Fehlerbehebung Reverse Transparent Caching für WCCP

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie Sie eine Fehlerbehebung für das Web Cache Communication Protocol (WCCP) durchführen, wenn dieses zum Implementieren der umgekehrten transparenten Zwischenspeicherung verwendet wird.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

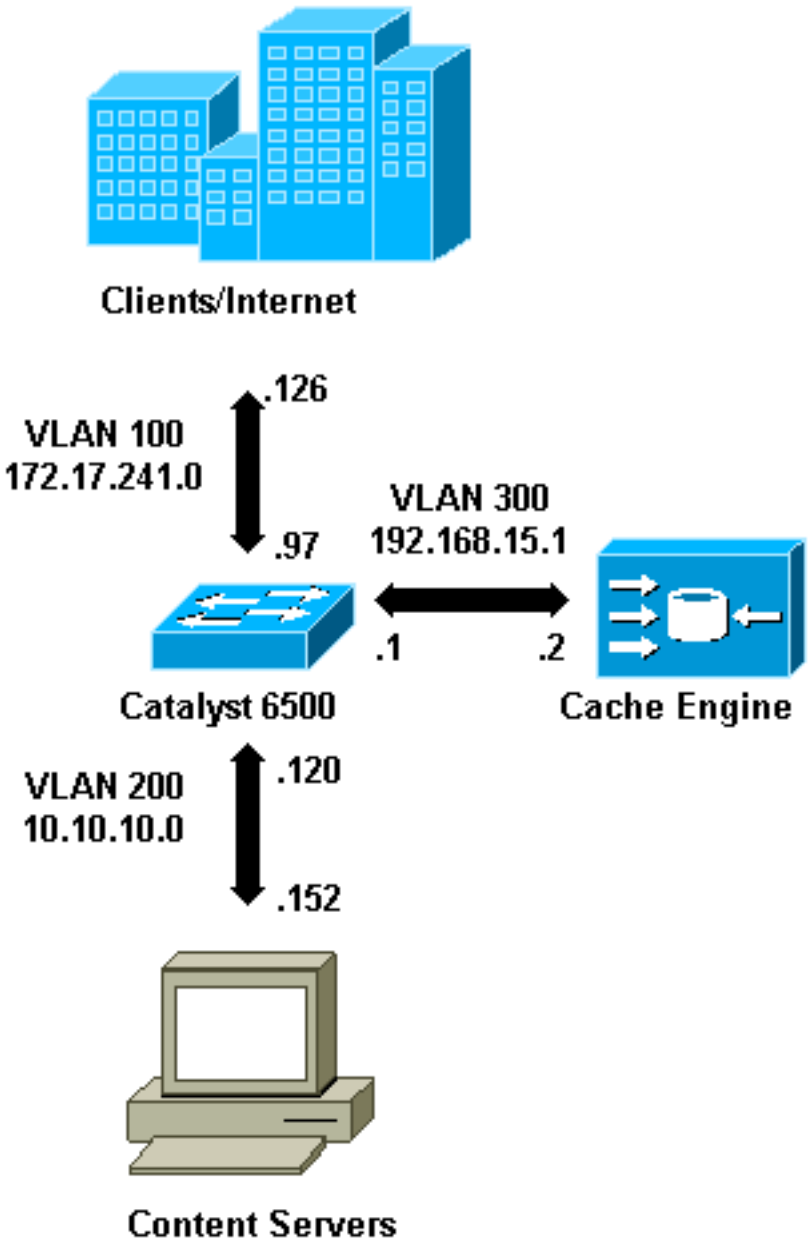
- Catalyst 6500 mit Supervisor 1 und MSFC 1 konfiguriert im nativen Modus
- Cisco IOS® Softwareversion 12.1(8a)EX (c6sup11-jsv-mz.121-8a.EX.bin)
- Cache Engine 550 mit Version 2.51

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps von Cisco zu Konventionen).

Konfiguration



Wenn Sie eine Cache Engine installieren, empfiehlt Cisco, nur die Befehle zu konfigurieren, die für die Implementierung von WCCP erforderlich sind. Sie können zu einem späteren Zeitpunkt weitere Funktionen wie Authentifizierung zum Router und Umleitungslisten für Clients hinzufügen.

Auf der Cache Engine müssen Sie die IP-Adresse des Routers und die Version von WCCP angeben, die Sie verwenden möchten.

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

Wenn die IP-Adresse und die Version von WCCP konfiguriert sind, wird möglicherweise eine Meldung angezeigt, die Sie darauf hinweist, dass der Dienst 99 im Router aktiviert werden sollte,

um eine umgekehrte transparente Zwischenspeicherung zu implementieren. Service 99 ist die WCCP-Dienstkennung für umgekehrtes transparentes Caching. Der Bezeichner für normale transparente Zwischenspeicherung ist das Wort "Web-Cache" im Cisco IOS. Um Service 99 (Reverse Transparent Caching) auf dem Router zu aktivieren und um den Port anzugeben, an dem die Umleitung ausgeführt wird, fügen Sie diese Befehle im globalen Konfigurationsmodus hinzu:

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

Wenn Sie die umgekehrte transparente Zwischenspeicherung konfigurieren, fängt der Router, der den WCCP-Dienst 99 ausführt, Anfragen an, die an die Webserver gerichtet sind. Der Befehl **ip wccp 99 redirect out** wird auf die Schnittstelle angewendet, auf der Sie die HTTP-Clientpakete in ihrem Pfad zum Webserver abfangen möchten. In der Regel ist dies das Webserver-VLAN. Dies ist normalerweise nicht das VLAN, in dem die Cache-Engine installiert ist.

Wenn WCCP aktiv ist, überwacht der Router alle Ports, für die WCCP-Umleitung konfiguriert ist. Um seine Präsenz zu signalisieren, sendet die Cache Engine kontinuierlich WCCP. **Hier sind** Pakete an die IP-Adressen, die in der Router-Liste konfiguriert sind.

Es wird eine WCCP-Verbindung zwischen Router und Cache hergestellt. Um Verbindungsinformationen anzuzeigen, führen Sie den Befehl **show ip wccp aus**.

Die Router-ID ist die IP-Adresse des Routers, wie sie von den Cache Engines angezeigt wird. Dieser Bezeichner ist nicht unbedingt die Router-Schnittstelle, die vom umgeleiteten Datenverkehr zum Erreichen des Cache verwendet wird. Die Router-ID in diesem Beispiel lautet 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
```

Der Befehl **show ip wccp 99 detail** enthält detaillierte Informationen zu den Caches.

```
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
```

Das Feld `Umleitung` stellt die Methode dar, mit der die Pakete vom Router an die Cache Engine umgeleitet werden. Diese Methode ist entweder eine generische Routing-Kapselung (GRE) oder Layer 2. Bei GRE werden Pakete in einem GRE-Paket gekapselt. Bei Layer 2 werden Pakete direkt an den Cache gesendet. Für die Layer-2-Umleitung müssen jedoch die Cache-Engine und der Switch bzw. der Router an Layer 2 angrenzen.

Die `Hash-Zuweisung`, die im Hexadezimalformat in den Feldern `Initial Hash Info` und `Assigned Hash Info` dargestellt wird, ist die Anzahl der Hash-Buckets, die diesem Cache zugewiesen sind. Alle möglichen Internet-Quelladressen sind in 64 Bereiche gleicher Größe unterteilt, ein Eimer pro Bereich, und jedem Cache wird Datenverkehr aus einer Reihe dieser Bucket-Quelladressenbereiche zugewiesen. Dieser Betrag wird dynamisch von WCCP entsprechend der Last- und Lastgewichtung des Cache verwaltet. Wenn Sie nur einen Cache installiert haben, kann diesem Cache alle Buckets zugewiesen werden.

Wenn der Router beginnt, Pakete an die Cache-Engine umzuleiten, wird die Anzahl im Feld `"Total Packets Redirected`" (Umgeleitete Pakete insgesamt) erhöht.

Das Feld `"Gesamtzahl der Pakete, die nicht zugewiesen` sind" gibt die Anzahl der Pakete an, die nicht umgeleitet wurden, weil sie keinem Cache zugewiesen wurden. In diesem Beispiel beträgt die Anzahl der Pakete 5. Die Zuweisung von Paketen kann bei der ersten Erkennung von Caches oder für ein kleines Intervall beim Entfernen eines Cache aufgehoben werden.

```
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
```

Wenn der Cache nicht vom Router abgerufen wird, kann es hilfreich sein, die WCCP-Aktivität zu debuggen. Wenn der Router ein **Here I am** Packet aus dem Cache empfängt, antwortet er mit einem **I see you** Packet, und dies wird im Debugger berichtet. Die verfügbaren **Debug-**Befehle sind **debug ip wccp events** und debug **ip wccp pakete**.

Hinweis: Beachten Sie vor der Verwendung von **Debug-**Befehlen die Informationen zu Debug-Befehlen.

Diese Ausgabe enthält ein Beispiel für normale WCCP-Debugmeldungen:

```
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
```

Um die Debugstufe zu erhöhen, können Sie den IP-Paketverkehr verfolgen, um zu überprüfen, ob der Router Pakete von der Cache Engine empfängt. Um zu verhindern, dass ein Router in einer Produktionsumgebung überlastet wird, und um nur den interessanten Datenverkehr anzuzeigen, können Sie eine ACL verwenden, um die Debugging-Meldungen nur auf die Pakete zu beschränken, die die IP-Adresse des Cache als Quelle haben. Eine Beispiel-ACL ist **access-list 130 permit ip host 192.168.15.2 host 192.168.15.1**.

```
Router#debug ip wccp event
   WCCP events debugging is on
  Router#debug ip wccp packet
   WCCP packet info debugging is on
  Router#debug ip packet 130
   IP packet debugging is on for access list 130
   2d19h: WCCP-EVNT:S00: Built new router view: 1 routers,  1 usable web caches,
          change # 00000002
   2d19h: WCCP-PKT:S00: Received valid Redirect_Assignment  packet from 192.168.15.2
```

```
       w/rcv_id 0000001B
2d19h: datagramsize=174, IP 18390: s=192.168.15.2  (Vlan300), d=192.168.15.1
       (Vlan300), totlen 160, fragment 0, fo 0, rcvd 3
2d19h: WCCP-PKT:S00: Sending I_See_You packet to 192.168.15.2  w/ rcv_id 0000001C
2d19h: datagramsize=174, IP 18392: s=192.168.15.2  (Vlan300), d=192.168.15.1
       (Vlan300), totlen 160, fragment 0, fo 0, rcvd 3
2d19h: WCCP-PKT:S00: Sending I_See_You packet to 192.168.15.2  w/ rcv_id 0000001D
2d19h: datagramsize=174, IP 18394: s=192.168.15.2  (Vlan300), d=192.168.15.1
       (Vlan300), totlen 160, fragment 0, fo 0, rcvd 3
2d19h: WCCP-PKT:S00: Sending I_See_You packet to 192.168.15.2  w/ rcv_id 0000001E
2d19h: datagramsize=378, IP 18398: s=192.168.15.2  (Vlan300), d=192.168.15.1
       (Vlan300), totlen 364, fragment 0, fo 0, rcvd 3
2d19h: WCCP-EVNT:S00: Built new router view: 1 routers,  1 usable web caches,
       change # 00000002
2d19h: WCCP-PKT:S00: Received valid Redirect_Assignment  packet from 192.168.15.2
       w/rcv_id 0000001E
2d19h: datagramsize=174, IP 18402: s=192.168.15.2  (Vlan300), d=192.168.15.1
       (Vlan300), totlen 160, fragment 0, fo 0, rcvd 3
2d19h: WCCP-PKT:S00: Sending I_See_You packet to 192.168.15.2  w/ rcv_id 0000001F
2d19h: datagramsize=174, IP 18404: s=192.168.15.2  (Vlan300), d=192.168.15.1
       (Vlan300), totlen 160, fragment 0, fo 0, rcvd 3
2d19h: WCCP-PKT:S00: Sending I_See_You packet to 192.168.15.2  w/ rcv_id 00000020
2d19h: datagramsize=174, IP 18406: s=192.168.15.2  (Vlan300), d=192.168.15.1
       (Vlan300), totlen 160, fragment 0, fo 0, rcvd 3
2d19h: WCCP-PKT:S00: Sending I_See_You packet to 192.168.15.2  w/ rcv_id 00000021
2d19h: datagramsize=378, IP 18410: s=192.168.15.2  (Vlan300), d=192.168.15.1
       (Vlan300), totlen 364, fragment 0, fo 0, rcvd 3
2d19h: WCCP-EVNT:S00: Built new router view: 1 routers,  1 usable web caches,
       change # 00000002
2d19h: WCCP-PKT:S00: Received valid Redirect_Assignment  packet from 192.168.15.2
       w/rcv_id 00000021
2d19h: datagramsize=174, IP 18414: s=192.168.15.2  (Vlan300), d=192.168.15.1
       (Vlan300), totlen 160, fragment 0, fo 0, rcvd 3
2d19h: WCCP-PKT:S00: Sending I_See_You packet to 192.168.15.2  w/ rcv_id 00000022
2d19h: datagramsize=174, IP 18416: s=192.168.15.2  (Vlan300), d=192.168.15.1
       (Vlan300), totlen 160, fragment 0, fo 0, rcvd 3
```

Wenn der Router keine Caches erkennt und keine WCCP-Aktivität zu erkennen ist, überprüfen Sie die grundlegende Verbindung. Versuchen Sie, den Cache vom Router oder Router aus dem Cache zu pingen. Wenn der Ping funktioniert, kann in der Konfiguration ein Fehler vorhanden sein.

Wenn der Cache erfasst, aber keine Pakete umgeleitet werden, überprüfen Sie, ob der Router Datenverkehr empfängt und der Datenverkehr an die Schnittstelle weitergeleitet wird, auf der der Befehl **ip wccp 99 redirect out** angewendet wird. Beachten Sie, dass der abgefangen und umgeleitet wird nur der Datenverkehr, der an den TCP-Port 80 geleitet wird.

Wenn der Datenverkehr immer noch nicht umgeleitet wird und der Webinhalt direkt von den Servern kommt, stellen Sie sicher, dass der Cache die Anweisungen zum Abfangen korrekt durchläuft. Sie müssen einige Hintergrundinformationen über WCCP haben, um diesen Vorgang abzuschließen.

WCCP erkennt zwei verschiedene Diensttypen: *Standard* und *dynamisch*. Der Router kennt implizit einen Standarddienst. Der Router muss also nicht unbedingt Port 80 verwenden, da er dies bereits weiß. Der normale transparente Caching (Web-Cache - Standard Service 0) ist ein Standardservice.

In allen anderen Fällen (einschließlich transparenter Zwischenspeicherung) wird dem Router mitgeteilt, welcher Port abgefangen werden soll. Diese Informationen werden im Paket **Hier bin ich**.

Sie können den Befehl **debug ip packet dump** ausführen, um die Pakete selbst zu überprüfen. Verwenden Sie die erstellte ACL, um nur die Pakete zu debuggen, die von der Cache Engine gesendet wurden.

```
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
```

Mit diesem Befehl können Sie festlegen, ob der Port angekündigt wird oder nicht, ohne dass die gesamte Request For Comments (RFC) angezeigt werden muss. Wenn der Port nicht angekündigt wird, ist das Problem höchstwahrscheinlich in der Konfiguration des Caches.

Weitere Informationen finden Sie im Web Cache Coordination Protocol V2.0 .

Wenn der Cache erfasst und Pakete umgeleitet werden, Ihre Internet-Clients jedoch nicht in der Lage sind, die Server zu durchsuchen, prüfen Sie, ob der Cache über eine Verbindung zum Internet und zu Ihren Servern verfügt. Ping vom Cache an verschiedene IP-Adressen im Internet und an einige Ihrer internen Server. Wenn Sie statt IP-Adressen vollqualifizierte Domänen (URLs) pingen, sollten Sie den DNS-Server angeben, der in der Cache-Konfiguration verwendet werden soll.

Wenn Sie nicht sicher sind, ob der Cache die Anforderungen verarbeitet, können Sie die HTTP-Aktivität im Cache debuggen. Um die HTTP-Aktivität im Cache zu debuggen, müssen Sie den Datenverkehr einschränken, um eine Überladung des Cache zu vermeiden. Erstellen Sie auf dem Router eine ACL mit der Quell-IP-Adresse eines Clients im Internet, die Sie als Gerät für Ihre Tests verwenden können, und verwenden Sie die Option **Redirect-List** des globalen Befehls **ip wccp 99**.

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

Führen Sie nach dem Erstellen und Anwenden der Zugriffskontrollliste die folgenden Schritte aus:

1. Aktivieren Sie das HTTP-Debuggen im Cache mit dem Befehl **debug http all** (Cisco Cache Engine Version 2.x) oder **debug http all** (Cisco Cache Engine Version 3 und ACNS Version 4, 5).
2. Aktivieren Sie die Terminalüberwachung (geben Sie den **Begriff mon**-Befehl ein).
3. Versuchen Sie, einen Ihrer Server vom Client aus zu durchsuchen, den Sie in der ACL

konfiguriert haben.

Hier ein Beispiel für die Ausgabe:

```
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
```

Die relevanten Informationen, die Sie möglicherweise im Debuggen finden, sind **fett** hervorgehoben.

Dies sind die verschiedenen Phasen einer Websitetransaktion:

1. HTTP-Anforderungsheader, die vom Client empfangen wurden.
2. HTTP-Anforderungs-Header werden an den Server gesendet.
3. HTTP-Antwortheader, die vom Server empfangen wurden.
4. HTTP-Antwortheader werden an den Client gesendet.

Wenn die durchsuchte Webseite mehrere Objekte enthält, existieren mehrere Instanzen dieser Ereignissequenz. Verwenden Sie die einfachste Anforderung, um die Debug-Ausgabe zu reduzieren.

Auf einem Catalyst 6500- oder 7600-Router übernimmt ein Funktionsmanager alle im Cisco IOS konfigurierten Funktionen, um eine zusätzliche Ebene der Fehlerbehebung bereitzustellen. Wenn in diesen Geräten eine Layer-3-Funktion konfiguriert ist, werden Informationen, die die Behandlung der empfangenen Frames festlegen, an die Layer-2-Steuerungsfunktionen des Switches oder Routers (den Feature-Manager) weitergeleitet. Für WCCP definieren diese Steuerelementinformationen, welche Pakete von IOS und WCCP abgefangen und an den transparenten Cache weitergeleitet werden.

Der Befehl **show fm features** zeigt die im Cisco IOS aktivierten Funktionen an. Mit diesem Befehl können Sie überprüfen, ob der abzuhörende Port von der Cache Engine ordnungsgemäß angekündigt wurde.

```
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
```

Der Befehl **show fm int vlan 200** zeigt den genauen Inhalt des Ternary Content Addressable Memory (TCAM) an.

```
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
```

Der `vmr IP-Wert 1:` -Zeile definiert die Interception-Umgehung für Frames, die von der Cache Engine kommen. Andernfalls gäbe es eine Umleitungsschleife. Der `vmr IP-Wert Nr. 2:` -Zeile

definiert das Abfangen aller Pakete, die Port 80 als Ziel haben. Wenn Port 80 nicht in der zweiten Zeile angezeigt wird, aber WCCP aktiv ist und der Cache vom Router verwendet werden kann, kann es zu Problemen in der Cache-Konfiguration kommen. Sammeln Sie einen Dump des **Here I am** Packet, um zu bestimmen, ob der Port vom Cache gesendet wird oder nicht.

Wenn Sie das Problem nach der Fehlerbehebung nicht beheben können, wenden Sie sich an das Cisco Technical Assistance Center (TAC).

Hier sind einige grundlegende Informationen, die Sie dem Cisco TAC bereitstellen müssen. Erfassen Sie diese Informationen vom Router:

- Die Ausgabe des Befehls **show tech**. Die Ausgabe der Befehle **show running-config** und **show version output** kann ersetzt werden, wenn Probleme mit der Größe der **show tech-**Ausgabe auftreten.
- Die Ausgabe des Befehls **show ip wccp**.
- Ausgabe des Befehls **show ip wccp web-cache detail**.
- Wenn ein Problem mit der Kommunikation zwischen dem Router und dem Web-Cache besteht, geben Sie die Ausgabe der **debug ip wccp-Ereignisse** und die Befehle **debug ip wccp packages** an, während das Problem auftritt.

Erfassen Sie auf der Cache Engine (nur Cisco Cache Engines) die Ausgabe des Befehls **show tech**.

Gehen Sie wie folgt vor, wenn Sie sich an das TAC wenden:

1. Stellen Sie eine klare Beschreibung des Problems bereit. Sie sollten Antworten auf folgende Fragen einfügen:Welche Symptome treten auf?Kommt es ständig oder selten vor?Wurde das Problem nach einer Änderung der Konfiguration ausgelöst?Werden Caches von Cisco oder Drittanbietern verwendet?
2. Geben Sie eine klare Beschreibung der Topologie an. Fügen Sie ein Diagramm ein, wenn dies klarer wird.
3. Geben Sie alle weiteren Informationen an, die Sie für die Lösung des Problems für nützlich halten.

Die Ausgabe einer Beispielkonfiguration lautet wie folgt:

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

Zugehörige Informationen

- Cisco Cache-Software
- Cisco Cache Engines der Serie 500
- Web Cache Communications Protocol (WCCP)
- Cisco Cache Engine 2.0 Software-Download-Seite (nur registrierte Kunden)
- Cisco Cache Engine 3.0 Software-Download-Seite (nur registrierte Kunden)
- Technischer Support und Dokumentation - Cisco Systems