Cisco版本的4.1.3 WAAS故障排除指南及以后

章节：排除WCCP故障

此条款描述如何排除WCCP问题故障。

指南

主要
了解
初步
排除
排除
排除
排除
排除
排除
排除
排除
排除
排除
排除
排除
排除
排除
排除
排除
排除
排除
排除

Contents

- 1排除在路由器的WCCP故障
  - 1.1排除在Catalyst 6500 Series Switches的WCCP故障和ISR和3700系列路由器
  - 1.2排除在ASR 1000系列路由器的WCCP故障
- 2排除在WAE的WCCP故障
- 3个排除可配置服务ID和可变的超时故障在版本4.4.1

以下症状指示可能的WCCP问题：

- WAE不收到数据流(可能归结于WCCP误配置)
- 终端用户不能到达他们的服务器应用(可能归结于陷入黑洞数据流)
- 网络缓慢，当WCCP是启用的(时可能归结于下降信息包或高路由器CPU使用方法)的路由器
- 过度地高路由器CPU使用方法(可能归结于在软件的重定向而不是硬件)

WCCP问题能起因于从关于路由器(或重定向设备的)问题或WAE设备。查看WCCP配置在路由器和在WAE设备是必要的。首先我们将查看在路由器的WCCP配置，然后我们将检查在WAE的WCCP配置。

排除在路由器的WCCP故障

此部分包括排除故障在以下设备：

- Catalyst 6500 Series Switches和ISR和3700系列路由器
- ASR 1000系列路由器

排除在Catalyst 6500 Series Switches的WCCP故障和ISR和3700系列路由器

排除故障通过验证的Begin在交换机或路由器的WCCPv2拦截通过使用**show ip wccp** ios命令如下：

```
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，请验证信息包总数s/w重定向的计数器在上述命令输出中增加。在使用基于硬件的重定向的平台上，这些计数器不应该增加。如果看到这些计数器在基于硬件的平台极大增加， WCCP在路由器可能被不正确配置(默认情况下WCCP GRE在软件被处理)，或者路由器可能落回到软件重定向由于硬件资源问题例如用尽TCAM资源。需要更多调查是否看到这些计数器增加在一个基于硬件的平台，可能导致高CPU使用方法。

被拒绝的信息包总数重定向计数器为匹配服务组的信息包增加，但是不匹配重定向列表。

总认证失败抵抗带着不正确服务组密码被接收的信息包的增量。

通过使用**show ip wccp 61详细资料**ios命令如下，在WCCP重定向在软件执行的路由器上，请通过验证WCCPv2拦截继续在路由器：

```
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
```

验证在服务组61的WAE状态是可用的。验证哈希桶分配到在哈希分配字段的WAE。百分比告诉您多少总哈希桶由此WAE处理。时间WAE在服务组在连接时间字段报告。哈希分配方法应该与基于软件的重定向一起使用。

您能确定哪些WAE在组群将处理一个特定的请求通过使用show ip wccp*服务*哈希dst *IP src IP dst端口src端口*被隐藏的ios命令在路由器如下：

```
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
```

通过使用show ip wccp 61详细资料ios命令如下，在WCCP重定向在硬件里执行的路由器上，请通过验证WCCPv2拦截继续在路由器：

```
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)
```

您要为有能力在硬件重定向上的路由器发现掩码分配方法。

为了节约TCAM资源在路由器，请考虑修改默认WCCP掩码配合您的网络环境。考虑这些推荐：

- 当曾经WCCP重定向ACL时，请使用的掩码位小数量可能。掩码位的一个更小的编号，当使用与重定向ACL一道导致更低的TCAM利用率。如果有簇的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，则请使用3位等等。
- 我们不推荐使用WAAS默认掩码(0x1741)。对于数据中心配置，目标是装载平衡分支机构站点到数据中心而不是客户端或主机。正确的掩码使数据中心WAE同位体减到最小并且扩展存贮。例如，请使用0x100对0x7F00有/24分支机构网络的零售数据中心。对于与/16的大企业每个事务，请使用0x10000对0x7F0000装载平衡企业到企业数据中心。在分支机构，目标是平衡通过DHCP获得他们的IP地址的客户端。DHCP通常发出增加从在子网的最低的IP地址的客户端IP地址。对最佳的平衡DHCP与掩码的指定的IP地址，使用0x1对0x7F只考虑客户端IP地址的最低位达到最佳的分配。

WCCP重定向访问列表浪费的TCAM资源是该ACL内容的产品被倍增被配置的WCCP位掩码。所以，有在数量的争用的根据掩码被创建)的WCCP桶之间(和条目的数量在重定向ACL的。例如， 0xF (4位)和第200行重定向许可证ACL掩码可能导致3200年(2^4 x 200) TCAM条目。使掩码降低到0x7 (3位)减少TCAM使用方法50% (2^3 x 200 = 1600)。

Catalyst 6500 series和Cisco 7600系列平台能够处理WCCP重定向在软件和硬件方面。如果信息包在软件疏忽地重定向，当您期待硬件重定向时，可能导致过度地高路由器CPU使用。

您能检查TCAM信息确定重定向是否在软件或硬件里被处理。请使用**show tcam** ios命令如下：

```
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
```

“平底船”匹配表示在硬件里没处理的请求。此情况能由以下错误造成：

- 而不是掩码的哈希分配
- 而不是入站的outbound重定向
- 重定向排除
- 未知WAE MAC地址
- 使用通用的GRE隧道目的地的一个环回地址

在以下示例中，路由条目表示，路由器执行充分的硬件重定向：

```
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)
```

这里我在(HIA)从WAE必须进入同一个接口WAE MAC通过知道。我们建议您在WAE路由器列表使用一个环回接口而不是一个直接地连接的接口。

排除在ASR 1000系列路由器的WCCP故障

排除的WCCP故障命令在Cisco ASR 1000系列路由器是与其他路由器不同。此部分表示命令，您能使用获得关于ASR 1000的WCCP信息。

要显示路由处理器WCCP信息，请使用**显示平台软件WCCP RP活动**命令如下：

```
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
```

以下示例表示其它命令，您能使用检查转发处理器信息：

```
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>
```

要显示重定向每个接口的信息包统计数据，使用**显示平台软件WCCP接口计数器**命令如下：

```
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
```

请使用**显示平台软件wccp网站缓存**计数器命令显示WCCP缓存信息如下：

```
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
```

要显示低级详细资料，请使用以下命令：

- **如此显示平台接口F0摘要**
- **显示平台软件WCCP f0接口**
- **调试平台软件WCCP配置**

欲知更多信息，请参阅白皮书[“配置和排除在Cisco ASR 1000系列汇聚服务路由器的WEB缓存控制协议版本2故障”]

排除在WAE的WCCP故障

排除故障在WAE的Begin通过使用**show wccp services**命令。您要发现两服务被配置的61和62，如下：

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

下检查通过使用**show wccp status**命令的WCCP状态。您要发现WCCP版本2启用和活动如下：

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

通过使用**显示WCCP宽区域引擎**命令，查看WCCP农厂信息。此命令在组群显示WAEs的编号，他们的IP地址，哪个是能看到WAEs的lead WAE，路由器和其他信息，如下：

```
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
. . .
```

通过使用**show wccp routers**命令，查看路由器信息。验证有双向通信用支持WCCP的路由器，并且所有路由器显示同样KeyIP和KeyCN (更改编号)，如下：

```
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-
. . .
```

在WAE不是处2相邻与路由器或者使用环回地址，静态路由或默认网关要求层支持WCCP。

要检查在服务组的哈希桶分配，请使用**show wccp flows TCP混乱**命令如下：

```
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，您能使用命令的概略的版本发现相似的信息，以及漏流率信息：

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

请使用**显示WCCP gre**命令显示GRE信息包统计数据如下：

```
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重定向工作，前两个计数器之一应该增加。

透明非GRE信息包收到的计数为使用WCCP第2层重定向转发方法，重定向的信息包增加。

透明非GRE非WCCP信息包收到的计数为是用非WCCP拦截方法重定向的信息包增加(例如ACE或PBR)。

信息包总数接受了计数器指示为最优化接受的信息包，因为自动发现查找一个对等体WAE。

对路由器(不是旁路)计数器的GRE发送的数据包指示使用WCCP协商的回归出口方法，被处理的信息包。

对另一个WAE计数器的发送的数据包表明流保护发生，当另一个WAE被添加到服务组并且开始处理由另一个WAE以前处理的桶分配时。

验证使用的出口方法是期待的部分通过使用**显示出口方法**命令如下：

```
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
```

出口方法不匹配能在以下条件下发生：

- 配置协商的回归出口方法，但是WCCP协商第2层回归方法，并且WAAS支持仅GRE回归。
- 配置通用的GRE出口方法，但是拦截方法是第2层，并且仅WCCP GRE支持作为拦截方法，当配置时通用的GRE出口。

在这些案件之一，一个次要告警发出和被清除，当更改出口方法或WCCP配置解决时不匹配。直到清除警报，使用默认IP转发出口方法。

当不匹配存在时，以下示例显示命令输出：

```
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，我们推荐使用通用的GRE出口方法，在硬件方面被处理。另外，我们推荐使用一条多点隧道配置方便，而不是每个WAE的一个点到点隧道。关于隧道配置详细资料，请参见配置在一个路由器的部分一个GRE隧道接口在*Cisco广域应用服务配置指南*。

要查看每个拦截的路由器的GRE封装隧道统计数据，请使用**show statistics通用的gre**命令如下：

```
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
```

疏忽保证自WAE的出口信息包没有reintercepted可能导致重定向循环。如果WAE发现在TCP选项域返回的其自己的ID，重定向循环出现并且导致以下系统消息：

```
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
```

通过使用**find命令**如下，您能搜索syslog.txt文件此错误实例：

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

此错误在TFO也出现流统计数据可用在**过滤**命令的**show statistics**如下：

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

如果执行在路由器的outbound重定向，因为数据流离开路由器将重新定向回到WAE，将重路由信息包路由器，引起路由循环。如果数据中心WAE和服务器在不同的VLAN，并且分组WAE和客户端在不同的VLAN，您能避免路由循环通过使用在WAE VLAN的下列路由器配置：

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

如果WAE与其相邻客户端或服务器共享同样VLAN，通过使用协商的回归方法，您能避免路由循环或者WCCP重定向在硬件里执行的平台的通用的GRE回归。当曾经通用的GRE回归时， WAE使用一个GRE封装隧道对回程数据流到路由器。

排除可配置服务ID和可变的超时故障在版本4.4.1

NOTE:WCCP可配置服务ID和可变的故障检测超时功能在WAAS版本4.4.1被介绍了。此部分不是可适用的对初期的WAAS版本。

所有WAEs在WCCP组群必须使用同一个对WCCP服务ID (默认值是61和62)，并且这些ID必须匹配支持组群的所有路由器。用不同的WCCP服务ID的WAE比在路由器配置的那些没有允许加入组群，并且现有的“路由器不可得到的”警报发出。同样，所有WAEs在组群必须使用同一值故障检测超时。如果用配错的值，配置它WAE发出警报。

如果看到警报WAE不能加入WCCP组群，请检查在WAE和路由器配置的WCCP服务ID在组群配比。在WAEs，请使用**显示WCCP宽区域引擎**命令检查配置的服务ID。在路由器上，您能使用ios命令的**show ip wccp**。

要检查WAE是否有连接到路由器，请使用**show wccp services详细资料**并且**显示WCCP路由器详细资料**命令。

另外，通过使用**debug ip WCCP事件**或**debug ip WCCP**信息包命令，您能enable (event) WCCP在WAE的调试输出。

如果为WAE看到“路由器不可用的”次要告警，可能意味着路由器不支持在WAE的可变的故障检测超时值集。请使用**显示警报较小detail命令**检查警报的原因是否是“计时器间隔不匹配用路由器”：

```
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，请检查被配置的故障检测超时如下：

```
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，请检查IOS版本是否支持可变的故障检测超时。如果那样，您能检查被配置的设置通过使用**show ip wccp *xx* detail命令**，其中*xx*是WCCP服务ID。有三个可能的结果：

- WAE使用默认30秒故障检测超时，并且配置路由器同样或不支持可变的超时：路由器输出不显示关于超时设置的详细资料。此配置优良运行。
- WAE使用9或15秒非默认故障检测超时，并且路由器不支持可变的超时：State字段显示“不可用”和WAE不能使用路由器。通过使用**WCCP tcp故障检测30**全局配置命令，更改WAE故障检测超时到DEFAULT值30秒。
- WAE使用9或15秒非默认故障检测超时，并且路由器支持可变的超时：客户端超时字段显示被配置的故障检测超时，匹配WAE。此配置优良运行。

如果WCCP组群不稳定归结于链路飘荡，可能这是因为WCCP故障检测超时是太低的。