

# Omgekeerd doorzichtige training voor probleemoplossing voor WCCP

## Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Conventies](#)

[Configuratie](#)

[Gerelateerde informatie](#)

## [Inleiding](#)

Dit document beschrijft hoe u Web Cache Communication Protocol (WCCP) problemen kunt oplossen wanneer deze wordt gebruikt om omgekeerde transparante caching te implementeren.

## [Voorwaarden](#)

### [Vereisten](#)

Er zijn geen specifieke vereisten van toepassing op dit document.

### [Gebruikte componenten](#)

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

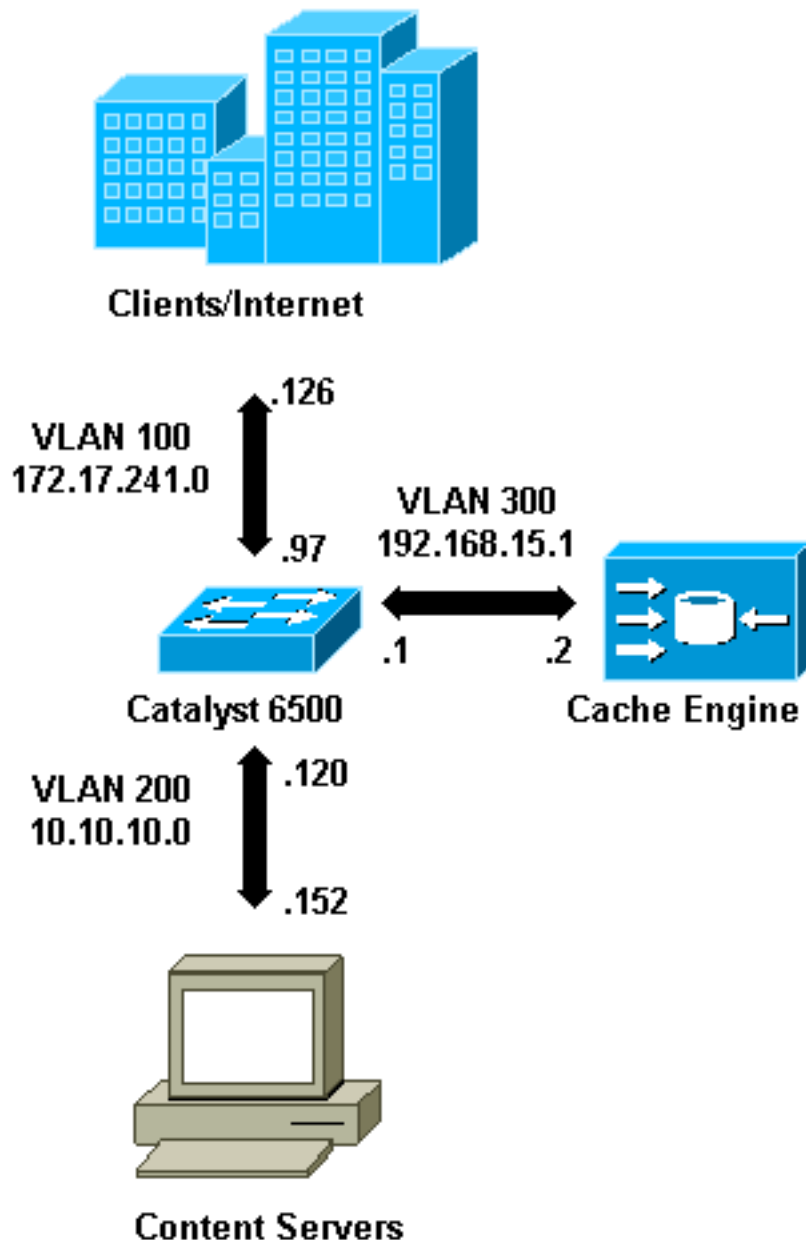
- Catalyst 6500 met supervisor 1 en MSFC 1 ingesteld in native modus
- Cisco IOS® software release 12.1(8a)EX (c6sup11-jsv-mz.121-8a.EX.bin)
- Cache Engine 550 met versie 2.5.1

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

### [Conventies](#)

Raadpleeg [Cisco Technical Tips Convention](#) voor informatie over documentconventies.

## [Configuratie](#)



Wanneer u een Cache Engine installeert, raadt Cisco u aan alleen de opdrachten te configureren die nodig zijn om WCCP uit te voeren. U kunt andere eigenschappen, zoals authenticatie aan de router en klanten omrichtingslijsten, op een later tijdstip toevoegen.

In de Cache Engine, moet u het IP-adres van de router en de versie van WCCP specificeren die u wilt gebruiken.

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

Zodra het IP-adres en de versie van WCCP zijn ingesteld, ziet u een bericht dat Service 99 waarschuwt en in de router moet worden geactiveerd om omgekeerde transparante caching te kunnen uitvoeren. Service 99 is de WCCP-service ID voor omgekeerde transparante caching. De identificator voor normale transparante caching is het woord "web-cache" in Cisco IOS. Om service 99 op de router te activeren (omgekeerde transparante caching) en om de poort te

specificeren waar de omleiding uitgevoerd zal worden, voegt u deze opdrachten in de mondiale configuratie-modus toe:

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

Wanneer u omgekeerde, transparante caching configureren, de router die WCCP-service 99 beheert, onderscheppingsverzoeken gericht op de webserver. De opdracht **ip wcp 99** is toegepast op de interface waar u de client HTTP-pakketten in hun pad naar uw webserver wilt onderscheppen. Meestal is dit het VLAN van de webserver. Dit is normaal niet het VLAN waar de Cache Engine is geïnstalleerd.

Zodra WCCP actief is, luistert de router op alle poorten die WCCP-omleiding hebben ingesteld. Om zijn aanwezigheid te signaleren, verstuurt de Cache Engine continu WCCP **Hier** versturen **ik** pakketten naar de IP-adressen die in de routerlijst zijn geconfigureerd.

Er wordt een WCCP-verbinding tussen de router en het cache gevormd. Geef de opdracht **ip wcp** op om verbindinginformatie te bekijken.

De router ID is het IP-adres van de router zoals deze door de Cache Engines wordt gezien. Deze identicator is niet noodzakelijkerwijs de router interface die door het hergerichte verkeer wordt gebruikt om het cache te bereiken. De router identifier in dit voorbeeld is 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
```

De opdracht **detaillering** over de caches op **ip Wcp 99** toont gedetailleerde informatie.

```
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
```

```

Hash Allotment:          256 (100.00%)
Packets Redirected:     0
Connect Time:           00:00:39

```

Het veld `Omlleiding` vertegenwoordigt de methode die wordt gebruikt om de pakketten van de router naar de Cache Engine om te sturen. Deze methode is of generiek Routing Encapsulation (GRE) of Layer 2. Met GRE worden pakketten ingesloten in een GRE-pakket. Met Layer 2 worden pakketten rechtstreeks naar het cache verzonden, maar de Cache Engine en switch of router moeten Layer 2 bij Layer 2-omleiding zijn.

De `Hash Allotment` in hexadecimaal weergegeven in de `Initiële Hash Info` en `Assigned Hash Info` velden is het aantal haken emmers dat aan deze cache is toegewezen. Alle mogelijke bron Internetadressen zijn verdeeld in 64 gelijke grootteklassen, één emmer per bereik, en elk cache wordt toegewezen verkeer van een aantal van deze emmer bron adresbereik. Dit bedrag wordt dynamisch door WCCP beheerd volgens de belasting- en belastingsweging van de cache. Als er maar één cache geïnstalleerd is, kan deze cache alle emmers toegewezen krijgen.

Wanneer de router pakketten opnieuw naar de Cache Engine begint te richten, wordt het aantal in het veld `Total Packets-omleiding` verhoogd.

Het veld `Total Packets UnToewijzing` is het aantal pakketten dat niet is omgeleid omdat ze niet zijn toegewezen aan een cache. In dit voorbeeld is het aantal pakketten 5. Packets kunnen niet worden toegewezen tijdens eerste ontdekking van caches of voor een klein interval wanneer een cache wordt verwijderd.

```

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

```

Als het cache niet door de router wordt aangeschaft, kan het handig zijn om de WCCP-activiteit te debug. Wanneer de router een **hier** ontvangt **ben ik** pakketjes uit de cache, het antwoordt met een pakketje **dat ik zie**, en dit wordt in de apparaten gemeld. De beschikbare **debug** opdrachten **debug ip-gebeurtenissen** en **debug ip-pakketten**.

**Opmerking:** Raadpleeg [Belangrijke informatie over debug Commands](#) voordat u **debug-**opdrachten gebruikt.

Deze uitvoer biedt een steekproef van normale WCCP-debug-berichten:

```

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

```

Om het debug niveau te verhogen, kunt u het IP-pakketverkeer overtrekken om te controleren of de router pakketten van de Cache Engine ontvangt. Om te vermijden een router in een productieomgeving te overladen en om alleen het interessante verkeer te tonen kunt u een ACL gebruiken om de diepten slechts tot de pakketten te beperken die het IP adres van het cache als bron hebben. Een steekproef ACL is toegangslijst 130 vergunninghouder ip 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

```

Als de router geen caches heeft gezien en er geen WCCP-activiteit is gezien, controleert u de basisconnectiviteit. Probeer het cache van de router of de router van het cache te pingelen. Als het pingelen werkt, zou een fout in de configuratie kunnen bestaan.

Als het cache wordt aangeschaft maar er geen pakketten worden hergeleid, controleert u of de router verkeer ontvangt en of het verkeer wordt doorgestuurd naar de interface waar de **ip wcp 99** opdracht om terug te sturen wordt toegepast. Denk eraan dat het verkeer dat wordt onderschept en opnieuw wordt gericht alleen het verkeer is dat naar TCP poort 80 wordt gericht.

Als het verkeer nog steeds niet wordt omgeleid en de webinhoud direct van de servers komt, controleer of de cache juist de instructie doorgeeft op wat te onderscheppen. U moet enige achtergrondinformatie over WCCP hebben om deze actie te voltooien.

WCCP erkent twee verschillende soorten diensten: *standaard* en *dynamisch*. De router kent impliciet van een standaarddienst. Dat wil zeggen dat de router niet hoeft te worden gezegd dat hij haven 80 moet gebruiken, omdat hij dat al weet. De normale transparante caching (web-cache - standaard service 0) is een standaardservice.

In alle andere gevallen (die transparante caching omvatten), wordt de router verteld welke haven aan onderschepping heeft. Deze informatie wordt doorgegeven in het **hier** pakje.

U kunt de opdracht **ip-pakketdumpen** uitvoeren om de pakketten zelf te onderzoeken. Gebruik ACL die wordt gemaakt om alleen de pakketten te reinigen die door de Cache Engine worden verzonden.

```

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

```

Met deze opdracht kunt u bepalen of de poort al dan niet wordt geadverteerd zonder dat u het gehele verzoek om Opmerkingen (RFC) moet bekijken. Als de poort niet wordt geadverteerd, is het probleem zeer waarschijnlijk in de configuratie van het cache.

Raadpleeg het [Coördinatieprotocol voor webcaches V2.0](#) voor meer informatie.

Als de cache wordt aangeschaft en pakketjes worden omgeleid, maar uw internetklanten kunnen niet door uw servers bladeren, controleren of de cache aansluitingen heeft op het internet en op uw servers. Ping van de cache naar verschillende IP-adressen op het internet en naar enkele van uw interne servers. Als u volledig gekwalificeerde domeinen (URLs) in plaats van IP adressen pingelt, zorg ervoor dat u de DNS server om in de cache configuratie te gebruiken specificeert.

Als u niet zeker bent of het cache de verzoeken verwerkt, kunt u de HTTP-activiteit in het cache debug. Om de HTTP activiteit in het cache te debug te geven moet u het verkeer beperken om overbelasting van het cache te voorkomen. Op de router, creëer een ACL met het bron IP adres van één client in het internet die u als apparaat voor uw tests kunt gebruiken en gebruik de optie **redirect-list** van het globale bevel **ip wcp 99**.

```

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

```

Zodra u ACL maakt en toepast, voltooit u deze stappen:

1. Activeer het HTTP debug in het cache met de opdracht **debug http all** (Cisco Cache Engine versie 2.x) of **debug http all** (Cisco Cache Engine versie 3 en ACNS versie 4.5).
2. Activeer terminalbewaking (voer de **term mon** commando uit).
3. Probeer een van uw servers te bladeren vanaf de client die u in ACL hebt ingesteld.

Hier is een voorbeeld van de output:

```

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(): 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
```

De relevante informatie die u in het debug-venster vindt, wordt **vet** gemarkeerd.

Dit zijn de verschillende fases van een webpagina-transactie:

1. HTTP-aanvraag headers ontvangen van client.
2. HTTP-aanvraagheaders verzonden naar server.
3. HTTP-responskoppen ontvangen van server.
4. HTTP-reactiekopers naar client verzonden.

Als de webpagina waar u doorheen bladert meerdere objecten bevat, bestaan er meerdere voorbeelden van deze opeenvolging van gebeurtenissen. Gebruik het eenvoudigst mogelijke verzoek om de debug-uitvoer te beperken.

Op een Catalyst 6500 of een Cisco 7600 router verwerkt een functiemanager alle functies in Cisco IOS om een extra laag probleemoplossing te bieden. Wanneer een Layer 3 optie in deze apparaten is geconfigureerd, wordt informatie die bepaalt hoe de ontvangen frames moeten worden verwerkt doorgegeven aan Layer 2-bedieningsfuncties van de switch of router (de functiebeheerder). Voor WCCP, definieert deze controle informatie welke pakketten door IOS en WCCP worden onderschept en op het transparante cache worden gericht.

De opdracht **show fm** geeft de functies weer die in Cisco IOS zijn ingeschakeld. U kunt deze opdracht gebruiken om te controleren of de poort die u wilt onderscheppen, correct geadverteerd is door de Cache Engine.

```
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

De opdracht **toont fm in vlan 200** geeft de exacte inhoud van het Ternary Content Adresseerbare Geheugen (TCAM) weer.

```
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
```

De `Vmr IP-waarde # 1`: De lijn definieert interceptie bypass op frames die afkomstig zijn van de Cache Engine. Zonder dit zou er een omleiding zijn. De `Vmr IP waarde # 2`: de lijn definieert interceptie van alle pakketten die port 80 als hun bestemming hebben. Als port 80 niet in de tweede lijn wordt weergegeven, maar WCCP is actief en het cache is bruikbaar in de router, dan kan er een probleem zijn in de cache configuratie. Verzamel een vuilnisbelt van het **Hier ben ik** pakketjes om te bepalen of de poort al dan niet wordt verzonden door het cache.

Als u het probleem niet kunt oplossen nadat u problemen hebt opgelost, rapporteer het probleem aan het Cisco [Technical Assistance Center \(TAC\)](#).

Hier is enige basisinformatie die u aan Cisco TAC moet verstrekken. Verzamel deze informatie op de router:

- De output van de **show tech** opdracht. De output van de **show in werking stellen-akker** en de **show versie uitvoer** opdrachten kan worden vervangen als er probleem is met de grootte van

de **show tech** uitvoer.

- De output van de opdracht **tonen ip wcp**.
- De output van de **show ip web-cache** opdracht voor **details**.
- Als er een probleem lijkt te zijn met de communicatie tussen de router en het Web cache, dient u uitvoer van de **debug ip wcp-gebeurtenissen** te leveren en opdrachten voor **IP-pakketten** te **debug** terwijl het probleem zich voordoet.

Op de Cache Engine (alleen Cisco Cache Engine) verzamelt u de uitvoer van de opdracht **show-technologie**.

Voltooi de volgende stappen wanneer u contact opneemt met de TAC:

1. Geef een duidelijke beschrijving van het probleem. U dient antwoorden op deze vragen op te nemen: Wat zijn de symptomen? Komt het de hele tijd of zelden voor? Is het probleem begonnen na een verandering in de configuratie? Zijn Cisco- of derdepartijcaches gebruikt?
2. Geef een duidelijke beschrijving van de topologie. Voeg een diagram toe als dat het duidelijker maakt.
3. Geef alle andere informatie op die u nuttig acht voor het oplossen van het probleem.

Hier wordt een voorbeeldconfiguratie uitgevoerd:

```
***** 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
```

## [Gerelateerde informatie](#)

- [Cisco Cache-software](#)
- [Cisco 500 Series cache-motoren](#)
- [Web Cache Communications Protocol \(WCCP\)](#)
- [Cisco Cache Engine 2.0 Software Download Page](#) (alleen [geregistreerde](#) klanten)
- [Cisco Cache Engine 3.0 Software Download Page](#) (alleen [geregistreerde](#) klanten)
- [Technische ondersteuning en documentatie – Cisco Systems](#)