

# Résolution des problèmes de mise en cache transparente inversée pour WCCP

## Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Conventions](#)

[Configuration](#)

[Informations connexes](#)

## [Introduction](#)

Ce document explique comment effectuer le dépannage pour le Web Cache Communication Protocol (WCCP) lorsqu'il est utilisé afin d'intégrer la mise en cache transparente inversée.

## [Conditions préalables](#)

### [Conditions requises](#)

Aucune spécification déterminée n'est requise pour ce document.

### [Composants utilisés](#)

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

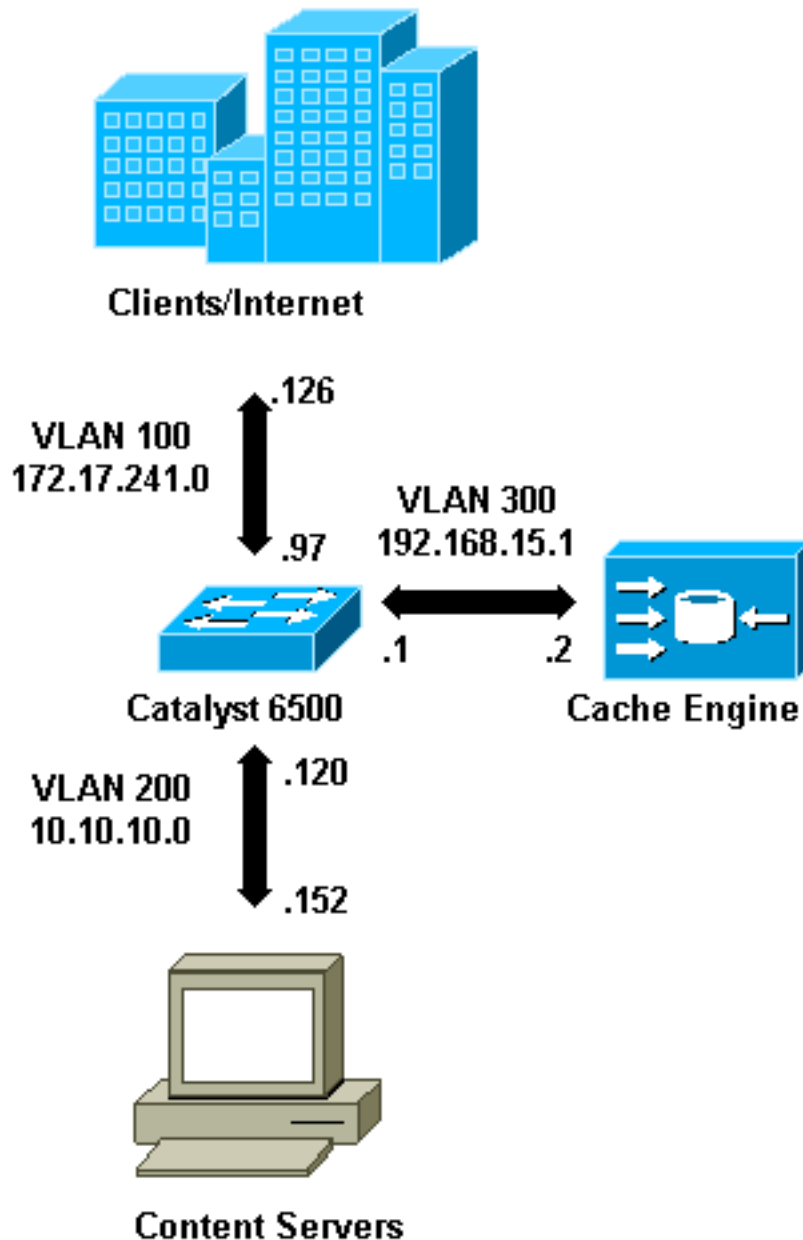
- Catalyst 6500 avec le superviseur 1 et MSFC 1 configuré dans le mode natif
- Version de logiciel 12.1(8a)EX de Cisco IOS® (c6sup11-jsv-mz.121-8a.EX.bin)
- Moteur de cache 550 avec la version 2.51

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

### [Conventions](#)

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à [Conventions relatives aux conseils techniques Cisco](#).

## Configuration



Quand vous installez un moteur de cache, Cisco recommande que vous configuriez seulement les commandes nécessaires pour implémenter le WCCP. Vous pouvez ajouter d'autres caractéristiques, telles que l'authentification au routeur et aux listes de redirection de clients, à une date ultérieure.

Sur le moteur de cache, vous devez spécifier l'adresse IP du routeur et la version du WCCP que vous voulez utiliser.

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

Une fois que l'adresse IP et la version du WCCP sont configurées, vous pourriez voir qu'un message qui avertit le service 99 devrait être lancé dans le routeur afin d'implémenter la mise en cache transparente inverse. Le service 99 est l'identifiant de service WCCP pour la mise en



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

Le champ de `redirection` représente la méthode utilisée pour réorienter les paquets du routeur au moteur de cache. Cette méthode est Encapsulation de routage générique (GRE) ou couche 2. Avec GRE, des paquets sont encapsulés dans un paquet GRE. Avec la couche 2, des paquets sont envoyés directement dans le cache, mais le moteur de cache et le commutateur ou le routeur doivent être la couche 2 adjacente pour la redirection de la couche 2.

L'attribution d'informations parasites représentée dans l'hexadécimal dans les informations initiales d'informations parasites et les zones d'informations assignées d'informations parasites est le nombre de positions d'informations parasites qui sont assignées dans ce cache. Toutes les adresses Internet possibles de source sont divisées en 64 plages de taille égales, une position par plage, et chaque cache est assigné au trafic de l'un certain nombre ces derniers des plages d'adresse source de position. Cette quantité est gérée dynamiquement par WCCP selon le chargement et le coefficient de chargement du cache. Si vous faites installer seulement un cache, ce cache pourrait être assigné toutes les positions.

Quand les débits de routeur pour réorienter des paquets au moteur de cache, le nombre dans tous les paquets réorientés mettent en place des augmentations.

Le gisement non affecté de paquets totaux est le nombre de paquets qui n'ont pas été réorientés parce qu'ils n'ont été assignés dans aucun cache. Dans cet exemple, le nombre de paquets est 5. paquets pourrait être non affecté pendant la découverte initiale des caches ou pour un petit intervalle quand un cache est retiré.

```
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 le cache n'obtient pas saisi par le routeur, il pourrait être utile de mettre au point l'activité WCCP. Toutes les fois que le routeur me reçoit ici suis le paquet du cache, il répond avec je vous voient paquet, et ceci est signalé dans met au point. Les commandes de débogage disponibles sont `debug ip wccp events` et mettent au point des paquets d'ip wccp.

**Remarque:** Référez-vous aux [informations importantes sur les commandes de débogage](#) avant d'utiliser les commandes de débogage.

Cette sortie fournit un échantillon de messages de débogage normaux 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

```

Afin d'augmenter le niveau de débogage, vous pourriez vouloir tracer le trafic de paquet IP afin de vérifier si le routeur reçoit des paquets du moteur de cache. Afin d'éviter de surcharger un routeur dans un environnement de production et afin d'afficher seulement le trafic intéressant, vous pouvez employer un ACL pour limiter met au point seulement aux paquets qui ont l'adresse IP du cache comme source. Un ACL d'échantillon est hôte 192.168.15.1 de 192.168.15.2 d'hôte d'IP d'autorisation de la liste d'accès 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

```

Au cas où aucun cache ne serait vu par le routeur et aucune activité WCCP n'est vue, vérifiez la Connectivité de base. Essayez de cingler le cache du routeur ou du routeur du cache. Si le ping fonctionne, une erreur pourrait exister dans la configuration.

Si le cache est saisi, mais aucun paquet n'est réorienté, vérifiez que le routeur reçoit le trafic et que le trafic est expédié à l'interface où l'**ip wccp 99 réorientent** commande est appliqué. Souvenez-vous que le trafic qui est intercepté et réorienté est seulement le trafic dirigé vers le port TCP 80.

Si le trafic n'est toujours pas en cours de réorientation et le contenu Web est livré directement des serveurs, vérifiez que le cache passe correctement l'instruction sur quoi intercepter. Vous devez avoir une certaine information générale sur le WCCP afin de se terminer cette action.

Le WCCP identifie deux types de services différents : *standard* et *dynamique*. Le routeur sait implicitement d'un service standard. C'est-à-dire, le routeur n'a pas besoin d'être dit pour utiliser le port 80, parce qu'il sait déjà pour faire ainsi. La mise en cache transparente normale (Web-cache - service standard 0) est un service standard.

Dans tous les autres cas (qui inclut la mise en cache transparente), le routeur est dit quel port à intercepter. Ces informations sont passées dans **ici je suis** paquet.

Vous pouvez émettre la commande de **vidage mémoire de debug ip packet** afin d'examiner les paquets eux-mêmes. Utilisez l'ACL créé pour mettre au point seulement les paquets envoyés en le moteur de cache.

```

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

```

Avec cette commande, vous pouvez déterminer si le port est annoncé sans nécessité de visualiser le Request For Comments entier (RFC). Si le port n'est pas annoncé, le problème est le plus susceptible dans la configuration du cache.

Référez-vous au pour en savoir plus de [Protocol V2.0 de coordination de cache](#) de Web.

Si le cache est saisi et des paquets sont réorientés, mais vos clients d'Internet ne peuvent pas parcourir vos serveurs, vérifiez si le cache a la Connectivité à l'Internet et à vos serveurs. Cinglez du cache à de diverses adresses IP sur l'Internet et à certains de vos serveurs internes. Si vous cinglez entièrement - les domaines qualifiés (URLs) au lieu des adresses IP, soient sûrs que vous spécifiez le serveur DNS pour utiliser dans la configuration de cache.

Si vous êtes incertain si le cache traite les demandes, vous pouvez mettre au point l'activité de HTTP dans le cache. Afin de mettre au point l'activité de HTTP dans le cache, vous devez limiter le trafic pour éviter de surcharger le cache. Sur le routeur, créez un ACL avec l'adresse IP source d'un client en Internet que vous pouvez utiliser comme périphérique pour vos tests et utilisez la réorienter-liste d'option de l'ip wccp 99 de commande globale.

```

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

```

Une fois que vous créez et appliquez l'ACL, terminez-vous ces étapes :

1. Lancez le HTTP mettent au point dans le cache avec la commande **mettent au point le HTTP tout le tout** (version 2.x de moteur de cache de Cisco) ou **mettent au point le HTTP tout** (version 3 de moteur de cache de Cisco et version 4 ACNS, 5).
2. Lancez la surveillance terminale (émettez la commande de **lundi de terme**).
3. Essayez de parcourir un de vos serveurs du client que vous avez configuré dans l'ACL.

Voici un exemple de la sortie :

```

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
```

Les informations pertinentes que vous pourriez trouver dans le débogage sont mises en valeur en gras.



Ce sont les différentes phases d'une transaction de page de page Web :

1. En-têtes de demande de HTTP reçues du client.
2. En-têtes de demande de HTTP envoyées au serveur.
3. En-têtes de réponse de HTTP reçues du serveur.
4. En-têtes de réponse de HTTP envoyées au client.

Si la page Web que vous parcourez contient de plusieurs objets, des multiples instances de cette séquence d'opérations existent. Utilisez la demande la plus simple possible de réduire la sortie de débogage.

Sur un Catalyst 6500 ou un routeur de Cisco 7600, un gestionnaire de caractéristique manipule toutes les caractéristiques configurées dans le Cisco IOS afin de fournir une couche ajoutée de dépannage. Quand une caractéristique de la couche 3 est configurée dans des ces périphériques, les informations qui définissent comment ont traité les trames reçues sont passées aux fonctions de contrôle de la couche 2 du commutateur ou du routeur (le gestionnaire de caractéristique). Pour le WCCP, cette information de contrôle définit quels paquets sont interceptés par l'IOS et le WCCP et dirigés dans le cache transparent.

La commande de **show fm features** affiche les caractéristiques qui sont activées dans le Cisco IOS. Vous pouvez employer cette commande afin de vérifier si le port intercepter est correctement annoncé en le moteur de cache.

```
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

**Le VLAN 200 du show fm international de commande affiche le contenu précis de la mémoire associative ternaire (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	

La valeur IP de vmr # 1 : la ligne définit le contournement d'interception sur les trames qui proviennent le moteur de cache. Sans ceci, il y aurait une boucle de redirection. La valeur IP de vmr # 2 : la ligne définit l'interception de tous les paquets qui ont le port 80 en tant que leur destination. Si le port 80 n'est pas affiché dans la deuxième ligne, mais le WCCP est en activité et le cache est utilisable par le routeur, alors il pourrait y a un problème dans la configuration de cache. Collectez un vidage mémoire de **ici je suis** paquet afin de déterminer si le port est envoyé par le cache.

Si vous ne pouvez pas résoudre le problème après que vous dépannez, signalez le problème au [centre d'assistance technique Cisco \(TAC\)](#).

Voici quelques informations de base que vous devez fournir à Cisco TAC. Du routeur, collectez ces informations :

- La sortie de la commande de **tech d'exposition**. La sortie des commandes de **sortie de show running-config** et de **show version** peut être substituée s'il y a difficulté avec la taille de la sortie de **tech d'exposition**.
- La sortie de la commande de **show ip wccp**.
- La sortie de la commande de **détail de Web-cache de show ip wccp**.
- S'il semble y a un problème avec la transmission entre le routeur et le cache de Web, fournissez la sortie du **debug ip wccp events** et **mettez au point les commandes de paquets d'ip wccp** tandis que le problème se pose.

Sur le moteur de cache (moteurs de cache de Cisco seulement), collectez la sortie de la commande de **tech d'exposition**.

Quand vous entrez en contact avec le TAC, terminez-vous ces étapes :

1. Fournissez une description claire du problème. Vous devriez inclure des réponses à ces questions :Quels sont les symptômes ?Se produit-il tout le temps ou rarement ?A-t-il fait le début de problème après un changement de la configuration ?Cisco ou des caches de tiers sont-ils utilisés ?
2. Fournissez une description claire de la topologie. Incluez un diagramme si cela expliquera.
3. Fournissez n'importe quelles autres informations que vous pensez est utile en résolvant le problème.

Voici la sortie d'une configuration d'échantillon :

```
***** 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

```

## [Informations connexes](#)

- [Logiciel de cache Cisco](#)
- [Cache Engines de la gamme Cisco 500](#)
- [Protocole WCCP \(Web Cache Communications Protocol\)](#)
- [Page de téléchargement du logiciel du moteur de cache 2.0 de Cisco \(clients enregistrés seulement\)](#)
- [Page de téléchargement du logiciel du moteur de cache 3.0 de Cisco \(clients enregistrés seulement\)](#)
- [Support et documentation techniques - Cisco Systems](#)