WAAS - WCCP故障排除

章节：排除WCCP故障

本文介绍如何排除WCCP问题。

目录

以下症状表示可能的WCCP问题：

- WAE未接收流量（可能是由于WCCP配置错误）
- 最终用户无法访问其服务器应用（可能是由于流量黑洞）
- 启用WCCP时网络速度变慢（可能是由于路由器丢弃数据包或路由器CPU使用率较高）
- 路由器CPU使用率过高（可能是由于软件而非硬件中的重定向）

WCCP问题可能是路由器（或重定向设备）或WAE设备问题导致的。必须查看路由器和WAE设备上的WCCP配置。首先，我们将查看路由器上的WCCP配置，然后检查WAE上的WCCP配置。

排除路由器上的WCCP故障

本节介绍对以下设备的故障排除：

- Catalyst 6500系列交换机、ISR和3700系列路由器
- ASR 1000系列路由器

排除Catalyst 6500系列交换机和ISR和3700系列路由器上的WCCP故障

使用show ip wccp IOS命令，首先检验交换机或路由器上的WCCPv2拦截，**如**下所示：

```
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--
```

在使用基于软件的重定向的平台上，验证上述命令输出中的数据包总数/w重定向计数器是否在增加。在使用基于硬件的重定向的平台上，这些计数器的增量不应太大。如果您看到这些计数器在基于硬件的平台上显着增加，则路由器上的WCCP可能配置错误（默认情况下，WCCP GRE在软件中处理），或者路由器可能因硬件资源问题（如TCAM资源耗尽）而退回到软件重定向。如果您看到这些计数器在基于硬件的平台上增加，这可能导致CPU使用率较高，则需要进行更多调查。

与服务组匹配但与重定向列表不匹配的数据包的Total Packets Denied Redirect计数器递增。

Total Authentication failures计数器对使用错误服务组密码接收的数据包递增。

在软件中执行WCCP重定向的路由器上，继续使用show ip wccp 61 detail IOS命令在路由器上验证WCCPv2侦听，**如下所示：**

```
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
```

验证服务组61中的WAE状态为“可用”。在Hash Allovam字段中，验证是否已将哈希桶分配给WAE。百分比告诉您此WAE处理的哈希桶总数。WAE在服务组中的时间量在连接时间字段中报告。哈希分配方法应与基于软件的重定向一起使用。

在路由器上使用**show ip wccp *service* hash** dst-ip src-ip dst-port src-port hidden IOS命令，可以确定场中的哪个WAE将处理特定请求，如下所示：

```
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
```

在硬件中执行WCCP重定向的路由器上，继续使用show ip wccp 61 detail IOS命令在路由器上验证WCCPv2侦听，**如下所示：**

```
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)
```

您希望看到能够进行硬件重定向的路由器的掩码分配方法。

为了在路由器上保存TCAM资源，请考虑更改默认WCCP掩码以适应您的网络环境。请考虑以下建议：

- 使用WCCP重定向ACL时，使用尽可能少的掩码位数。与重定向ACL结合使用时，掩码位数越

少，TCAM利用率越低。如果集群中有1-2个WCCP客户端，请使用一位。如果有3-4个WCCP客户端，请使用2位。如果有5-8个WCCP客户端，则使用3位等。
- 我们不建议使用WAAS默认掩码(0x1741)。 对于数据中心部署，目标是将分支机构站点负载均衡到数据中心，而不是客户端或主机。正确的掩码将数据中心WAE对等最小化，从而扩展存储。例如，对于具有/24分支网络的零售数据中心，使用0x100到0x7F00。对于每个企业/16的大型企业，使用0x10000到0x7F0000将企业负载均衡到企业数据中心。在分支机构中，目标是平衡通过DHCP获取其IP地址的客户端。DHCP通常会发出客户端IP地址，从子网中最低的IP地址递增。要使DHCP分配的IP地址与掩码达到最佳平衡，请使用0x1到0x7F仅考虑客户端IP地址的最低位，以实现最佳分配。

WCCP重定向访问列表使用的TCAM资源是该ACL内容与已配置的WCCP位掩码相乘的乘积。因此，WCCP桶数（根据掩码创建）与重定向ACL中的条目数之间存在争用。例如，掩码0xF（4位）和200行重定向允许ACL可能会产生3200(2^4 x 200)个TCAM条目。将掩码减小到0x7（3位）可将TCAM使用率降低50%(2^3 x 200 = 1600)。

Catalyst 6500系列和Cisco 7600系列平台能够在软件和硬件中处理WCCP重定向。如果数据包在软件中无意中被重定向，当您预期硬件重定向时，可能会导致路由器CPU使用率过高。

您可以检查TCAM信息，以确定在软件还是硬件中处理重定向。使用**show tcam** IOS命**令，如下所示：**

```
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”匹配表示未在硬件中处理的请求。此情况可能由以下错误引起：

- 哈希分配而非掩码
- 出站重定向，而非入站
- 重定向排除
- 未知WAE MAC地址
- 为通用GRE隧道目标使用环回地址

在以下示例中，策略路由条目显示路由器正在执行完全硬件重定向：

```
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)
```

来自WAE的Here I Am(HIA)必须进入与WAE MAC通过的接口相同的接口。我们建议您在WAE路由器列表中使用环回接口，而不是直连接口。

排除ASR 1000系列路由器上的WCCP故障

Cisco ASR 1000系列路由器上排除WCCP故障的命令与其他路由器不同。本部分显示可用于获取ASR 1000上WCCP信息的命令。

要显示路由处理器WCCP信息，请按如**下方式使用show platform software wccp rp** active命令：

```
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
```

以下示例显示可用于检查转发处理器信息的其他命令：

```
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>
```

要显示每个接口的重定向数据包统计信息，请使用**show platform software wccp interface counters命令**，如下所示：

```
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
```

使用show platform software wccp web-cache counters**命令显示WCCP缓存信息，**如下所示：

```
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
```

要显示低级详细信息，请使用以下命令：

- **show platform so interface F0 brief**
- **show platform software wccp f0 interface**
- **debug platform software wccp configuration**

有关详细信息，请参阅白皮书[“在Cisco ASR 1000系列聚合服务路由器上部署Web缓存控制协议第2版并进行故障排除”]

排除WAE上的WCCP故障

使用show wccp services命令开始对WAE进**行故障**排除。您希望看到服务61和62都已配置，如下所示：

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

接下来，使用show wccp status命令检**查WCCP状**态。您希望看到WCCP第2版已启用并处于活动状态，如下所示：

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

使用show wccp wide-area-engine命令查**看WCCP场信**息。此命令显示场中WAE的数量、其IP地址（其中一个是主WAE）、可查看WAE的路由器以及其他信息，如下所示：

```
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
. . .
```

使用show wccp routers命令查看**路由器信**息。验证是否与启用WCCP的路由器存在双向通信，且所有路由器显示相同的KeyIP和KeyCN（更改号），如下所示：

```
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-
. . .
```

如果WAE与路由器不相邻于第2层，或者使用环回地址，则需要静态路由或默认网关来支持WCCP。

要检查服务组中的哈希桶分布，请使用**show wccp flows tcp-promiscuous**命令，如下所示：

```
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
```

或者，您可以使用命令的摘要版本查看类似信息以及旁路流信息：

```
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: .......... ......
. . .
```

使用show wccp gre命令显示GRE数据包统计信息，如下所示：

```
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--
```

如果WCCP重定向正在工作，前两个计数器中的任何一个应递增。

对于使用WCCP第2层重定向转发方法重定向的数据包，透明非GRE数据包收到的计数器增加。

透明非GRE非WCCP数据包收到由非WCCP侦听方法（如ACE或PBR）重定向的数据包的计数器增量。

Total packets accepted计数器指示由于自动发现找到对等WAE而被接受以进行优化的数据包。

发送到路由器（非旁路）计数器的GRE数据包指示使用WCCP协商的返回出口方法处理的数据包。

发送到另一个WAE计数器的数据包表示当另一个WAE添加到服务组并开始处理之前由另一个WAE处理的桶分配时，会发生流保护。

使用以下show egress-methods命令，验证正在使用的出口方法是**预期的方法**:

```
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
```

出口方法不匹配可能在以下条件下发生：

- 协商的返回出口方法已配置，但WCCP会协商第2层返回方法，并且WAAS仅支持GRE返回。
- 已配置通用GRE出口方法，但侦听方法为第2层，并且当配置通用GRE出口时，仅支持WCCP GRE作为侦听方法。

在这两种情况中，当通过更改出口方法或WCCP配置解决不匹配问题时，会发出轻微警报并清除。在清除警报之前，使用默认IP转发出口方法。

以下示例显示存在不匹配时的命令输出：

```
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.
```

对于Catalyst 6500 Sup720或Sup32路由器，我们建议使用通用GRE出口方法，该方法在硬件中处理。此外，我们建议使用一个多点隧道来简化配置，而不是每个WAE使用一个点对点隧道。有关隧道配置详细信息，请参阅《Cisco Wide Area Application Services配置指南》中的在路由器上*配置GRE隧道接口一节*。

要查看每个拦截路由器的GRE隧道统计信息，请使用**show statistics generic-gre命**令，如下所示：

```
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
```

如果无法确保来自WAE的出口数据包不会被重新拦截，则可能导致重定向环路。如果WAE在TCP选项字段中检测到自己返回的ID，则会发生重定向环路并导致以下系统日志消息：

```
%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.
```

使用以下查找命令，可以搜索syslog.txt文件以查找此错**误的**实例：

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

此错误还显示在show statistics filtering命令中可用的TFO流统**计信息中**，如下所示：

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

如果您在路由器上执行出站重定向，当流量离开路由器时，它将被重定向回WAE，WAE会将数据包重新路由到路由器之外，从而导致路由环路。如果数据中心WAE和服务器位于不同的VLAN上，而分支WAE和客户端位于不同的VLAN上，则可以在WAE VLAN上使用以下路由器配置来避免路由环路：

```
ip wccp redirect exclude in
```

如果WAE与其相邻客户端或服务器共享相同的VLAN，则可以使用协商返回方法或在硬件中执行WCCP重定向的平台的通用GRE返回来避免路由环路。当使用通用GRE返回时，WAE使用GRE隧道将流量返回到路由器。

4.4.1版中可配置服务ID和变量超时故障排除

NOTE:WAAS版本4.4.1中引入了WCCP可配置服务ID和变量故障检测超时功能。本部分不适用于早期的WAAS版本。

WCCP场中的所有WAE必须使用相同的一对WCCP服务ID（默认为61和62），并且这些ID必须与支持该场的所有路由器匹配。与路由器上配置的WCCP服务ID不同的WAE不允许加入场，并且会引发现有的"路由器不可达"警报。同样，场中的所有WAE必须对故障检测超时使用相同的值。如果您为WAE配置了不匹配的值，WAE会发出警报。

如果您看到WAE无法加入WCCP场的警报，请检查WAE上配置的WCCP服务ID与场中的路由器是否匹配。在WAE上，使用**show wccp wide-area-engine**命令检查已配置的服务ID。在路由器上，可以使用**show ip wccp** IOS命令。

要检查WAE是否与路由器连接，请使用**show wccp services detail和**show wccp router detail**命令**。

此外，您还可以使用debug ip wccp event或debug ip wccp packet命**令在WAE上启**用WCCP**调试**输出。

如果您看到WAE的"路由器不可用"小警报，可能意味着路由器不支持在WAE上设置的变量故障检测超时值。使用**show alarm minor detail**命令检查警报的原因是否为"Timer interval mismatch with router"：

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

在WAE上，按如下方式检查配置的故障检测超时：

```
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
. . .
```

在路由器上，检查IOS版本是否支持变量故障检测超时。如果是，您可以使用**show ip wccp *xx* detail**命令检查配置的设置，其中*xx* 是WCCP服务ID。有三种可能的结果：

- WAE使用默认故障检测超时30秒，路由器配置相同或不支持变量超时：路由器输出不显示有关超时设置的详细信息。此配置运行正常。
- WAE使用9或15秒的非默认故障检测超时，并且路由器不支持变量超时：状态字段显示“不可用”，WAE无法使用路由器。使用wccp tcp failure-detection 30全局配置命令，将WAE故障检测超时更**改为默认值30**秒。
- WAE使用9或15秒的非默认故障检测超时，并且路由器支持可变超时：客户端超时字段显示已配置的故障检测超时，与WAE匹配。此配置运行正常。

如果WCCP场因链路抖动而不稳定，则可能是因为WCCP故障检测超时过低。