

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Configuración](#)

[Información Relacionada](#)

Introducción

Este documento describe cómo solucionar problemas de Web Cache Communication Protocol (WCCP) cuando se utiliza para implementar caché transparente inversa.

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

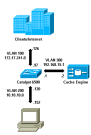
- Catalyst 6500 con el Supervisor 1 y MSFC1 configurado en el modo nativo
- Software Release 12.1(8a)EX de Cisco IOS® (c6sup11-jsv-mz.121-8a.EX.bin)
- Motor 550 del caché con la versión 2.51

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Consulte [Convenciones de Consejos Técnicos de Cisco](#) para obtener información sobre las convenciones sobre documentos.

Configuración



Cuando usted instala un motor del caché, Cisco recomienda que usted configura solamente los comandos necesarios implementar el WCCP. Usted puede agregar las otras funciones, tales como autenticación al router y a las listas del cambio de dirección de los clientes, más adelante.

En el motor del caché, usted debe especificar la dirección IP del router y la versión del WCCP que usted quiere utilizar.

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

Una vez que el IP Address y la versión del WCCP se configuran, usted puede ser que vea que un mensaje que advierte el servicio 99 se debe activar en el router para implementar el Almacenamiento en memoria caché transparente reverso. El servicio 99 es el identificador de servicio WCCP para el Almacenamiento en memoria caché transparente reverso. El Almacenamiento en memoria caché transparente del identificador para normal es la palabra "caché Web" en el Cisco IOS. Para activar el servicio 99 (Almacenamiento en memoria caché transparente reverso) en el router y para especificar el puerto en donde el cambio de dirección será realizado, agregue estos comandos en el modo de configuración global:

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

Cuando usted configura el Almacenamiento en memoria caché transparente reverso, el router que funciona con el servicio 99 WCCP intercepta las peticiones dirigidas a los servidores Web. Aplican al comando ip wccp 99 redirect out en la interfaz donde usted quiere interceptar los paquetes HTTP cliente en su trayectoria a su servidor Web. Típicamente, éste es el VLA N del servidor Web. Éste no es normalmente el VLA N donde el motor del caché está instalado.

Una vez que el WCCP es activo, el router escucha en todos los puertos que hagan que el WCCP reoriente configurado. Para señalar su presencia, el motor del caché envía continuamente el WCCP **aquí que soy los** paquetes a los IP Addresses que se configuran en la lista del router.

Una conexión WCCP entre el router y el caché se forma. Para ver la información de conexión, publique el **comando show ip wccp**.

El identificador de router es la dirección IP del router pues es visto por los motores del caché. Este identificador no es necesariamente la interfaz del router usada por el tráfico redirigido para alcanzar el caché. El identificador de router en este ejemplo es 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
```

El comando show ip wccp 99 detail proporciona la información detallada sobre los cachés.

```
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
```

El campo del cambio de dirección representa el método usado para reorientar los paquetes del router al motor del caché. Este método es Generic Routing Encapsulation (GRE) o la capa 2. Con el GRE, los paquetes se encapsulan en un Paquete GRE. Con la capa 2, los paquetes se envían

derecho al caché, pero el motor del caché y el Switch o el router deben ser la capa 2 adyacente para el cambio de dirección de la capa 2.

La asignación del hash representada en el hexadecimal en la información inicial del hash y los campos de información asignados del hash es el número de compartimientos del hash que se asignen a este caché. Dividen a todas las direcciones de Internet de la fuente posible en el igual 64 - clasificó los rangos, un compartimiento por el rango, y cada caché se asigna a tráfico de varios éstos los rangos de dirección de origen del compartimiento. Esta cantidad es manejada dinámicamente por el WCCP según la carga y el equilibrio de carga del caché. Si usted hace solamente un caché instalar, este caché se pudo asignar todos los compartimientos.

Cuando el router comienza a reorientar los paquetes al motor del caché, el número en los totales de paquetes reorientó los aumentos del campo.

El campo no asignado de los totales de paquetes es el número de paquetes que no fueron reorientados porque no fueron asignados a ningún caché. En este ejemplo, el número de paquetes es 5. paquetes pudo ser no asignado durante la detección inicial de cachés o para un pequeño intervalo cuando se quita un caché.

```
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
```

Si el caché no consigue adquirido por el router, puede ser que sea útil hacer el debug de la actividad de WCCP. Siempre que el router me reciba aquí es el paquete del caché, contesta con yo le ve paquete, y esto está señalada en los debugs. Los comandos debug disponibles son eventos wccp del IP del debug y hacen el debug de los paquetes del wccp del IP.

Nota: Consulte [Información Importante sobre Comandos de Debug](#) antes de usar un comando debug.

Esta salida proporciona una muestra de mensajes normales del debug WCCP:

```
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
```

Para aumentar el nivel de debug, usted puede ser que quiera localizar el tráfico del paquete del IP para marcar si el router recibe los paquetes del motor del caché. Para evitar sobrecargar a un router en un entorno de producción y para mostrar solamente el tráfico interesante, usted puede utilizar un ACL para restringir los debugs solamente a los paquetes que tienen la dirección IP del caché como fuente. Una muestra ACL es host 192.168.15.1 de 192.168.15.2 del host del IP del permiso de la lista de acceso 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
```

En caso que no se considere ningunos cachés por el router y no se considera ninguna actividad de WCCP, marque la conectividad básica. Intente hacer ping el caché del router o del router del caché. Si el ping trabaja, un error pudo existir en la configuración.

Si se adquiere el caché, pero no se reorienta ningunos paquetes, verifique que el router reciba el tráfico y que el tráfico está remitido a la interfaz donde está aplicado el comando **ip wccp 99 redirect out**. Recuerde que el tráfico se intercepta y se reorienta que es solamente el tráfico dirigido al puerto TCP 80.

Si el tráfico todavía no se está reorientando y el contenido de la Web está viniendo derecho de los servidores, verifique que el caché pase correctamente la instrucción en qué interceptar. Usted debe tener cierta información previa en el WCCP para completar esta acción.

El WCCP reconoce dos diversos tipos de servicio: *estándar* y *dinámico*. El router sabe implícito de un servicio estándar. Es decir, el router no necesita ser dicho para utilizar el puerto 80, porque sabe ya para hacer tan. El Almacenamiento en memoria caché transparente normal (caché Web - el servicio estándar 0) es un servicio estándar.

En el resto de casos (que incluye el Almacenamiento en memoria caché transparente), dicen el

router qué puerto a interceptar. Esta información se pasa en **aquí yo es paquete**.

Usted puede publicar el **comando debug ip packet dump** para examinar los paquetes ellos mismos. Utilice el ACL creado para hacer el debug de solamente los paquetes enviados por el motor del caché.

```
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 (FFF...). 072C5190: FFFFFFFF
FFFFFFFF FFFFFFFF FFFFFFFF ..... 072C51A0: FFFFFFFF FFFFFFFF FFFF0000 00000000
..... 072C51B0: 00050018 00000002 00000001 C0A80F01 .....@(..
072C51C0: 0000000C 00000001 C0A80F02 00080008 .....@(.
00000001 30      .....0
```

Con este comando, usted puede determinar independientemente de si el puerto está hecho publicidad sin la necesidad de ver la Solicitud de comentarios (RFC) entera. Si el puerto no se hace publicidad, el problema es más probable en la configuración del caché.

Refiera al [protocolo web cache coordination V2.0](#) para más información.

Si se adquiere el caché y se reorientan los paquetes, pero sus clientes de Internet no pueden hojear sus servidores, marque si el caché tiene Conectividad a Internet y a sus servidores. Haga ping del caché a los diversos IP Addresses en Internet y a algunos de sus servidores internos. Si usted hace ping los dominios calificado completamente (URL) en vez de los IP Addresses, esté seguro que usted especifica al servidor DNS para utilizar en la configuración de caché.

Si usted es inseguro si el caché procesa las peticiones, usted puede hacer el debug de la actividad de HTTP en el caché. Para hacer el debug de la actividad de HTTP en el caché, usted debe restringir el tráfico para evitar sobrecargar el caché. En el router, cree un ACL con la dirección IP de origen de un cliente en Internet que usted puede utilizar como dispositivo para sus pruebas y utilice la reorientar-lista de la opción del **wccp 99 del IP del comando global**.

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

Una vez que usted crea y aplica el ACL, complete estos pasos:

1. Active el debug HTTP en el caché con el comando `debug http all all` (versión 2.x del Cisco Cache Engine) o **haga el debug de HTTP todo** (la versión 3 y la versión ACNS 4 del Cisco Cache Engine, 5).
2. Active el control de terminal (publique el **comando term mon**).
3. Intente hojear uno de sus servidores del cliente que usted configuró en el ACL.

Aquí está un ejemplo de la salida:

```
irq0#conf tcework_readfirstdata() Start the rcv: 0xb820800 len 4096 timeout      0x3a98 ms ctx
0xb87d800      cework_rcvurl() 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-AliveProtocol 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: 172.17.241.126cework_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/htmlGetUpdateCode(): 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-alivecework_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

```

La información pertinente que usted puede ser que encuentre en el debug se resalta en **intrépido**.

Éstas son las diversas fases de una transacción de la página de la página web:

1. Encabezados de pedido de HTTP recibidas del cliente.
2. Encabezados de pedido de HTTP enviadas al servidor.
3. Encabezados del HTTP de respuesta recibidas del servidor.
4. Encabezados del HTTP de respuesta enviadas al cliente.

Si existe la página web que usted hojea contiene los varios objetos, las instancias múltiples de esta Secuencia de eventos. Utilice la petición posible más simple de reducir la salida de los debugs.

En un Catalyst 6500 o un Cisco 7600 Router, un administrador de la característica maneja todas las características configuradas en el Cisco IOS para proporcionar una capa agregada de troubleshooting. Cuando una característica de la capa 3 se configura en estos dispositivos, la información que define cómo manejó las tramas recibidas se pasa a las funciones de control de la capa 2 del Switch o del router (el administrador de la característica). Para el WCCP, esta información de control define qué paquetes son interceptados por el IOS y el WCCP y dirigidos al caché transparente.

El comando show fm features visualiza las características que se habilitan en el Cisco IOS. Usted puede utilizar este comando para marcar si el puerto interceptar es hecho publicidad correctamente por el motor del caché.

```

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: 1The 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
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

```

El comando `show fm int vlan 200` visualiza el contenido exacto del 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

```

El valor IP del vmr # 1: la línea define puente de la interceptación en las tramas que vienen del motor del caché. Sin esto, habría un loop del cambio de dirección. El valor IP del vmr # 2: la línea define la interceptación de todos los paquetes que tienen puerto 80 como su destino. Si el puerto 80 no se visualiza en la segunda línea, pero el WCCP es activo y el caché es usable por el router, después pudo haber un problema en la configuración de caché. Recoja un vaciado del **aquí yo son** paquete para determinar independientemente de si el puerto es enviado por el caché.

Si usted no puede solucionar el problema después de que usted Troubleshooting, señale el problema al

Aquí está una cierta información básica que usted debe proporcionar al TAC de Cisco. Del router, recoja esta información:

- La salida del **comando show tech**. La salida de los **comandos show running-config y show version output** puede ser substituida si hay dificultad con el tamaño de la salida de la **tecnología de la demostración**.
- La salida del **comando show ip wccp**.
- La salida del **comando show ip wccp web-cache detail**.
- Si parece haber un problema con la comunicación entre el router y caché Web, proporcione la salida de los **comandos debug ip wccp events y debug ip wccp packets** mientras que está ocurriendo el problema.

En el motor del caché (motores del Cisco Cache solamente), recoja la salida del **comando show tech**.

Cuando usted entra en contacto TAC, complete estos pasos:

1. Proporcione una descripción clara del problema. Usted debe incluir las respuestas a estas preguntas: ¿Cuáles son los síntomas? ¿Ocurre todo el tiempo o infrecuentemente? ¿El problema comenzó después de un cambio en la configuración? ¿Se utiliza Cisco o los cachés de las de otras compañías?
2. Proporcione una descripción clara de la topología. Incluya un diagrama si eso lo hace más claro.
3. Proporcione cualquier otra información que usted piense sea útil en solucionar el problema.

Aquí está la salida de una configuración de muestra:

```

***** 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 runningBuilding 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

```

[Información Relacionada](#)

- [Software Cisco Cache](#)
- [Cisco Cache Engines de la serie 500](#)
- [Web Cache Communications Protocol \(WCCP\)](#)
- [Página de descarga del software del Cisco Cache Engine 2.0 \(clientes registrados solamente\)](#)
- [Página de descarga del software del 3.0 del Cisco Cache Engine \(clientes registrados solamente\)](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)