WAAS - WCCP voor probleemoplossing

Hoofdstuk: WCCP-probleemoplossing

In dit artikel wordt beschreven hoe u problemen met uw probleemoplossing bij WCCP-kwesties kunt oplossen.

Inh

Inhoud

De volgende symptomen duiden op mogelijke WCCP-problemen:

- WAE ontvangt geen verkeer (dit kan zijn toe te schrijven aan verkeerde configuratie van WCCP)
- Eindgebruikers kunnen hun servertoepassingen niet bereiken (dit kan te wijten zijn aan blokkering van het verkeer)
- Netwerkvertraging wanneer WCCP is ingeschakeld (dit kan zijn veroorzaakt door het vallen van pakketten op routers of een hoog CPU-gebruik)
- Gebruik van een te hoge router CPU (mogelijk te wijten aan omleiding in software in plaats van hardware)

WCCP-problemen kunnen resulteren uit problemen met de router (of apparaat voor omleiding) of het WAE-apparaat. Het is nodig om de WCCP-configuratie zowel op de router als op het WAE-apparaat te bekijken. Eerst zullen we de WCCP-configuratie op de router bekijken, dan zullen we de WCCP-configuratie op WAE controleren.

WCCP-oplossing voor problemen op de router

Dit gedeelte gaat over problemen oplossen bij de volgende apparaten:

- Catalyst 6500 Series Switches en ISR- en 3700 Series routers
- ASR 1000 Series routers

WCCP-oplossing voor problemen op Catalyst 6500 Series Switches en ISR- en 3700 Series routers

Begin met het oplossen van problemen door de interceptie van WCCPv2 op de switch of router te controleren door de IOS-opdracht **van** de **show ip wcp** als volgt te gebruiken:

```
Router# show ip wccp
Global WCCP information:
   Router information:
       Router Identifier:                  10.88.81.242
       Protocol Version:                   2.0

   Service Identifier: 61
       Number of Service Group Clients:    1                 <-----Client = WAE
       Number of Service Group Routers:    1
       Total Packets s/w Redirected:       68755             <-----Increments for software-
based redirection
         Process:                          2                 <-----
         Fast:                             0                 <-----
         CEF:                              68753             <-----
       Service mode:                       Open
       Service access-list:                -none-
       Total Packets Dropped Closed:       0
       Redirect access-list:               -none-
       Total Packets Denied Redirect:      0                 <-----Match service group but not
redirect list
       Total Packets Unassigned:           0
       Group access-list:                  -none-
       Total Messages Denied to Group:     0
       Total Authentication failures:      0                 <-----Packets have incorrect
service group password
       Total Bypassed Packets Received:    0
--More--
```

Op platforms die software-gebaseerde omleiding gebruiken, controleer of de Total Packets s/w Rebooters in de bovenstaande opdrachtoutput toenemen. Op platforms die hardware-gebaseerde omleiding gebruiken, zouden deze tellers niet veel moeten verhogen. Als u deze tellers aanzienlijk zien stijgen op op hardware gebaseerde platforms, zou WCCP op de router verkeerd kunnen worden ingesteld (WCCP GRE wordt standaard in software verwerkt) of zou de router terug kunnen vallen op software-omleiding door problemen met hardwarebronnen zoals het opraken van TCAM-bronnen. Er is meer onderzoek vereist als u deze tellers ziet groeien op een op hardware gebaseerd platform, dat tot een hoog CPU-gebruik zou kunnen leiden.

De totale ontkende Packets leiden tegen stappen voor pakketten die overeenkomen met de

servicegroep maar niet overeenkomen met de vervolgkeuzelijst.

De totale tegenstappen van de Verificatie voor pakketten die met het incorrecte wachtwoord van de servicegroep worden ontvangen.

Op routers waar WCCP-omleiding in de software wordt uitgevoerd, kunt u doorgaan door WCCPv2-interceptie op de router te controleren door de volgende opdracht voor **detaillering** (**IP Wcp 61)** van **detaillering** IOS te gebruiken:

```
Router# show ip wccp 61 detail
WCCP Client information:
       WCCP Client ID:          10.88.81.4
       Protocol Version:        2.0
       State:                   Usable                                  <-----Should be Usable
       Initial Hash Info:       00000000000000000000000000000000
                                00000000000000000000000000000000
       Assigned Hash Info:      FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
                                FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
       Hash Allotment:          256 (100.00%)                           <-----Buckets handled by
this WAE
       Packets s/w Redirected:  2452
       Connect Time:            01:19:46                                <-----Time WAE has been
in service group
       Bypassed Packets
         Process:               0
         Fast:                  0
         CEF:                   0
```

Controleer of de WAE-status in het servicegroep 61 in gebruik is. Controleer dat de haakjes aan de WAE zijn toegewezen in het veld Hash Allotment. Het percentage vertelt je hoeveel van de totale haken emmers door deze WAE worden verwerkt. De hoeveelheid tijd die de WAE in de servicegroep is geweest, wordt in het veld Connect Time gemeld. De hash taaicodus moet worden gebruikt met software-gebaseerde omleiding.

U kunt bepalen welke WAE in de boerderij een bepaald verzoek zal behandelen door het verborgen IOS-opdracht **van de** router van de **show ip** *wcp Service* **hash** *dst-ip src-ip src-port src-port* als volgt op de router te gebruiken:

```
Router# show ip wccp 61 hash 0.0.0.0 10.88.81.10 0 0
WCCP hash information for:
   Primary Hash:   Src IP: 10.88.81.10
   Bucket:   9
   WCCP Client: 10.88.81.12                                  <-----Target WAE
```

Op routers waar WCCP-omleiding in de hardware wordt uitgevoerd, kunt u doorgaan door WCCPv2-interceptie op de router te controleren door de volgende opdracht voor **detaillering** (**IP Wcp 61)** van **detaillering** IOS te gebruiken:

```
Cat6k# sh ip wccp 61 detail
WCCP Client information:
   WCCP Client ID:          10.88.80.135
   Protocol Version:        2.0
   State:                   Usable
   Redirection:             L2
   Packet Return:           GRE                     <-----Use generic GRE for hardware-based
```

```
platforms
   Packets Redirected:    0
   Connect Time:          1d18h
   Assignment:            MASK                      <-----Use Mask for hardware-based
redirection

   Mask  SrcAddr    DstAddr    SrcPort DstPort
   ----  -------    -------    ------- -------
   0000: 0x00001741 0x00000000 0x0000  0x0000       <-----Default mask

   Value SrcAddr    DstAddr    SrcPort DstPort CE-IP
   ----- -------    -------    ------- ------- -----
   0000: 0x00000000 0x00000000 0x0000  0x0000  0x0A585087 (10.88.80.135)
   0001: 0x00000001 0x00000000 0x0000  0x0000  0x0A585087 (10.88.80.135)
   0002: 0x00000040 0x00000000 0x0000  0x0000  0x0A585087 (10.88.80.135)
   0003: 0x00000041 0x00000000 0x0000  0x0000  0x0A585087 (10.88.80.135)
```

U wilt de maskertoekenningsmethode voor routers zien die hardware kunnen omleiden.

Om TCAM-bronnen op de router op te slaan, moet u overwegen het standaard WCCP-masker aan te passen aan uw netwerkomgeving. Bekijk deze aanbevelingen:

- Gebruik het kleinste aantal masker bits dat mogelijk is bij het gebruik van WCCP-omleiding. Een kleiner aantal maskerbits bij gebruik in combinatie met ACL-omleiding resulteert in een lager gebruik van CAM. Als er 1-2 WCCP-klanten in een cluster zijn, gebruik dan één bit. Als er 3-4 WCCP-clients zijn, gebruikt u 2 bits. Als er 5-8 WCCP-klanten zijn, gebruik dan 3 bits enzovoort.
- We raden niet aan het WAAS-standaardmasker te gebruiken (0x1741). Voor implementaties van datacenters is het doel om de balans van de filialen in het datacenter te laden in plaats van klanten of hosts. Het juiste masker minimaliseert de WAE-prestaties van het datacenter en dus de schaalopslag. Bijvoorbeeld, gebruik 0x100 tot 0x7F00 voor detailhandeldatacentra die /24 kantornetwerken hebben. Voor grote ondernemingen met een /16 per bedrijf, gebruik 0x10000 tot 0x7F0000 om de bedrijven in het bedrijfsdatacentrum in evenwicht te brengen. In het bijkantoor is het doel om de klanten in balans te brengen die hun IP adressen via DHCP verkrijgen. DHCP geeft over het algemeen IP-adressen van clients uit die hoger zijn dan het laagste IP-adres in het subsysteem. Om DHCP toegewezen IP adressen met masker het best in balans te brengen, gebruik 0x1 tot 0x7F om slechts de laagste bestelbits van het client-IP-adres te gebruiken om de beste distributie te bereiken.

De TCAM-middelen die worden verbruikt door een WCCP-toegangslijst voor omleiding is een product van de inhoud van die ACL-code, vermenigvuldigd met het geconfigureerde WCCP-bits masker. Daarom is er geschil tussen het aantal WCCP-emmers (die op basis van het masker worden gemaakt) en het aantal items in de ACL-omleiding. Bijvoorbeeld, een masker van 0xF (4 bits) en een 200 lijn redirect vergunning ACL kan resulteren in 3200 (2^4 x 200) TCAM ingangen. Het verminderen van het masker tot 0x7 (3 bits) vermindert het gebruik van TCAM met 50% (2^3 x 200 = 1600).

Catalyst 6500 Series en Cisco 7600 Series platforms zijn in staat om WCCP-omleiding in zowel de software als de hardware te verwerken. Als pakketten onbedoeld in software worden omgeleid, wanneer u hardware-omleiding verwacht, kan dit resulteren in overmatig hoog gebruik van de router CPU.

U kunt de TCAM-informatie controleren om te bepalen of de omleiding in de software of de hardware wordt verwerkt. Gebruik de opdracht ShowCAM IOS als volgt:

```
Cat6k# show tcam interface vlan 900 acl in ip

* Global Defaults not shared


Entries from Bank 0


Entries from Bank 1

    permit       tcp host 10.88.80.135 any
    punt         ip any any (8 matches)              <-----Packets handled in software
```

"Punt" overeenkomsten vertegenwoordigen verzoeken die niet in de hardware worden behandeld. Deze situatie kan worden veroorzaakt door de volgende fouten:

- Hash opdracht in plaats van masker
- Uitgaande omleiding in plaats van inkomende
- Uitsluiten omleiden in
- Onbekend WAE MAC-adres
- Gebruik van een loopback-adres voor de generieke GRE-tunnelbestemming

In het volgende voorbeeld, tonen de beleid-route ingangen dat de router volledige hardware omleiding doet:

```
Cat6k# show tcam interface vlan 900 acl in ip

* Global Defaults not shared


Entries from Bank 0


Entries from Bank 1

   permit       tcp host 10.88.80.135 any
   policy-route tcp any 0.0.0.0 255.255.232.190 (60 matches)         <-----These entries show
hardware redirection
   policy-route tcp any 0.0.0.1 255.255.232.190 (8 matches)
   policy-route tcp any 0.0.0.64 255.255.232.190 (16 matches)
   policy-route tcp any 0.0.0.65 255.255.232.190 (19 matches)
   policy-route tcp any 0.0.1.0 255.255.232.190
   policy-route tcp any 0.0.1.1 255.255.232.190
   policy-route tcp any 0.0.1.64 255.255.232.190
   policy-route tcp any 0.0.1.65 255.255.232.190
   policy-route tcp any 0.0.2.0 255.255.232.190
   policy-route tcp any 0.0.2.1 255.255.232.190
   policy-route tcp any 0.0.2.64 255.255.232.190
   policy-route tcp any 0.0.2.65 255.255.232.190 (75 matches)
   policy-route tcp any 0.0.3.0 255.255.232.190 (222195 matches)
```

Hier moet I Am (HIA) vanuit de WAE dezelfde interface invoeren als de WAE MAC bekend is. We raden u aan een loopback-interface te gebruiken en geen direct verbonden interface in de WAE-routerlijst.

WCCP voor probleemoplossing op de ASR 1000 Series routers

De opdrachten voor het oplossen van problemen WCCP op Cisco ASR 1000 Series routers zijn anders dan de andere routers. In dit gedeelte worden opdrachten weergegeven die u kunt gebruiken om WCCP-informatie op de ASR 1000 te verkrijgen.

Om WCCP-informatie over routeprocessors weer te geven, gebruikt u de **actieve** opdrachten **van de** WCCP**-software van het** platform als volgt:

```
ASR1000# sh platform software wccp rp active
Dynamic service 61
Priority: 34, Number of clients: 1                          <-----Number of WAE clients
Assign Method: Mask, Fwd Method: GRE, Ret Method: GRE       <-----Assignment, forwarding, and
return methods
L4 proto: 6, Use Source Port: No, Is closed: No
Dynamic service 62
Priority: 34, Number of clients: 1                          <-----
Assign Method: Mask, Fwd Method: GRE, Ret Method: GRE       <-----
L4 proto: 6, Use Source Port: No, Is closed: No
```

Het volgende voorbeeld toont extra opdrachten die u kunt gebruiken om het doorsturen van processorinformatie te onderzoeken:

```
ASR1000# sh platform software wccp fp active ?
  <0-255>     service ID
  cache-info  Show cache-engine info
  interface   Show interface info
  statistics  Show messaging statistics
  web-cache   Web-cache type
  |           Output modifiers
  <cr>
```

Als u pakketstatistieken met herleiding voor elke interface wilt weergeven, gebruikt u de opdracht **Wcp-interfacetellers van het platform** als volgt:

```
ASR1000# sh platform software wccp interface counters
Interface GigabitEthernet0/1/2
       Input Redirect Packets  = 391
       Output Redirect Packets  = 0
Interface GigabitEthernet0/1/3
       Input Redirect Packets  = 1800
       Output Redirect Packets  = 0
```

Gebruik de opdracht **van de WCCP-**cacheloketten van de **show platform software Wcp** om de WCCP-cacheinformatie als volgt weer te geven:

```
ASR1000# sh platform software wccp web-cache counters
Service Group (0, 0) counters
       unassigned_count = 0
       dropped_closed_count = 0
       bypass_count = 0
       bypass_failed_count = 0
       denied_count = 0
       redirect_count = 0
```

U kunt de volgende opdrachten gebruiken om informatie over een laag niveau weer te geven:

- **tonen platform zodat de F0-interface**

- **WCP-interface met platform tonen**
- **wcp-configuratie van platform software**

Zie voor meer informatie het witboek "Web Cache Control Protocol, versie 2, implementeren en oplossen van problemen met betrekking tot Cisco ASR 1000 Series Aggregation Services Routers"

WCCP voor probleemoplossing op WAE

Begin met het oplossen van problemen in de WAE door de opdracht **tonen wcp-services** te gebruiken. U wilt beide services 61 en 62 als volgt configureren:

```
WAE-612# show wccp services
Services configured on this File Engine
       TCP Promiscuous 61
       TCP Promiscuous 62
```

Controleer de WCCP-status vervolgens met de opdracht **WCCP-status weergeven**. U wilt zien dat WCCP, versie 2, als volgt is ingeschakeld en actief is:

```
WAE-612# show wccp status
WCCP version 2 is enabled and currently active
```

Kijk naar de WCCP-bedrijfsinformatie door de opdracht **WCCP-**motor **voor groot gebied** te gebruiken. Deze opdracht toont het aantal WAE's in de boerderij, hun IP-adressen, die de lead WAE zijn, routers die WAE's kunnen zien en andere informatie, als volgt:

```
WAE612# show wccp wide-area-engine
Wide Area Engine List for Service: TCP Promiscuous 61

Number of WAE's in the Cache farm: 3
Last Received Assignment Key IP address: 10.43.140.162     <-----All WAEs in farm should have
same Key IP
Last Received Assignment Key Change Number: 17
Last WAE Change Number: 16
Assignment Made Flag = FALSE

       IP address = 10.43.140.162       Lead WAE = YES  Weight = 0
       Routers seeing this Wide Area Engine(3)
               10.43.140.161
               10.43.140.166
               10.43.140.168

       IP address = 10.43.140.163       Lead WAE = NO  Weight = 0
       Routers seeing this Wide Area Engine(3)
               10.43.140.161
               10.43.140.166
               10.43.140.168

       IP address = 10.43.140.164       Lead WAE = NO  Weight = 0
       Routers seeing this Wide Area Engine(3)
               10.43.140.161
               10.43.140.166
               10.43.140.168
. . .
```

Kijk naar de routerinformatie door de opdracht **WCCP-routers** te gebruiken. Controleer of er bidirectionele communicatie is met routers die WCCP-enabled hebben, en alle routers tonen dezelfde KeyIP en KeyCN (verandering-nummer), als volgt:

```
WAE-612# show wccp routers

Router Information for Service: TCP Promiscuous 61
       Routers Seeing this Wide Area Engine(1)
       Router Id       Sent To         Recv ID     KeyIP        KeyCN  MCN
       10.43.140.161   10.43.140.161   00203A21    10.43.140.162  17    52   <-----Verify
routers have same KeyIP and KeyCN
       10.43.140.166   10.43.140.166   00203A23    10.43.140.162  17    53
       10.43.140.168   10.43.140.165   00203A2D    10.43.140.162  17    25
       Routers not Seeing this Wide Area Engine
               -NONE-
       Routers Notified of from other WAE's
               -NONE-
       Multicast Addresses Configured
               -NONE-
. . .
```

In gevallen waar WAE geen Layer 2-eenheid is naast de router, of een loopback-adres wordt gebruikt, moeten statische routes of een standaardgateway worden gebruikt om WCCP te ondersteunen.

Om de verdeling van de zakemmer in de dienstgroep te onderzoeken, gebruik de opdracht van het **tonen wcp stromen tcp-promiscuous** order:

```
wae# sh wccp flows tcp-promiscuous
Flow counts for service: TCP Promiscuous 61
Bucket                              Flow Counts
  0- 11:     0     0     0     0     0     0     0     0     0     0     0     0
 12- 23:     0     0     0     0     0     0     0     0     0     0     0     0
 24- 35:     0     0     0     0     0     0     0     0     0     0     0     0
 36- 47:     0     0     0     0     0     0     0     0     0     0     0     0
 48- 59:     0     0     0     0     0     0     0     0     0     0     0     0
 60- 71:     0     0     0     0     0     0     0     0     0     0     0     0
 72- 83:     0     0     0     0     0     0     0     0     0     0     0     0
 84- 95:     0     0     0     0     0     0     0     0     0     0     0     0
 96-107:     0     0     0     0     0     0     0     0     0     0     0     0
108-119:     0     0     0     0     0     0     0     0     0     0     0     0
120-131:     0     0     0     0     0     0     0     0     0     0     0     0
132-143:     0     0     0     0     0     0     0     0     0     0     0     0
144-155:     0     0     0     0     0     0     0     0     0     0     0     0
156-167:     0     0     0     0     0     0     0     0     0     0     0     0
168-179:     0     0     0     0     0     0     0     0     0     0     0     0
180-191:     0     0     0     0     0     0     0     0     0     0     0     0
192-203:     0     0     0     0     0     0     0     0     0     0     0     0
204-215:     0     0     0     0     0     0     0     0     0     0     0     0
216-227:     0     0     0     0     0     0     0     0     0     0     0     0
228-239:     0     0     0     0     0     0     0     0     0     3     0     0
240-251:     0     0     0     0     0     0     0     0     0     0     0     0
252-255:     0     0     0     0
```

U kunt ook de summiere versie van de opdracht gebruiken om soortgelijke informatie te zien, evenals informatie over de bypass-flow:

```
wae# sh wccp flows tcp-promiscuous summary
Flow summary for service: TCP Promiscuous 61
Total Buckets
OURS = 256

  0- 59: 0000000000 0000000000 0000000000 0000000000 0000000000 0000000000
 60-119: 0000000000 0000000000 0000000000 0000000000 0000000000 0000000000
120-179: 0000000000 0000000000 0000000000 0000000000 0000000000 0000000000
180-239: 0000000000 0000000000 0000000000 0000000000 0000000000 0000000000
240-255: 0000000000 000000

BYP  = 0

  0- 59: .......... .......... .......... .......... .......... ..........
 60-119: .......... .......... .......... .......... .......... ..........
120-179: .......... .......... .......... .......... .......... ..........
180-239: .......... .......... .......... .......... .......... ..........
240-255: .......... ......

AWAY = 0

  0- 59: .......... .......... .......... .......... .......... ..........
 60-119: .......... .......... .......... .......... .......... ..........
120-179: .......... .......... .......... .......... .......... ..........
180-239: .......... .......... .......... .......... .......... ..........
240-255: .......... ......
. . .
```

Gebruik de opdracht **WCCP Gre** om GRE-pakketstatistieken als volgt weer te geven:

```
WAE-612# show wccp gre
Transparent GRE packets received:              5531561         <-----Increments for WCCP GRE
redirection
Transparent non-GRE packets received:          0               <-----Increments for WCCP L2
redirection
Transparent non-GRE non-WCCP packets received: 0               <-----Increments for ACE or PBR
redirection
Total packets accepted:                        5051            <-----Accepted for optimization;
peer WAE found
Invalid packets received:                      0
Packets received with invalid service:         0
Packets received on a disabled service:        0
Packets received too small:                    0
Packets dropped due to zero TTL:               0
Packets dropped due to bad buckets:            0
Packets dropped due to no redirect address:    0
Packets dropped due to loopback redirect:      0
Pass-through pkts dropped on assignment update:0
Connections bypassed due to load:              0
Packets sent back to router:                   0
GRE packets sent to router (not bypass)        0               <-----Handled with WCCP
negotiated return egress
Packets sent to another WAE:                   0
GRE fragments redirected:                      0
GRE encapsulated fragments received:           0
Packets failed encapsulated reassembly:        0
Packets failed GRE encapsulation:              0
--More--
```

Als de WCCP-omleiding goed werkt, moet een van de eerste twee tellers worden verhoogd.

De transparante niet-GRE-pakketten hebben tegenstappen voor pakketten ontvangen die opnieuw

worden gericht met de WCCP Layer 2-omleidingsmethode.

De pakketten Transparent niet-GRE niet-WCCP ontvingen tegenstappen voor pakketten die door een niet-WCCP interception methode (zoals ACE of PBR) worden hergeleid.

De totaal geaccepteerde tellers wijzen op pakketten die voor optimalisatie zijn geaccepteerd omdat de auto-ontdekking een peer WAE vond.

De GRE-pakketten die naar de router (niet bypass) worden verzonden, wijzen op pakketten die werden behandeld met de WCCP-onderhandelde methode van het retourneren.

De pakketten die naar een andere WAE-teller worden verzonden geven aan dat de stroombescherming plaatsvindt wanneer er een andere WAE aan de servicegroep wordt toegevoegd en beginnen met het verwerken van een emmer-toewijzing die eerder door een andere WAE werd verwerkt.

Controleer dat de grasmethoden die worden gebruikt de verwachte zijn door de opdracht **showegress-methods** te gebruiken:

```
WAE674# show egress-methods

Intercept method : WCCP

 TCP Promiscuous 61 :
     WCCP negotiated return method : WCCP GRE

                       Egress Method      Egress Method
     Destination        Configured           Used
     -----------  ----------------------  -------------
     any          WCCP Negotiated Return  WCCP GRE               <-----Verify these are
expected

 TCP Promiscuous 62 :
     WCCP negotiated return method : WCCP GRE

                       Egress Method      Egress Method
     Destination        Configured           Used
     -----------  ----------------------  -------------
     any          WCCP Negotiated Return  WCCP GRE               <-----Verify these are
expected
```

Onjuist toegewezen methoden kunnen onder de volgende voorwaarden voorkomen:

- De onderhandelde terugkeermethode is geconfigureerd, maar WCCP onderhandelt over de Layer 2 retourmethode en alleen GRE-rendement wordt ondersteund door WAAS.
- De generieke GRE-compressiemethode wordt ingesteld, maar de interceptiemethode is Layer 2 en alleen WCCP GRE wordt ondersteund als de interceptiemethode wanneer generieke GRE-prioriteit is ingesteld.

In een van deze gevallen wordt een minimaal alarm opgestoken en wordt geklaard wanneer de mismatch wordt opgelost door de compressiemethode of de WCCP-configuratie te wijzigen. Totdat het alarm is gewist, wordt de standaard IP-verzendmethode gebruikt.

Het volgende voorbeeld toont de opdrachtoutput wanneer er een fout-match is:

```
WAE612# show egress-methods
Intercept method : WCCP
 TCP Promiscuous 61 :
     WCCP negotiated return method : WCCP GRE

                      Egress Method      Egress Method
     Destination       Configured           Used
     -----------  ---------------------  -------------
     any          Generic GRE            IP Forwarding                    <-----Mismatch

     WARNING:  WCCP has negotiated WCCP L2 as the intercept method for     <-----Warning if
mismatch occurs
               which generic GRE is not supported as an egress method
               in this release. This device uses IP forwarding as the
               egress method instead of the configured generic GRE
               egress method.
 TCP Promiscuous 62 :

     WCCP negotiated return method : WCCP GRE
                      Egress Method      Egress Method
     Destination       Configured           Used
     -----------  ---------------------  -------------
     any          Generic GRE            IP Forwarding                    <-----Mismatch

     WARNING:  WCCP has negotiated WCCP L2 as the intercept method for     <-----Warning if
mismatch occurs
               which generic GRE is not supported as an egress method
               in this release. This device uses IP forwarding as the
               egress method instead of the configured generic GRE
               egress method.
```

Voor Catalyst 6500 Sup720- of Sup32-routers raden we aan de generieke GRE-compressiemethode te gebruiken, die in hardware wordt verwerkt. Daarnaast raden we aan één multipoint tunnel te gebruiken voor het gemak van configuratie, in plaats van één point-to-point tunnel voor elke WAE. Raadpleeg voor informatie over tunnelconfiguratie het gedeelte Een GRE-tunnelinterface configureren op een router in de *Cisco Wide Area Application Services Configuration Guide*.

Om de GRE tunnelstatistieken voor elke onderscheppende router te bekijken, gebruikt u de opdracht van de **show statistics generieke-gre** als volgt:

```
WAE# sh stat generic
Tunnel Destination:                             10.10.14.16
Tunnel Peer Status:                             N/A
Tunnel Reference Count:                         2
Packets dropped due to failed encapsulation:    0
Packets dropped due to no route found:          0
Packets sent:                                   0
Packets sent to tunnel interface that is down:  0
Packets fragmented:                             0
```

Als u er niet voor wilt zorgen dat pakketten die afkomstig zijn van een WAE, niet worden onderschept, kan dit leiden tot een omleidingslus. Als een WAE zijn eigen ID detecteert die in het veld TCP-opties is geretourneerd, is er een omleidingsloop opgetreden en levert dit het volgende syslig-bericht op:

```
%WAAS-SYS-3-900000: 137.34.79.11:1192 - 137.34.77.196:139 - opt_syn_rcv: Routing Loop detected -
Packet has our own devid. Packet dropped.
```

U kunt het bestand syslog.txt op gevallen van deze fout zoeken door de opdracht **Zoeken** als volgt te gebruiken:

```
WAE-612# find match “Routing Loop” syslog.txt
```

Deze fout blijkt ook in de TFO-stroomstatistieken beschikbaar in de opdracht **Statistieken filteren** als volgt:

```
WAE-612# show statistics filtering
. . .
Syn packets dropped with our own id in the options:   8        <-----Indicates a redirection
loop
. . .
```

Als u uitgaande omleiding op de router doet, omdat het verkeer de router verlaat, zal het teruggeleid worden naar de WAE, die het pakje uit de router zal terugkeren, wat een routing loop veroorzaakt. Als het datacenter WAE en servers op verschillende VLAN’s zijn en de tak WAE en de clients op verschillende VLAN’s zijn, kunt u een routinglus vermijden door de volgende routerconfiguratie op WAE VLAN te gebruiken:

```
ip wccp redirect exclude in
```

Als WAE hetzelfde VLAN deelt met zijn aangrenzende klanten of servers, kunt u het routeren van lijnen vermijden door de overeengekomen retourmethode te gebruiken, of het generieke GRE-rendement voor platforms waar WCCP-omleiding in de hardware wordt uitgevoerd. Wanneer u generieke GRE-opbrengst gebruikt, gebruikt WAE een GRE-tunnel om verkeer naar de router terug te brengen.

Configureerbare service-ID’s en variabele Time-outs voor probleemoplossing in versie 4.4.1

OPMERKING: De WCCP-configureerbare service-ID’s en de opties voor de detectie van variabele uitvallen zijn in WAAS versie 4.4.1 geïntroduceerd. Deze sectie is niet van toepassing op eerdere WAAS-versies.

Alle WAE’s in een WCCP-kwekerij moeten dezelfde WCCP-service-ID’s gebruiken (de standaardinstelling is 61 en 62), en deze ID’s moeten overeenkomen met alle routers die de boerderij ondersteunen. Een WAE met andere WCCP-service-ID’s dan die welke op de routers zijn ingesteld, mag zich niet bij het bedrijf aansluiten en het bestaande "Router onbereikbaar" alarm wordt verhoogd. Op dezelfde manier moeten alle WAE's in een boerderij dezelfde waarde gebruiken voor de time-out van de detectie van fouten. Een WAE heft een alarm op als u het met een mislopende waarde configureren.

Als u een alarm ziet dat een WAE zich niet bij een WCCP-boerderij kan aansluiten, controleer dan dat de WCCP-service-ID’s die op WAE zijn geconfigureerd en de routers in de boerderij-match. Gebruik in de WAE's de opdracht **WCCP-groot gebiedsmotor** om de geconfigureerde service-ID’s te controleren. Op de routers kunt u de IOS-opdracht **tonen** IP **WCCP** IOS gebruiken.

Om te controleren als WAE connectiviteit aan de router heeft, gebruik het **zeer gedetailleerde** de **diensten van** WCCP **en laat** de opdrachten van de **WCCP-router met** details **zien**.

Daarnaast kunt u WCCP-debug van uitvoer in de WAE inschakelen door de opdrachten **debug ip-wcp** te gebruiken of **IP-**pakketopdrachten **te debug**.

Als u een "Router Onbruikbaar" minimaal alarm voor een WAE ziet, kan dit betekenen dat de variabele waarde voor de detectie van fouten die op WAE is ingesteld niet door de router wordt ondersteund. Gebruik de opdracht van het **hoogtealarm minimaal detail** om te controleren of de reden voor het alarm "mismatch van het tussenpoos met router" is:

```
WAE# show alarm minor detail

Minor Alarms:
-------------
       Alarm ID                 Module/Submodule               Instance
  ---------------             --------------------          ---------------
  1 rtr_unusable              WCCP/svc051/rtr2.192.9.161

    Jan 11 23:18:41.885 UTC, Communication Alarm, #000005, 17000:17003
    WCCP router 2.192.9.161 unusable for service id: 51 reason: Timer interval       <-----Check
reason
mismatch with router                                                                 <-----
```

Controleer in de WAE de ingestelde tijd voor de detectie van fouten als volgt:

```
WAE# show wccp services detail

Service Details for TCP Promiscuous 61 Service
       Service Enabled                    : Yes
       Service Priority                   : 34
       Service Protocol                   : 6
       Application                        : Unknown
       Service Flags (in Hex)             : 501
       Service Ports                      :      0     0     0     0
                                          :      0     0     0     0
       Security Enabled for Service       : No
       Multicast Enabled for Service      : No
       Weight for this Web-CE             : 1
       Negotiated forwarding method       : GRE
       Negotiated assignment method       : HASH
       Negotiated return method           : GRE
       Negotiated HIA interval            : 2 second(s)
       Negotiated failure-detection timeout  : 30 second(s)          <-----Failure detection
timeout configured
. . .
```

Op de router, controleer of de IOS versie variabele timeout van de detectie van mislukkingen ondersteunt. Als dit het geval is, kunt u de ingestelde instelling controleren door de opdracht *Voorbeeld* van **ip** xx **detail** te gebruiken, waarbij *xx* de WCCP dienst-ID is. Er zijn drie mogelijke resultaten:

- WAE gebruikt de timeout van de detectie van standaardfouten van 30 seconden en de router is ingesteld om het even of ondersteunt geen variabele timeout: De routeruitvoer toont geen details over de timeout instelling. Deze configuratie werkt prima.
- WAE gebruikt een time-out van 9 of 15 seconden voor de detectie van niet-standaard fouten en de router ondersteunt geen variabele timeout: Het staatsveld toont "NIET bruikbaar" en de WAE kan de router niet gebruiken. Verander de time-out van de WAE-detectie van fouten naar de standaardwaarde van 30 seconden door de opdracht **voor** de **detectie van** een **TCP-**

storing 30 te gebruiken.
- WAE gebruikt een time-out van 9 of 15 seconden voor de detectie van niet-standaard fouten en de router ondersteunt variabele timeout: Het veld Client timeout toont de tijd voor de detectie van fouten, die overeenkomt met de WAE. Deze configuratie werkt prima.

Als de WCCP-boerderij instabiel is als gevolg van 'link flapping', kan dat zijn omdat de WCCP-detectie te laag is.