Web Cache Communications Protocol \(WCCP\)](#)
- [Página de download de software do Cisco Cache Engine 2.0 \(clientes registrados somente\)](#)
- [Página de download de software do 3.0 do Cisco Cache Engine \(clientes registrados somente\)](#)

- [Suporte Técnico e Documentação - Cisco Systems](#)