Cisco WAAS-Fehlerbehebungsleitfaden für Version 4.1.3 und höher

Kapitel: Fehlerbehebung WCCP

In diesem Artikel wird die Fehlerbehebung bei WCCP-Problemen beschrieben.

Inh

Ha
An
Da
Vo
Op
Pro
Fel
Fel
Fel
Fel
Fel
Fel
Fel
Fel
Fel
Fel
Fel
Fel
Ha
Fel
vW
Fel
Fel

Inhalt

- 1 Fehlerbehebung bei WCCP auf dem Router
  - 1,1 Fehlerbehebung bei WCCP auf den Catalyst Switches der Serie 6500 und den Routern der Serien ISR und 3700
  - 1,2 Fehlerbehebung bei WCCP auf Routern der Serie ASR 1000
- 2 Fehlerbehebung bei WCCP in der WAE
- 1 Fehlerbehebung: Konfigurierbare Service-IDs und variable Timeouts in Version 4.4.1

Die folgenden Symptome weisen auf mögliche WCCP-Probleme hin:

- Die WAE empfängt keinen Datenverkehr (möglicherweise aufgrund einer WCCP-Fehlkonfiguration).
- Endbenutzer können ihre Serveranwendungen nicht erreichen (kann auf Blackholing-Verkehr zurückzuführen sein)
- Langsame Netzwerke bei Aktivierung von WCCP (möglicherweise aufgrund von

Paketverlusten des Routers oder hoher CPU-Auslastung des Routers)
- Übermäßig hohe CPU-Auslastung des Routers (möglicherweise aufgrund einer Umleitung in die Software anstatt in die Hardware)

WCCP-Probleme können auf Probleme mit dem Router (oder dem Umleitungsgerät) oder dem WAE-Gerät zurückzuführen sein. Die WCCP-Konfiguration muss sowohl auf dem Router als auch auf dem WAE-Gerät überprüft werden. Zunächst wird die WCCP-Konfiguration auf dem Router überprüft. Anschließend wird die WCCP-Konfiguration auf der WAE überprüft.

Fehlerbehebung bei WCCP auf dem Router

In diesem Abschnitt wird die Fehlerbehebung für die folgenden Geräte beschrieben:

- Catalyst Switches der Serie 6500 sowie Router der Serien ISR und 3700
- Router der Serie ASR 1000

Fehlerbehebung bei WCCP auf den Catalyst Switches der Serie 6500 und den Routern der Serien ISR und 3700

Beginnen Sie mit der Fehlerbehebung, indem Sie die WCCPv2-Interception auf dem Switch oder Router überprüfen. Verwenden Sie dazu den Befehl **show ip wccp** IOS wie folgt:

```
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--
```

Überprüfen Sie auf Plattformen, die eine softwarebasierte Umleitung verwenden, ob die Zähler für umgeleitete Pakete insgesamt in der oben angegebenen Befehlsausgabe erhöht werden. Auf Plattformen, die hardwarebasierte Umleitungen verwenden, sollten diese Zähler nicht viel erhöhen. Wenn diese Zähler auf hardwarebasierten Plattformen erheblich erhöht werden, kann WCCP auf dem Router falsch konfiguriert werden (WCCP GRE wird standardmäßig in der Software verarbeitet), oder der Router kann aufgrund von Problemen mit den

Hardwareressourcen, wie z. B. bei der Auslastung der TCAM-Ressourcen, wieder auf die Software-Umleitung zurückfallen. Weitere Untersuchungen sind erforderlich, wenn diese Zähler auf einer hardwarebasierten Plattform inkrementiert werden, was zu einer hohen CPU-Auslastung führen könnte.

Der Zähler für die Gesamtzahl der Pakete mit Umleitung mit Absage erhöht sich für Pakete, die der Servicegruppe entsprechen, jedoch nicht mit der Umleitungsliste übereinstimmen.

Der Zähler für Fehler bei der Gesamtauthentifizierung erhöht sich für Pakete, die mit dem falschen Dienstgruppenkennwort empfangen werden.

Bei Routern, bei denen die WCCP-Umleitung in der Software durchgeführt wird, überprüfen Sie weiterhin die WCCPv2-Interception auf dem Router, indem Sie den IOS-Befehl **show ip wccp 61 detail** wie folgt verwenden:

```
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
```

Überprüfen Sie, ob der WAE-Status in der Servicegruppe 61 verwendet werden kann. Stellen Sie sicher, dass der WAE im Feld Hash Alloment (Hash-Zuweisung) Hash-Buckets zugewiesen sind. Der Prozentsatz gibt an, wie viele der gesamten Hash-Buckets von dieser WAE behandelt werden. Die Zeit, die die WAE in der Service-Gruppe war, wird im Feld "Connect Time" (Zeit verbinden) gemeldet. Die Hash-Zuweisungsmethode sollte bei softwarebasierter Umleitung verwendet werden.

Sie können mithilfe des Befehls **show ip wccp** *service* **hash** *dst-ip src-ip dst-port src-port* secret IOS auf dem Router bestimmen, welche WAE in der Farm eine bestimmte Anforderung behandelt:

```
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
```

Bei Routern, bei denen die WCCP-Umleitung in der Hardware durchgeführt wird, überprüfen Sie weiterhin die WCCPv2-Interception auf dem Router, indem Sie den IOS-Befehl **show ip wccp 61 detail** wie folgt verwenden:

```
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)
```

Sie möchten die Maskenzuweisungsmethode für Router anzeigen, die eine Hardware-Umleitung ermöglichen.

Um TCAM-Ressourcen auf dem Router zu speichern, sollten Sie die Standard-WCCP-Maske an Ihre Netzwerkumgebung anpassen. Beachten Sie folgende Empfehlungen:

- Verwenden Sie die kleinste Anzahl an Maskenbits, die bei Verwendung der WCCP-Umleitungszugriffskontrollliste möglich ist. Eine geringere Anzahl an Maskenbits in Verbindung mit der Umleitungszugriffskontrollliste führt zu einer geringeren TCAM-Nutzung. Wenn sich 1-2 WCCP-Clients in einem Cluster befinden, verwenden Sie ein Bit. Wenn 3-4 WCCP-Clients vorhanden sind, verwenden Sie 2 Bit. Wenn 5-8 WCCP-Clients vorhanden sind, verwenden Sie 3 Bit usw.
- Die Verwendung der WAAS-Standardmaske (0x1741) wird nicht empfohlen. Bei Bereitstellungen im Rechenzentrum besteht das Ziel darin, den Lastenausgleich zwischen den Außenstellen und dem Rechenzentrum anstelle von Clients oder Hosts vorzunehmen. Die rechte Maske minimiert das WAE-Peering im Rechenzentrum und ermöglicht somit eine Skalierung des Speichers. Verwenden Sie beispielsweise 0x100 bis 0x7F00 für Rechenzentren im Einzelhandel mit /24 Zweigstellennetzwerken. Für große Unternehmen mit einem Volumen von /16 pro Unternehmen sollten Sie 0x1000 bis 0x7F0000 verwenden, um die Geschäftsabläufe in das Rechenzentrum des Unternehmens zu verlagern. In der Zweigstelle soll ein Gleichgewicht zwischen den Clients hergestellt werden, die ihre IP-Adressen über DHCP beziehen. DHCP gibt im Allgemeinen Client-IP-Adressen aus, die von der niedrigsten IP-Adresse im Subnetz inkrementiert werden. Verwenden Sie 0x1 bis 0x7F, um die DHCP-zugewiesenen IP-Adressen am besten mit der Maske zu vergleichen, um nur die Bits der niedrigsten Reihenfolge der Client-IP-Adresse zu berücksichtigen, um die beste Verteilung zu erzielen.

Die TCAM-Ressourcen, die von einer WCCP-Liste für die Umleitung verwendet werden, sind ein Produkt des Inhalts dieser ACL, multipliziert mit der konfigurierten WCCP-Bitmaske. Daher gibt es einen Konflikt zwischen der Anzahl der WCCP-Gruppen (die basierend auf der Maske erstellt werden) und der Anzahl der Einträge in der Umleitungszugriffskontrollliste. Beispielsweise können

eine Maske von 0xF (4 Bit) und eine 200-Zeilen-Umleitungszugriffskontrollliste zu 3200 (2^4 x 200) TCAM-Einträgen führen. Durch die Reduzierung der Maske auf 0x7 (3 Bit) wird die TCAM-Nutzung um 50 % reduziert (2^3 x 200 = 1600).

Plattformen der Serien Catalyst 6500 und 7600 von Cisco können die WCCP-Umleitung sowohl in der Software als auch in der Hardware unterstützen. Wenn Pakete versehentlich in Software umgeleitet werden und Sie Hardwareumleitung erwarten, kann dies zu einer zu hohen CPU-Nutzung des Routers führen.

Sie können die TCAM-Informationen überprüfen, um festzustellen, ob die Umleitung in der Software oder der Hardware durchgeführt wird. Verwenden Sie den Befehl **show tcam** IOS wie folgt:

```
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
```

"Sammelanschlüsse" stellen Anforderungen dar, die in der Hardware nicht behandelt werden. Diese Situation kann durch folgende Fehler verursacht werden:

- Hash-Zuordnung anstelle von Maske
- Umleitung ausgehender Anrufe anstelle von eingehenden Anrufen
- Umleiten in ausschließen
- Unbekannte WAE MAC-Adresse
- Verwenden einer Loopback-Adresse für das Ziel des generischen GRE-Tunnels

Im folgenden Beispiel zeigen die Einträge für die Richtlinienroute, dass der Router die vollständige Hardware-Umleitung durchführt:

```
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)
```

Der Here I Am (HIA) von der WAE muss die gleiche Schnittstelle wie die WAE MAC-Schnittstelle verwenden. Es wird empfohlen, in der Liste der WAE-Router eine Loopback-Schnittstelle und keine direkt verbundene Schnittstelle zu verwenden.

Fehlerbehebung bei WCCP auf Routern der Serie ASR 1000

Die Befehle zur Fehlerbehebung bei WCCP auf den Cisco Routern der Serie ASR 1000 unterscheiden sich von den anderen Routern. Dieser Abschnitt enthält Befehle, mit denen Sie WCCP-Informationen zum ASR 1000 abrufen können.

Verwenden Sie die folgenden Befehle **show plattform software wccp rp active**, um Routingprozessor-WCCP-Informationen anzuzeigen:

```
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
```

Das folgende Beispiel zeigt zusätzliche Befehle, mit denen Sie Weiterleitungsprozessorinformationen untersuchen können:

```
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>
```

Um umgeleitete Paketstatistiken für jede Schnittstelle anzuzeigen, verwenden Sie den Befehl **show platform software wccp interface counter**:

```
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
```

Verwenden Sie den Befehl **show platform software wccp web-cache counter**, um die WCCP-

Cacheinformationen wie folgt anzuzeigen:

```
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
```

Verwenden Sie die folgenden Befehle, um Details auf niedriger Ebene anzuzeigen:

- **show plattform so interface F0 brief**
- **show platform software wccp f0 interface**
- **debugplattform software wccp konfiguration**

Weitere Informationen finden Sie im Whitepaper "Bereitstellung und Fehlerbehebung im Web Cache Control Protocol Version 2 auf Cisco Aggregation Services Routern der Serie ASR 1000".

Fehlerbehebung bei WCCP in der WAE

Beginnen Sie mit der Fehlerbehebung für die WAE, indem Sie den Befehl **show wccp services** verwenden. Es wird empfohlen, die Services 61 und 62 wie folgt zu konfigurieren:

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

Überprüfen Sie anschließend den WCCP-Status mit dem Befehl **show wccp status**. Sie möchten sehen, dass WCCP Version 2 wie folgt aktiviert und aktiv ist:

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

Sehen Sie sich die WCCP-Informationen mithilfe des Befehls **show wccp wide-area-engine an**. Dieser Befehl zeigt die Anzahl der WAEs in der Farm, ihre IP-Adressen, eine davon ist die führende WAE, Router, die die WAEs anzeigen können, und andere Informationen wie folgt an:

```
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
. . .
```

Überprüfen Sie die Routerinformationen mit dem Befehl **show wccp routers**. Überprüfen Sie, ob eine bidirektionale Kommunikation mit WCCP-fähigen Routern besteht und alle Router dieselbe KeyIP- und KeyCN-Nummer (Änderungsnummer) wie folgt anzeigen:

```
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 Fällen, in denen die WAE nicht über Layer 2 mit dem Router verbunden ist oder eine Loopback-Adresse verwendet wird, sind zur Unterstützung von WCCP entweder statische Routen oder ein Standard-Gateway erforderlich.

Verwenden Sie den Befehl **show wccp flows tcp-Promiscuous**, um die Hash-Bucket-Verteilung in der Servicegruppe wie folgt zu untersuchen:

```
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
```

Alternativ können Sie die zusammengefasste Version des Befehls verwenden, um ähnliche Informationen anzuzeigen und Ablaufdaten zu umgehen:

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

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

BYP  = 0

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

AWAY = 0

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

Verwenden Sie den Befehl **show wccp gre**, um die GRE-Paketstatistiken wie folgt anzuzeigen:

```
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--
```

Wenn die WCCP-Umleitung funktioniert, sollte einer der beiden ersten Zähler inkrementiert werden.

Die empfangenen transparenten Nicht-GRE-Pakete enthalten Zählerinkremente für Pakete, die mithilfe der Weiterleitungsmethode WCCP Layer 2 umgeleitet werden.

Die transparenten Nicht-GRE-Nicht-WCCP-Pakete erhalten Zählerinkremente für Pakete, die durch eine Nicht-WCCP-Abfangmethode (z. B. ACE oder PBR) umgeleitet werden.

Der Zähler für akzeptierte Gesamtpakete gibt Pakete an, die zur Optimierung akzeptiert werden, da bei der automatischen Erkennung eine Peer-WAE gefunden wurde.

Der Zähler der an den Router gesendeten GRE-Pakete (nicht umgehen) gibt Pakete an, die mit der vom WCCP ausgehandelten Rückgabemethode behandelt wurden.

Die an einen anderen WAE-Zähler gesendeten Pakete weisen darauf hin, dass beim Hinzufügen einer weiteren WAE zur Servicegruppe ein Flow Protection erfolgt und mit der Verarbeitung einer Bucket-Zuweisung beginnt, die zuvor von einer anderen WAE behandelt wurde.

Stellen Sie sicher, dass die zu verwendenden Ausgangs-Methoden die erwarteten sind, indem Sie den Befehl **show ausgress-methods** wie folgt verwenden:

```
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
```

Diskrepanzen zwischen Ausgangsmethoden können unter den folgenden Bedingungen auftreten:

- Die ausgehandelte Rückgabemethode wird konfiguriert, WCCP handelt jedoch die Layer-2-Rückgabemethode aus, und nur die GRE-Rückgabe wird von WAAS unterstützt.
- Die generische GRE-Ausgangs-Methode ist konfiguriert, aber die Abfangmethode ist Layer 2, und nur WCCP GRE wird als Abfangmethode unterstützt, wenn ein generischer GRE-Ausgang konfiguriert wird.

In beiden Fällen wird ein kleinerer Alarm ausgelöst, der gelöscht wird, wenn die Nichtübereinstimmung durch Ändern der Ausgangs- oder WCCP-Konfiguration behoben wird. Bis der Alarm gelöscht ist, wird die IP-Weiterleitungs-Ausgangs-Standardmethode verwendet.

Im folgenden Beispiel wird die Befehlsausgabe bei einer Nichtübereinstimmung veranschaulicht:

```
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.
```

Für Catalyst 6500 Sup720- oder Sup32-Router wird die Verwendung der generischen GRE-Ausgangsmethode empfohlen, die in der Hardware verarbeitet wird. Darüber hinaus empfehlen wir die Verwendung eines Multipoint-Tunnels, um die Konfiguration zu vereinfachen, anstatt eines Point-to-Point-Tunnels für jede WAE. Einzelheiten zur Tunnelkonfiguration finden Sie im Abschnitt Konfigurieren einer GRE-Tunnelschnittstelle auf einem Router im *Konfigurationsleitfaden für Cisco Wide Area Application Services*.

Um die GRE-Tunnelstatistiken für jeden Intercepting-Router anzuzeigen, verwenden Sie den Befehl **show statistics allgemein-gre**:

```
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
```

Wenn nicht sichergestellt wird, dass ausgehende Pakete von einer WAE nicht abgefangen werden, kann dies zu einer Umleitungsschleife führen. Wenn eine WAE eine eigene ID erkennt, die im Feld "TCP options" (TCP-Optionen) zurückgegeben wird, ist eine Umleitungsschleife aufgetreten, die folgende Syslog-Meldung ergibt:

```
%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.
```

Sie können die Datei syslog.txt nach Instanzen dieses Fehlers suchen, indem Sie den Befehl **Find** wie folgt verwenden:

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

Dieser Fehler wird auch in den TFO-Flussstatistiken angezeigt, die im Befehl zum **Filtern** von Statistiken verfügbar sind:

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

Wenn Sie auf dem Router eine Umleitung für ausgehenden Datenverkehr durchführen, wird der Router beim Verlassen des Routers an die WAE umgeleitet, wodurch das Paket an den Router umgeleitet wird, was eine Routing-Schleife verursacht. Wenn sich die WAE und die Server im Rechenzentrum in unterschiedlichen VLANs befinden und die WAE in der Außenstelle und die Clients sich in unterschiedlichen VLANs befinden, können Sie eine Routing-Schleife vermeiden, indem Sie die folgende Router-Konfiguration im WAE-VLAN verwenden:

```
ip wccp redirect exclude in
```

Wenn die WAE dasselbe VLAN mit den benachbarten Clients oder Servern gemeinsam nutzt, können Sie Routing-Schleifen mithilfe der Negotiated-Return-Methode vermeiden oder generische GRE-Rückgabe für Plattformen, bei denen die WCCP-Umleitung in der Hardware durchgeführt wird. Bei der Verwendung einer generischen GRE-Rückgabe verwendet die WAE einen GRE-Tunnel, um den Datenverkehr an den Router zurückzugeben.

Fehlerbehebung: Konfigurierbare Service-IDs und variable Timeouts in Version 4.4.1

HINWEIS: In WAAS Version 4.4.1 wurden die konfigurierbaren WCCP-Dienst-IDs und die Zeitüberschreitungsfunktionen für die variable Fehlererkennung eingeführt. Dieser Abschnitt gilt nicht für frühere WAAS-Versionen.

Alle WAEs in einer WCCP-Farm müssen dasselbe Paar WCCP-Dienst-IDs verwenden (der Standardwert ist 61 und 62), und diese IDs müssen mit allen Routern übereinstimmen, die die Farm unterstützen. Eine WAE mit anderen WCCP-Dienst-IDs als die auf den Routern konfigurierten darf der Farm nicht beitreten, und der bestehende Alarm "Router Unreachable" (Router nicht erreichbar) wird ausgelöst. Ebenso müssen alle WAEs in einer Farm den gleichen Wert für das Timeout bei der Fehlererkennung verwenden. Eine WAE löst einen Alarm aus, wenn Sie ihn mit einem falsch übereinstimmenden Wert konfigurieren.

Wenn Sie einen Alarm sehen, dass eine WAE nicht in der Lage ist, einer WCCP-Farm beizutreten, überprüfen Sie, ob die auf der WAE konfigurierten WCCP-Dienst-IDs und die Router in der Farm übereinstimmen. Verwenden Sie auf den WAEs den Befehl **show wccp wide-area-engine**, um die konfigurierten Service-IDs zu überprüfen. Auf den Routern können Sie den Befehl **show ip wccp** IOS verwenden.

Um zu überprüfen, ob die WAE eine Verbindung zum Router hat, verwenden Sie die **Option show wccp services detail** und **show wccp router detail** befehle.

Darüber hinaus können Sie die WCCP-Debugausgabe auf der WAE mithilfe der Befehle **debug ip wccp event** oder **debug ip wccp packet** aktivieren.

Wenn Sie einen "Router Unusable"-Alarm für eine WAE sehen, kann dies bedeuten, dass der auf der WAE festgelegte Zeitüberschreitungswert für die variable Fehlererkennung vom Router nicht unterstützt wird. Mit dem Befehl **show alarm minor detail** können Sie überprüfen, ob der Grund für den Alarm "Timer interval inmatch with router" lautet:

```
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                                                                 <-----
```

Überprüfen Sie auf der WAE das konfigurierte Timeout für die Fehlererkennung wie folgt:

```
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
. . .
```

Überprüfen Sie auf dem Router, ob die IOS-Version das Timeout für die Erkennung variabler Ausfälle unterstützt. Wenn dies der Fall ist, können Sie die konfigurierte Einstellung mit dem Befehl **show ip wccp *xx* detail** überprüfen, wobei *xx* die WCCP-Dienst-ID ist. Es gibt drei mögliche Ergebnisse:

- Die WAE verwendet ein Standard-Timeout von 30 Sekunden für die Fehlererkennung, und der Router ist gleich konfiguriert oder unterstützt kein variables Timeout: Die Ausgabe des Routers enthält keine Details zur Timeout-Einstellung. Diese Konfiguration funktioniert einwandfrei.
- WAE verwendet ein Timeout von 9 oder 15 Sekunden, das nicht der Standardausfallerkennung entspricht, und der Router unterstützt kein variables Timeout: Das Statusfeld zeigt "NICHT verwendbar" an, und die WAE kann den Router nicht verwenden. Ändern Sie das WAE-Timeout mithilfe des globalen Konfigurationsbefehls **wccp tcp failure-detect 30** in den Standardwert von 30 Sekunden.
- Die WAE verwendet ein Timeout von 9 oder 15 Sekunden, das nicht der Standardausfallerkennung entspricht, und der Router unterstützt ein variables Timeout: Das Client-Timeout-Feld zeigt das konfigurierte Timeout für die Fehlererkennung an, das mit der WAE übereinstimmt. Diese Konfiguration funktioniert einwandfrei.

Wenn die WCCP-Farm aufgrund von Flapping-Verbindungen instabil ist, könnte dies daran liegen, dass das Timeout für die Erkennung von WCCP-Ausfällen zu niedrig ist.