Risoluzione dei problemi di Reverse Transparent Caching per WCCP

Sommario

Introduzione

In questo documento viene descritto come risolvere i problemi relativi al protocollo WCCP (Web Cache Communication Protocol) quando viene utilizzato per implementare la memorizzazione nella cache inversa trasparente.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

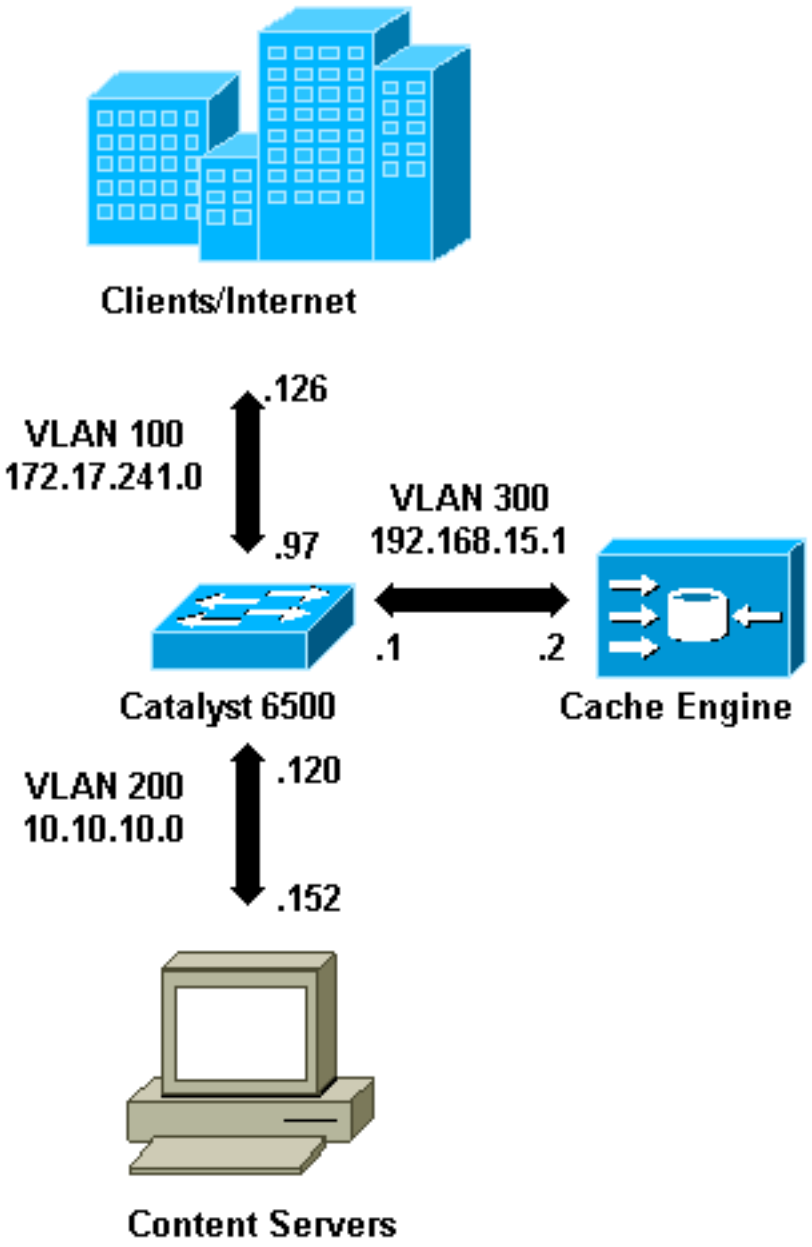
- Catalyst 6500 con Supervisor 1 e MSFC 1 configurato in modalità nativa
- Software Cisco IOS® versione 12.1(8a)EX (c6sup11-jsv-mz.121-8a.EX.bin)
- Cache Engine 550 con versione 2.51

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Configurazione



Quando si installa un Cache Engine, Cisco consiglia di configurare solo i comandi necessari per implementare WCCP. In un secondo momento, è possibile aggiungere altre funzionalità, ad esempio l'autenticazione agli elenchi di reindirizzamento dei router e dei client.

Sul Cache Engine, è necessario specificare l'indirizzo IP del router e la versione di WCCP da usare.

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

Dopo aver configurato l'indirizzo IP e la versione di WCCP, è possibile che venga visualizzato un messaggio in cui si avvisa che il servizio 99 deve essere attivato sul router per implementare la

memorizzazione nella cache inversa e trasparente. Service 99 è l'identificatore del servizio WCCP per la memorizzazione nella cache inversa e trasparente. L'identificatore della normale cache trasparente è la parola "web-cache" in Cisco IOS. Per attivare il servizio 99 (reverse transparent caching) sul router e specificare la porta su cui verrà eseguito il reindirizzamento, aggiungere questi comandi in modalità di configurazione globale:

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

Quando si configura la cache inversa trasparente, il router che esegue il servizio WCCP 99 intercetta le richieste dirette ai server Web. il comando **ip wccp 99 redirect out** viene applicato all'interfaccia in cui si desidera intercettare i pacchetti HTTP client nel percorso verso il server Web. In genere, si tratta della VLAN del server Web. In genere non si tratta della VLAN su cui è installato il motore di cache.

Quando WCCP è attivo, il router rimane in ascolto su tutte le porte per cui è stato configurato il reindirizzamento WCCP. Per segnalare la sua presenza, il Cache Engine invia continuamente i pacchetti WCCP **Here I am** agli indirizzi IP configurati nell'elenco dei router.

Èstata creata una connessione WCCP tra il router e la cache. Per visualizzare le informazioni sulla connessione, usare il comando **show ip wccp**.

L'identificativo del router è l'indirizzo IP del router così come viene visualizzato dai motori della cache. Questo identificatore non è necessariamente l'interfaccia del router utilizzata dal traffico reindirizzato per raggiungere la cache. L'identificatore del router nell'esempio è 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
```

Il comando **show ip wccp 99 detail** fornisce informazioni dettagliate sulle cache.

```
Router#show ip wccp 99 detail
   WCCP Cache-Engine information:
           IP Address:               192.168.15.2
           Protocol Version:         2.0
           State:                    Usable
```

```
        Redirection:             GRE
        Initial Hash Info:       FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
                                 FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
        Assigned Hash Info:      FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
                                 FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
        Hash Allotment:          256 (100.00%)
        Packets Redirected:      0
        Connect Time:            00:00:39
```

Il campo `Redirection` rappresenta il metodo utilizzato per reindirizzare i pacchetti dal router al motore di cache. Questo metodo è GRE (Generic Routing Encapsulation) o layer 2. Con il GRE, i pacchetti sono incapsulati in un pacchetto GRE. Con il layer 2, i pacchetti vengono inviati direttamente alla cache, ma il motore di cache e lo switch o router devono essere adiacenti al layer 2 per il reindirizzamento al layer 2.

L'`assegnazione hash` rappresentata in formato esadecimale nei campi `Initial Hash Info` e `Assigned Hash Info` è il numero di bucket di hash assegnati a questa cache. Tutti i possibili indirizzi Internet di origine sono divisi in 64 intervalli di dimensioni uguali, un bucket per intervallo, e a ogni cache viene assegnato il traffico proveniente da un certo numero di questi intervalli di indirizzi di origine bucket. Questo importo viene gestito dinamicamente da WCCP in base al carico e alla ponderazione del carico della cache. Se è installata una sola cache, questa potrebbe essere assegnata a tutti i bucket.

Quando il router inizia a reindirizzare i pacchetti al motore di cache, il numero nel campo `Totale pacchetti reindirizzati` aumenta.

Il campo `Totale pacchetti non assegnati` indica il numero di pacchetti che non sono stati reindirizzati perché non assegnati ad alcuna cache. In questo esempio, il numero di pacchetti è 5. È possibile che l'assegnazione dei pacchetti venga annullata durante il rilevamento iniziale delle cache o per un breve intervallo quando si rimuove una cache.

```
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
```

se la cache non viene acquisita dal router, potrebbe essere utile eseguire il debug dell'attività WCCP. Ogni volta che il router riceve un pacchetto **Here I am** dalla cache, risponde con un pacchetto **I see you**, e questo viene segnalato nei debug. I comandi **debug** disponibili sono **debug ip wccp events** e **debug ip wccp packets**.

Nota: consultare le informazioni importanti sui comandi di debug prima di usare i comandi di **debug**.

In questo output viene fornito un esempio di messaggi di debug WCCP normali:

```
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
```

Per aumentare il livello di debug, si potrebbe desiderare di tracciare il traffico dei pacchetti IP per controllare se il router riceve pacchetti dal motore di cache. Per evitare di sovraccaricare un router in un ambiente di produzione e mostrare solo il traffico interessante, è possibile usare un ACL per limitare i debug solo ai pacchetti con indirizzo IP della cache come origine. Un ACL di esempio è access-list 130 allow 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
```

Se il router non rileva alcuna cache e non rileva alcuna attività WCCP, verificare la connettività di base. Provare a eseguire il ping della cache dal router o dal router dalla cache. Se il ping funziona, è possibile che esista un errore nella configurazione.

Se la cache viene acquisita ma non vengono reindirizzati pacchetti, verificare che il router riceva il traffico e che il traffico venga inoltrato all'interfaccia a cui viene applicato il comando **ip wccp 99 redirect out**. Tenere presente che il traffico intercettato e reindirizzato riguarda solo il traffico diretto alla porta TCP 80.

Se il traffico non viene ancora reindirizzato e il contenuto Web proviene direttamente dai server, verificare che la cache passi correttamente le istruzioni su cosa intercettare. Per completare l'azione, è necessario disporre di alcune informazioni di base su WCCP.

WCCP riconosce due diversi tipi di servizi: *standard* e *dinamico*. Il router riconosce implicitamente un servizio standard. In altre parole, non è necessario che il router utilizzi la porta 80, perché è già in grado di farlo. La normale memorizzazione nella cache trasparente (web-cache - servizio standard 0) è un servizio standard.

In tutti gli altri casi (incluso il caching trasparente), al router viene detto quale porta intercettare. Queste informazioni vengono passate nel pacchetto **Eccomi**.

Èpossibile usare il comando **debug ip packet dump** per esaminare i pacchetti stessi. Usare l'ACL creato per eseguire il debug solo dei pacchetti inviati dal motore di 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
```

Con questo comando è possibile determinare se la porta viene annunciata o meno senza che sia necessario visualizzare l'intero RFC (Request For Comments). Se la porta non viene annunciata, è probabile che il problema si verifichi nella configurazione della cache.

per ulteriori informazioni, fare riferimento a Web Cache Coordination Protocol V2.0 .

Se la cache viene acquisita e i pacchetti vengono reindirizzati, ma i client Internet non sono in grado di esplorare i server, verificare se la cache è connessa a Internet e ai server. Ping dalla cache a vari indirizzi IP su Internet e ad alcuni server interni. Se si esegue il ping dei domini completi (URL) anziché degli indirizzi IP, verificare di aver specificato il server DNS da utilizzare nella configurazione della cache.

Se non si è certi che la cache elabori le richieste, è possibile eseguire il debug dell'attività HTTP nella cache. Per eseguire il debug dell'attività HTTP nella cache, è necessario limitare il traffico per evitare l'overload della cache. Sul router, creare un ACL con l'indirizzo IP di origine di un client in Internet che possa essere usato come dispositivo per i test e usare l'opzione **redirect-list** del comando globale **ip wccp 99**.

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

Dopo aver creato e applicato l'ACL, procedere come segue:

1. Attivare il debug HTTP nella cache con il comando **debug http all** (Cisco Cache Engine versione 2.x) o **debug http all** (Cisco Cache Engine versione 3 e ACNS versione 4, 5).
2. Attivare il monitoraggio del terminale (usare il comando **mon**).
3. Provare a sfogliare uno dei server dal client configurato nell'ACL.

Di seguito è riportato un esempio dell'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_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
```

Le informazioni pertinenti che possono essere trovate nel comando debug sono evidenziate in **grassetto**.

Di seguito sono riportate le diverse fasi della transazione di una pagina Web:

1. Intestazioni di richiesta HTTP ricevute dal client.
2. Intestazioni di richiesta HTTP inviate al server.
3. Intestazioni di risposta HTTP ricevute dal server.
4. Intestazioni di risposta HTTP inviate al client.

Se la pagina Web visualizzata contiene più oggetti, esistono più istanze di questa sequenza di eventi. Utilizzare la richiesta più semplice possibile per ridurre l'output del comando debug.

Su un router Catalyst 6500 o Cisco 7600, un Feature Manager gestisce tutte le funzionalità configurate in Cisco IOS in modo da fornire un ulteriore livello di risoluzione dei problemi. Quando si configura una funzione di layer 3 in questi dispositivi, le informazioni che definiscono come gestire i frame ricevuti vengono passate alle funzioni di controllo di layer 2 dello switch o del router (il gestore delle funzionalità). Per WCCP, queste informazioni di controllo definiscono quali pacchetti vengono intercettati da IOS e WCCP e diretti alla cache trasparente.

Il comando **show fm features** consente di visualizzare le funzionalità abilitate in Cisco IOS. È possibile utilizzare questo comando per verificare se la porta da intercettare è annunciata correttamente dal motore di 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
```

Il comando **show fm int vlan 200** visualizza l'esatto contenuto della TCAM (Ternary Content Addressable Memory).

```
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
```

Il `valore IP 1 del vmr:` definisce il bypass intercettazione sui frame provenienti dal motore cache. Senza questo, ci sarebbe un loop di reindirizzamento. Il `valore IP #2 del vmr:` Questa riga definisce l'intercettazione di tutti i pacchetti la cui destinazione è la porta 80. Se la porta 80 non viene visualizzata nella seconda riga, ma WCCP è attivo e la cache è utilizzabile dal router, potrebbe essersi verificato un problema nella configurazione della cache. Raccogliere un dump del pacchetto **Here I am** per determinare se la porta viene inviata o meno dalla cache.

Se non è possibile risolvere il problema dopo aver risolto il problema, segnalarlo al Cisco Technical Assistance Center (TAC).

Di seguito sono riportate alcune informazioni di base da fornire a Cisco TAC. Dal router, raccogliere queste informazioni:

- L'output del comando **show tech**. L'output dei comandi **show running-config** e **show version** può essere sostituito in caso di problemi con le dimensioni dell'output **show tech**.
- L'output del comando **show ip wccp**.
- L'output del comando **show ip wccp web-cache detail**.
- Se sembra esserci un problema di comunicazione tra il router e la Web cache, fornire l'output degli **eventi debug ip wccp** e dei comandi **debug ip wccp packets** mentre il problema si verifica.

Sul Cache Engine (solo Cisco Cache Engine), catturare l'output del comando **show tech**.

Quando si contatta il centro TAC, procedere come segue:

1. Fornire una descrizione chiara del problema. Devi includere le risposte alle seguenti domande:Quali sono i sintomi?Si verifica sempre o raramente?Il problema si è verificato dopo una modifica della configurazione?Vengono utilizzate cache Cisco o di terze parti?
2. Fornire una descrizione chiara della topologia. Includere un diagramma se questo lo rende più chiaro.
3. Fornire qualsiasi altra informazione ritenuta utile per la risoluzione del problema.

Di seguito viene riportato un esempio di configurazione.

```
********************************** 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
```

Informazioni correlate

- Software Cisco Cache
- Cisco serie 500 Cache Engine
- Protocollo WCCP (Web Cache Communication Protocol)
- Pagina di download del software Cisco Cache Engine 2.0 (solo utenti registrati)
- Pagina di download del software Cisco Cache Engine 3.0 (solo utenti registrati)
- Documentazione e supporto tecnico – Cisco Systems