

WCCP에 대한 역방향 투명 캐싱 문제 해결

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[표기 규칙](#)

[구성](#)

[관련 정보](#)

소개

이 문서에서는 WCCP(Web Cache Communication Protocol)가 역방향 투명 캐싱을 구현하는 데 사용될 때 문제를 해결하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

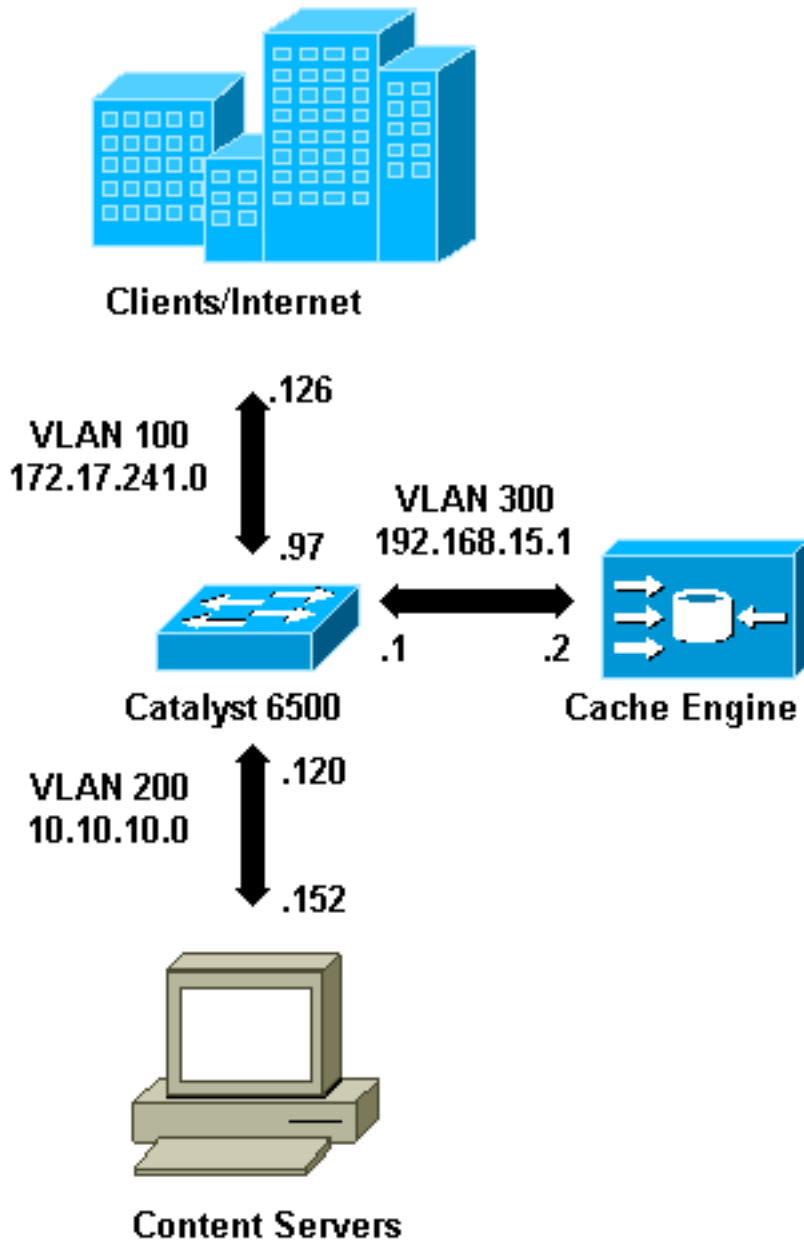
- 기본 모드에서 Supervisor 1 및 MSFC 1이 구성된 Catalyst 6500
- Cisco IOS® 소프트웨어 릴리스 12.1(8a)EX(c6sup11-jsv-mz.121-8a.EX.bin)
- Cache Engine 550(버전 2.51 포함)

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 [Cisco 기술 팁 규칙](#)을 참조하십시오.

구성



캐시 엔진을 설치할 때 WCCP를 구현하는 데 필요한 명령만 구성하는 것이 좋습니다. 나중에 라우터 및 클라이언트 리디렉션 목록에 인증과 같은 다른 기능을 추가할 수 있습니다.

Cache Engine에서 사용할 라우터의 IP 주소와 WCCP 버전을 지정해야 합니다.

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

WCCP의 IP 주소 및 버전이 구성되면 역투명 캐싱을 구현하기 위해 라우터에서 서비스 99를 활성화해야 한다는 경고 메시지가 표시될 수 있습니다. 서비스 99는 역방향 투명 캐싱을 위한 WCCP 서비스 식별자입니다. 일반 투명 캐싱의 식별자는 Cisco IOS의 "web-cache"입니다. 라우터에서 서비스 99(역방향 투명 캐싱)를 활성화하고 리디렉션을 수행할 포트를 지정하려면 글로벌 컨피그레이션 모드에서 다음 명령을 추가합니다.

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

역방향 투명 캐싱을 구성하면 WCCP 서비스 99를 실행하는 라우터가 웹 서버로 보내는 요청을 인터셉트합니다. ip wccp 99 redirect out 명령은 웹 서버에 대한 경로에서 클라이언트 HTTP 패킷을 차단하려는 인터페이스에 적용됩니다. 일반적으로 웹 서버 VLAN입니다. 일반적으로 캐시 엔진이 설치된 VLAN이 아닙니다.

WCCP가 활성화되면 라우터는 WCCP 리디렉션이 구성된 모든 포트에서 수신 대기합니다. Cache Engine은 WCCP를 지속적으로 전송합니다. 여기서는 라우터 목록에 구성된 IP 주소로 패킷을 전송합니다.

라우터와 캐시 간의 WCCP 연결이 구성됩니다. 연결 정보를 보려면 show ip wccp 명령을 실행합니다.

라우터 식별자는 캐시 엔진에서 볼 수 있는 라우터의 IP 주소입니다. 이 식별자는 리디렉션된 트래픽이 캐시에 도달하기 위해 사용하는 라우터 인터페이스가 아닐 수도 있습니다. 이 예에서 라우터 식별자는 192.168.15.1입니다.

```
Router#show ip wccp
Global WCCP information:
  Router information:
    Router Identifier:          192.168.15.1
    Protocol Version:          2.0
  Service Identifier: 99
    Number of Cache Engines:   1
    Number of routers:         1
    Total Packets Redirected:   0
    Redirect access-list:      -none-
    Total Packets Denied Redirect: 0
    Total Packets Unassigned:  0
    Group access-list:         -none-
    Total Messages Denied to Group: 0
    Total Authentication failures: 0
```

show ip wccp 99 detail 명령은 캐시에 대한 자세한 정보를 제공합니다.

```
Router#show ip wccp 99 detail
WCCP Cache-Engine information:
  IP Address:          192.168.15.2
  Protocol Version:    2.0
  State:               Usable
  Redirection:         GRE
  Initial Hash Info:   FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
                      FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
  Assigned Hash Info:  FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
                      FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
  Hash Allotment:      256 (100.00%)
  Packets Redirected:  0
  Connect Time:        00:00:39
```

Redirection 필드는 라우터에서 캐시 엔진으로 패킷을 리디렉션하는 데 사용되는 방법을 나타냅니다. 이 방법은 GRE(Generic Routing Encapsulation) 또는 Layer 2입니다. GRE를 사용하면 패킷이 GRE 패킷에 캡슐화됩니다. 레이어 2를 사용하면 패킷이 캐시로 직접 전송되지만, 레이어 2 리디렉션을 위해 캐시 엔진 및 스위치 또는 라우터가 레이어 2 옆에 있어야 합니다.

Initial Hash Info and Assigned Hash Info 필드에 16진수로 표시되는 Hash Contitch는 이 캐시에 할당된 해시 버킷 수입니다. 가능한 모든 소스 인터넷 주소는 64개의 동일한 크기 범위, 범위당 하나의 버킷으로 구분되며, 각 캐시는 이러한 버킷 소스 주소 범위의 여러 범위에서 트래픽을 할당합니다. 이 양은 캐시의 로드 및 로드 가중치에 따라 WCCP에서 동적으로 관리됩니다. 캐시가 하나만 설치된 경우 이 캐시에 모든 버킷이 할당될 수 있습니다.

라우터가 패킷을 캐시 엔진으로 리디렉션하기 시작하면 Total Packets Redirected 필드의 숫자가 증가합니다.

Total Packets Unassigned 필드는 캐시에 할당되지 않아 리디렉션되지 않은 패킷 수입니다. 이 예에서 패킷 수는 5입니다. 캐시는 초기 검색 중에 또는 캐시가 제거될 때 작은 간격으로 패킷이 할당되지 않을 수 있습니다.

```
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
```

라우터에서 캐시를 가져오지 않으면 WCCP 활동을 디버깅하는 것이 유용할 수 있습니다. 라우터가 Here I am packet from the cache를 받을 때마다, I see you packet과 함께 응답하며, 이는 디버그에 보고됩니다. 사용 가능한 debug 명령은 debug ip wccp 이벤트 및 debug ip wccp 패킷입니다.

참고: debug 명령을 사용하기 전에 디버그 [명령에 대한 중요 정보](#)를 참조하십시오.

이 출력은 일반 WCCP 디버그 메시지의 샘플을 제공합니다.

```
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

```

디버그 레벨을 증가시키기 위해 라우터가 캐시 엔진에서 패킷을 수신하는지 확인하기 위해 IP 패킷 트래픽을 추적할 수 있습니다. 프로덕션 환경에서 라우터를 오버로드하지 않고 흥미로운 트래픽만 표시하려면 ACL을 사용하여 캐시의 IP 주소를 소스로 사용하는 패킷으로만 디버그를 제한할 수 있습니다. 샘플 ACL은 **access-list 130 permit ip host 192.168.15.2 host 192.168.15.1**입니다.

```

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

```

라우터에서 캐시가 보이지 않고 WCCP 활동이 표시되지 않는 경우 기본 연결을 확인합니다. 캐시에서 라우터 또는 라우터에서 캐시를 ping합니다. ping이 작동하는 경우 컨피그레이션에 오류가 있을 수 있습니다.

캐시가 확보되었지만 패킷이 리디렉션되지 않은 경우 라우터가 트래픽을 수신하고 트래픽이 ip wccp 99 redirect out 명령이 적용되는 인터페이스로 전달되는지 확인합니다. 가로채기 및 리디렉션되는 트래픽은 TCP 포트 80으로 전달되는 트래픽입니다.

트래픽이 여전히 리디렉션되지 않고 웹 콘텐츠가 서버에서 바로 오는 경우, 캐시가 가로채기에 대한 명령을 올바르게 전달하는지 확인합니다. 이 작업을 완료하려면 WCCP에 대한 일부 배경 정보가 있어야 합니다.

WCCP는 두 가지 서비스 유형을 인식합니다. 표준 및 동적. 라우터는 표준 서비스를 암시적으로 알고 있습니다. 즉, 라우터가 포트 80을 사용하도록 지시할 필요가 없습니다. 포트 80은 이미 알고 있기 때문입니다. 일반 투명 캐싱(web-cache - standard service 0)은 표준 서비스입니다.

다른 모든 경우(투명 캐싱 포함), 어떤 포트를 가로채할지를 라우터에 알립니다. 이 정보는 **Here I am packet**에 전달됩니다.

패킷 자체를 검사하기 위해 **debug ip packet dump** 명령을 실행할 수 있습니다. 생성된 ACL을 사용하여 캐시 엔진에서 보낸 패킷만 디버깅합니다.

```

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

```

이 명령을 사용하면 전체 RFC(Request For Comments)를 볼 필요 없이 포트가 광고되는지 여부를

결정할 수 있습니다. 포트가 알려지지 않은 경우 캐시 구성에서 문제가 발생할 가능성이 높습니다.

자세한 내용은 [Web Cache Coordination Protocol V2.0](#) 을 참조하십시오.

캐시가 획득되고 패킷이 리디렉션되지만 인터넷 클라이언트가 서버를 검색할 수 없는 경우, 캐시가 인터넷과 서버에 연결되었는지 확인합니다. 캐시에서 인터넷의 다양한 IP 주소와 일부 내부 서버로 ping합니다. IP 주소 대신 정규화된 도메인(URL)을 ping하는 경우 캐시 컨피그레이션에서 사용할 DNS 서버를 지정해야 합니다.

캐시가 요청을 처리할지 확실하지 않은 경우 캐시에서 HTTP 활동을 디버깅할 수 있습니다. 캐시에서 HTTP 활동을 디버깅하려면 캐시를 오버로드하지 않도록 트래픽을 제한해야 합니다. 라우터에서 테스트용 디바이스로 사용할 수 있는 한 클라이언트의 소스 IP 주소로 ACL을 만들고 ip wccp 99 전역 명령 **redirect-list** 옵션을 사용합니다.

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

ACL을 생성하고 적용하면 다음 단계를 완료합니다.

1. **debug http all**(Cisco Cache Engine 버전 2.x) 또는 **debug http all**(Cisco Cache Engine 버전 3 및 ACNS 버전 4, 5) 명령을 사용하여 캐시에서 HTTP 디버깅을 활성화합니다.
2. 터미널 모니터링을 활성화합니다(**term mon** 명령 실행).
3. ACL에서 구성한 클라이언트에서 서버 중 하나를 찾아봅니다.

다음은 출력의 예입니다.

```
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
```

디버그에서 찾을 수 있는 관련 정보는 굵게 강조 표시됩니다.

다음은 웹 페이지 트랜잭션의 여러 단계입니다.

1. 클라이언트에서 받은 HTTP 요청 헤더입니다.
2. 서버로 전송된 HTTP 요청 헤더입니다.
3. 서버에서 받은 HTTP 응답 헤더
4. 클라이언트로 전송된 HTTP 응답 헤더.

탐색하는 웹 페이지에 여러 객체가 포함된 경우 이 이벤트 시퀀스의 여러 인스턴스가 존재합니다.
.디버그 출력을 줄이려면 가장 간단한 요청을 사용합니다.

Catalyst 6500 또는 Cisco 7600 라우터에서 기능 관리자는 추가적인 문제 해결 계층을 제공하기 위해 Cisco IOS에 구성된 모든 기능을 처리합니다. 이러한 디바이스에서 레이어 3 기능이 구성되면 수신된 프레임 처리하는 방법을 정의하는 정보가 스위치나 라우터의 레이어 2 제어 기능(기능 관리자)에 전달됩니다. WCCP의 경우 이 제어 정보는 IOS 및 WCCP에서 가로채고 투명 캐시로 전달되는 패킷을 정의합니다.

show fm features 명령은 Cisco IOS에서 활성화된 기능을 표시합니다. 이 명령을 사용하여 가로채려는 포트가 캐시 엔진에서 올바르게 광고되었는지 확인할 수 있습니다.

```
Router#show fm features
Redundancy Status: stand-alone
Interface: Vlan200 IP is enabled
  hw[EGRESS] = 1, hw[INGRESS] = 1
  hw_force_default[EGRESS] = 0, hw_force_default[INGRESS] = 0
  mcast = 0
  priority = 2
  reflexive = 0
  vacc_map :
  outbound label: 5
    merge_err: 0
    protocol: ip
      feature #: 1
      feature id: FM_IP_WCCP
      Service ID: 99
      Service Type: 1
```

The following are the used labels

```
label 5:
  swidb: Vlan200
  Vlous:
```

The following are the features configured

```
IP WCCP: service_id = 99, service_type = 1, state = ACTIVE
outbound users:
  user_idb: Vlan200
WC list:
  address: 192.168.15.2
Service ports:
  ports[0]: 80
```

The following is the ip ACLs port expansion information

```
FM_EXP knob configured: yes
```

FM mode for WCCP: GRE (flowmask: destination-only)

FM redirect index base: 0x7E00

The following are internal statistics

```
Number of pending tcam inserts: 0
Number of merge queue elements: 0
```

show fm int vlan 200 명령은 TCAM(Ternary Content Addressable Memory)의 정확한 내용을 표시합니다.

```
Router#show fm int vlan 200
Interface: Vlan200 IP is enabled
```

```

hw[EGRESS] = 1, hw[INGRESS] = 1
hw_force_default[EGRESS] = 0, hw_force_default[INGRESS] = 0
mcast = 0
priority = 2
reflexive = 0
vacc_map :
outbound label: 5
merge_err: 0
protocol: ip
feature #: 1
feature id: FM_IP_WCCP
Service ID: 99
Service Type: 1
(only for IP_PROT) DestAddr SrcAddr          Dpt   Spt   L4OP TOS Est  prot  Rslt
vmr IP value #1:   0.0.0.0 192.168.15.2      0     0     0   0   0    6    permit
vmr IP mask #1:   0.0.0.0 255.255.255.255  0     0     0   0   0    FF
vmr IP value #2:   0.0.0.0 0.0.0.0           80    0     0   0   0    6    bridge
vmr IP mask #2:   0.0.0.0 0.0.0.0           FFFF  0     0   0   0    FF
vmr IP value #3:   0.0.0.0 0.0.0.0           0     0     0   0   0    0    permit
vmr IP mask #3:   0.0.0.0 0.0.0.0           0     0     0   0   0    0

```

vmr IP # 1:선은 캐시 엔진에서 오는 프레임에 대한 가로채기 우회를 정의합니다.이렇게 하지 않으면 리디렉션 루프가 있습니다.vmr IP # 2:선은 포트 80을 대상으로 하는 모든 패킷의 가로채기를 정의합니다.포트 80이 두 번째 줄에 표시되지 않지만 WCCP가 활성 상태이고 라우터에서 캐시를 사용할 수 있는 경우 캐시 구성에 문제가 있을 수 있습니다.Here I am(여기는 패킷)의 덤프를 수집하여 포트가 캐시에 의해 전송되는지 여부를 확인합니다.

트러블슈팅 후 문제를 해결할 수 없는 경우 Cisco [TAC\(Technical Assistance Center\)](#)에 문제를 [보고하십시오](#).

다음은 Cisco TAC에 제공해야 하는 몇 가지 기본 정보입니다.라우터에서 다음 정보를 수집합니다.

- **show tech** 명령의 출력입니다.show running-config 및 **show version** 출력 명령의 출력은 **show tech** 출력 크기에 문제가 있는 경우 대신 사용할 수 있습니다.
- show ip wccp 명령의 **출력**입니다.
- **show ip wccp web-cache detail** 명령의 출력입니다.
- 라우터와 웹 캐시 간의 통신에 문제가 있는 경우 **debug ip wccp 이벤트**의 출력을 제공하고 문제가 발생하는 동안 **debug ip wccp packets** 명령을 제공합니다.

Cache Engine(Cisco Cache Engines만 해당)에서 **show tech** 명령의 출력을 수집합니다.

TAC에 문의하면 다음 단계를 완료하십시오.

1. 문제에 대한 명확한 설명을 제공합니다.다음 질문에 대한 답변을 포함해야 합니다.어떤 증상이 있나요?항상 발생합니까, 아니면 드물게 발생합니까?컨피그레이션이 변경된 후 문제가 시작되었습니까?Cisco 또는 타사 캐시가 사용됩니까?
2. 토폴로지에 대한 명확한 설명을 제공합니다.다이어그램을 더 명확하게 하려면 다이어그램을 포함하십시오.
3. 문제를 해결하는 데 유용하다고 생각하는 다른 정보를 제공하십시오.

다음은 샘플 컨피그레이션의 출력입니다.

```

***** 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
```

관련 정보

- [Cisco 캐시 소프트웨어](#)
- [Cisco 500 Series 캐시 엔진](#)
- [WCCP\(Web Cache Communications Protocol\)](#)
- [Cisco Cache Engine 2.0 소프트웨어 다운로드 페이지\(등록된 고객만 해당\)](#)
- [Cisco Cache Engine 3.0 소프트웨어 다운로드 페이지\(등록된 고객만 해당\)](#)
- [기술 지원 및 문서 - Cisco Systems](#)