

Solución de problemas de almacenamiento en caché transparente inverso para WCCP

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[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.

[Prerequisites](#)

[Requirements](#)

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.

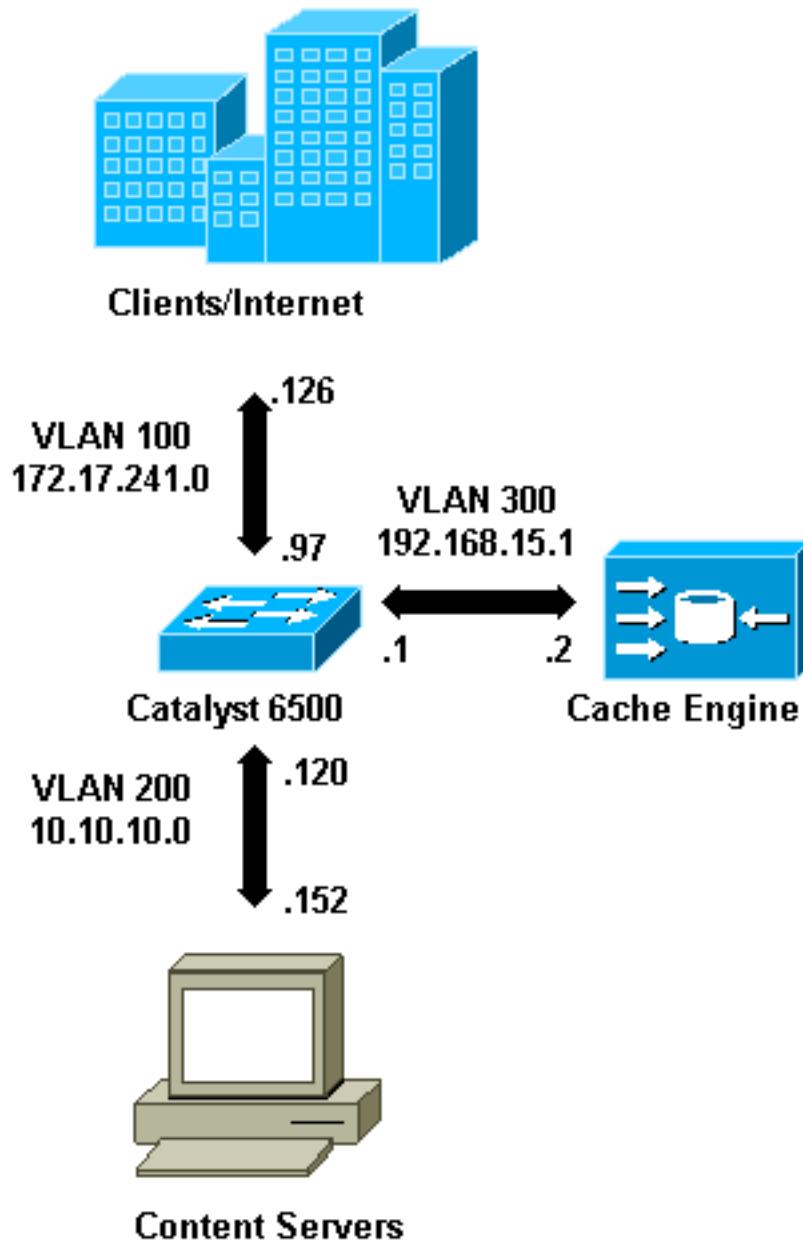
- Catalyst 6500 con Supervisor 1 y MSFC 1 configurados en modo nativo
- Software Cisco IOS® versión 12.1(8a)EX (c6sup11-jsv-mz.121-8a.EX.bin)
- Cache Engine 550 con la versión 2.51

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

[Convenciones](#)

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

Configuración



Cuando instala un Cache Engine, Cisco recomienda que configure solamente los comandos necesarios para implementar WCCP. Puede agregar otras funciones, como la autenticación al router y las listas de redirección de clientes, más adelante.

En Cache Engine, debe especificar la dirección IP del router y la versión de WCCP que desea utilizar.

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

Una vez configuradas la dirección IP y la versión de WCCP, es posible que vea un mensaje que avisa que el servicio 99 debe ser activado en el router para implementar el almacenamiento en

caché transparente inverso. El servicio 99 es el identificador de servicio WCCP para el almacenamiento en caché transparente inverso. El identificador para el almacenamiento en caché transparente normal es la palabra "web-cache" en Cisco IOS. Para activar el servicio 99 (almacenamiento en caché transparente inverso) en el router y para especificar el puerto donde se realizará la redirección, 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 configura el almacenamiento en caché transparente inverso, el router que ejecuta el servicio WCCP 99 intercepta las solicitudes dirigidas a los servidores web. El comando **ip wccp 99 redirect out** se aplica en la interfaz donde desea interceptar los paquetes HTTP del cliente en su trayecto hacia su servidor web. Normalmente, ésta es la VLAN del servidor web. Normalmente, esta no es la VLAN donde se instala el motor de memoria caché.

Una vez que WCCP está activo, el router escucha en todos los puertos que tienen la redirección WCCP configurada. Para indicar su presencia, el motor de memoria caché envía continuamente **paquetes WCCP Aquí estoy** a las direcciones IP configuradas en la lista del router.

Se forma una conexión WCCP entre el router y la memoria caché. Para ver la información de conexión, ejecute el comando **show ip wccp**.

El identificador del router es la dirección IP del router tal como la ven los Motores de memoria caché. Este identificador no es necesariamente la interfaz del router utilizada por el tráfico redirigido para alcanzar la memoria caché. El identificador del 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 información detallada sobre las memorias caché.

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

```

El campo `Redirección` representa el método utilizado para redirigir los paquetes del router al motor de memoria caché. Este método es Generic Routing Encapsulation (GRE) o Layer 2. Con GRE, los paquetes se encapsulan en un paquete GRE. Con la Capa 2, los paquetes se envían directamente a la memoria caché, pero el Cache Engine y el switch o router deben ser adyacentes a la Capa 2 para la redirección de la Capa 2.

La asignación de hash representada en hexadecimal en los campos `Información de hash inicial` y `Información de hash asignada` es el número de bloques de hash asignados a esta memoria caché. Todas las direcciones de Internet de origen posibles se dividen en 64 rangos de igual tamaño, una cubeta por rango, y a cada caché se le asigna tráfico de una serie de estos rangos de direcciones de origen de la cubeta. WCCP administra esta cantidad dinámicamente según la carga y el peso de carga de la memoria caché. Si sólo tiene una memoria caché instalada, esta memoria caché podría estar asignada a todos los bloques.

Cuando el router comienza a redirigir paquetes al motor de memoria caché, el número en el campo `Total de paquetes redirigidos` aumenta.

El campo `Total de paquetes sin asignar` es el número de paquetes que no fueron redirigidos porque no fueron asignados a ninguna memoria caché. En este ejemplo, el número de paquetes es 5. Los paquetes se pueden desasignar durante la detección inicial de memorias caché o durante un intervalo pequeño cuando se quita una memoria 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 router no adquiere la memoria caché, podría ser útil depurar la actividad WCCP. Cada vez que el router recibe un **Aquí soy** paquete de la memoria caché, responde con un **que le veo** paquete, y esto se informa en las depuraciones. Los comandos `debug` disponibles son `debug ip wccp events` y `debug ip wccp packets`.

Nota: Consulte [Información Importante sobre Comandos Debug](#) antes de utilizar los comandos `debug`.

Este resultado proporciona un ejemplo de mensajes de depuración WCCP normales:

```
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 depuración, es posible que desee rastrear el tráfico de paquetes IP para verificar si el router recibe paquetes del motor de memoria caché. Para evitar la sobrecarga de un router en un entorno de producción y para mostrar solamente el tráfico interesante, puede utilizar una ACL para restringir las depuraciones solamente a los paquetes que tienen la dirección IP de la memoria caché como origen. Un ejemplo de ACL es **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

```

En caso de que el router no vea ninguna memoria caché y no se vea ninguna actividad WCCP, verifique la conectividad básica. Intente hacer ping en la memoria caché desde el router o el router desde la memoria caché. Si el ping funciona, podría existir un error en la configuración.

Si se adquiere la memoria caché, pero no se redirecciona ningún paquete, verifique que el router reciba tráfico y que el tráfico se reenvíe a la interfaz donde se aplica el comando **ip wccp 99 redirect out**. Recuerde que el tráfico interceptado y redirigido es solamente el tráfico dirigido al puerto TCP 80.

Si el tráfico todavía no se redirige y el contenido web viene directamente de los servidores, verifique que la memoria caché pase correctamente la instrucción sobre qué interceptar. Debe tener información de fondo sobre WCCP para completar esta acción.

WCCP reconoce dos tipos diferentes de servicios: *estándar* y *dinámico*. El router conoce implícitamente un servicio estándar. Es decir, no es necesario indicar al router que utilice el puerto 80, porque ya sabe hacerlo. El almacenamiento en caché transparente normal (web-cache - servicio estándar 0) es un servicio estándar.

En todos los demás casos (que incluye almacenamiento en caché transparente), se indica al router qué puerto interceptar. Esta información se pasa en el paquete **Aquí estoy**.

Puede ejecutar el comando **debug ip packet dump** para examinar los paquetes por sí mismos. Utilice la ACL creada para depurar solamente los paquetes enviados por el motor de memoria

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 (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
```

Con este comando, puede determinar si el puerto se anuncia o no sin la necesidad de ver toda la solicitud de comentarios (RFC). Si el puerto no se anuncia, el problema es más probable en la configuración de la memoria caché.

Refiérase a [Protocolo de Coordinación de Caché Web V2.0](#) para obtener más información.

Si se adquiere la memoria caché y se redirigen los paquetes, pero los clientes de Internet no pueden examinar los servidores, verifique si la memoria caché tiene conectividad a Internet y a sus servidores. Haga ping desde la memoria caché a varias direcciones IP en Internet y a algunos de sus servidores internos. Si hace ping a dominios completos (URL) en lugar de direcciones IP, asegúrese de especificar el servidor DNS que se utilizará en la configuración de caché.

Si no está seguro de si la memoria caché procesa las solicitudes, puede depurar la actividad HTTP en la memoria caché. Para depurar la actividad HTTP en la memoria caché, debe restringir el tráfico para evitar sobrecargar la memoria caché. En el router, cree una ACL con la dirección IP de origen de un cliente en Internet que pueda utilizar como dispositivo para sus pruebas y utilice la opción **redirect-list** del comando global **ip wccp 99**.

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

Una vez que cree y aplique la ACL, complete estos pasos:

1. Active la depuración HTTP en la memoria caché con el comando **debug http all** (Cisco Cache Engine versión 2.x) o **debug http all** (Cisco Cache Engine versión 3 y ACNS versión 4, 5).
2. Active la supervisión de terminal (ejecute el comando **term mon**).
3. Intente examinar uno de sus servidores desde el cliente que configuró en la ACL.

Este es un ejemplo del resultado:

```
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

```

La información relevante que puede encontrar en la depuración se resalta en **negrita**.

Estas son las diferentes fases de una transacción de página Web:

1. Encabezados de solicitud HTTP recibidos del cliente.
2. Encabezados de solicitud HTTP enviados al servidor.
3. Encabezados de respuesta HTTP recibidos del servidor.
4. Encabezados de respuesta HTTP enviados al cliente.

Si la página web que examina contiene varios objetos, existen varias instancias de esta secuencia de eventos. Utilice la solicitud más simple posible para reducir el resultado de la depuración.

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

El comando **show fm features** muestra las funciones habilitadas en Cisco IOS. Usted puede utilizar este comando para verificar si el puerto a interceptar está correctamente anunciado por el Motor de 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: 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
```

El comando **show fm int vlan 200** muestra el contenido exacto de la Memoria direccionable de contenido ternario (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 de IP de vmr n° 1: line define la omisión de intercepción en las tramas que vienen del motor de memoria caché. Sin esto, habría un loop de redirección. Valor de IP de vmr n° 2: line define la intercepción de todos los paquetes que tienen el puerto 80 como su destino. Si el puerto 80 no se muestra en la segunda línea, pero WCCP está activo y la memoria caché es utilizable por el router, entonces podría haber un problema en la configuración de la memoria caché. Recopile un volcado del paquete **Aquí estoy** para determinar si el puerto es o no enviado por la memoria caché.

Si no puede resolver el problema después de resolver el problema, informe el problema al [Centro de asistencia técnica de Cisco \(TAC\)](#).

A continuación se incluye información básica que debe proporcionar al TAC de Cisco. En el router, recopile esta información:

- El resultado del comando **show tech**. La salida de los comandos **show running-config** y **show version output** se puede sustituir si hay dificultad con el tamaño del resultado de **show tech**.
- El resultado del comando **show ip wccp**.
- El resultado del comando **show ip wccp web-cache detail**.
- Si parece haber un problema con la comunicación entre el router y la memoria caché Web, proporcione la salida de los comandos **debug ip wccp events** y **debug ip wccp packets** mientras se produce el problema.

En Cache Engine (sólo Cisco Cache Engines), recopile el resultado del comando **show tech**.

Cuando se ponga en contacto con el TAC, complete estos pasos:

1. Proporcione una descripción clara del problema. Debe incluir respuestas a estas preguntas: ¿Cuáles son los síntomas? ¿Ocurre todo el tiempo o de forma poco frecuente? ¿El problema comenzó después de un cambio en la configuración? ¿Se utilizan cachés de Cisco o de terceros?
2. Proporcione una descripción clara de la topología. Incluya un diagrama si lo hace más claro.
3. Proporcione cualquier otra información que considere útil para resolver el problema.

A continuación se muestra el resultado de una configuración de ejemplo:

```
***** 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
```

[Información Relacionada](#)

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