This article describes how to troubleshoot WCCP issues.

Guide Contents
Main Article
Understanding the WAAS Architecture and Traffic Flow
Preliminary WAAS Troubleshooting
Troubleshooting Optimization
Troubleshooting Application Acceleration
Troubleshooting the CIFS AO
Troubleshooting the HTTP AO
Troubleshooting the EPM AO
Troubleshooting the MAPI AO
Troubleshooting the NFS AO
Troubleshooting the SSL AO
Troubleshooting the Video AO
Troubleshooting the Generic AO
Troubleshooting Overload Conditions
Troubleshooting WCCP
Troubleshooting AppNav
Troubleshooting Disk and Hardware Problems
Troubleshooting Serial Inline Clusters
Troubleshooting vWAAS
Troubleshooting WAAS Express
Troubleshooting NAM Integration

Contents

The following symptoms indicate possible WCCP issues:

- The WAE is not receiving traffic (could be due to WCCP misconfiguration)
- End users cannot reach their server applications (could be due to blackholing of traffic)
- Network slowness when WCCP is enabled (could be due to router dropping packets or high router CPU usage)
- Overly high router CPU usage (could be due to redirection in software instead of hardware)

WCCP issues can result from problems with the router (or redirecting device) or from the WAE device. It is necessary to look at the WCCP configuration both on the router and on the WAE device. First we will look at the WCCP configuration on the router, then we will check the WCCP configuration on the WAE.

Troubleshooting WCCP on the Router

This section covers troubleshooting on the following devices:

- Catalyst 6500 Series Switches and the ISR and 3700 Series Routers
- ASR 1000 Series Routers

Troubleshooting WCCP on the Catalyst 6500 Series Switches and the ISR and 3700 Series Routers

Begin troubleshooting by verifying WCCPv2 interception on the switch or router by using the **show ip wccp** IOS command as follows:

```
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
         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 r
       Total Packets Unassigned:           0
       Group access-list:                  -none-
       Total Messages Denied to Group:     0
       Total Authentication failures:      0                 <-----Packets have incorrect servic
       Total Bypassed Packets Received:    0
--More--
```

On platforms that use software-based redirection, verify that the Total Packets s/w Redirected counters are incrementing in the above command output. On platforms that use hardware-based redirection, these counters should not be incrementing much. If you are seeing these counters increment significantly on hardware-based platforms, WCCP could be misconfigured on the router (WCCP GRE is processed in software by default), or the router could be falling back to software redirection due to hardware resources issues such as running out of TCAM resources. More investigation is required if you see these counters incrementing on a hardware-based platform, which could lead to high CPU usage.

The Total Packets Denied Redirect counter increments for packets that match the service group but do not match the redirect list.

The Total Authentication failures counter increments for packets that are received with the incorrect service group password.

On routers where WCCP redirection is performed in the software, continue by verifying WCCPv2 interception on the router by using the **show ip wccp 61 detail** IOS command as follows:

```
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 th
       Packets s/w Redirected:  2452
       Connect Time:            01:19:46                                <-----Time WAE has been in
       Bypassed Packets
         Process:               0
         Fast:                  0
         CEF:                   0
```

Verify that the WAE state in the service group 61 is Usable. Verify that hash buckets are assigned to the WAE in the Hash Allotment field. The percentage tells you how many of the total hash buckets are handled by this WAE. The amount of time that the WAE has been in the service group is reported in the Connect Time field. The hash assignment method should be used with software-based redirection.

You can determine which WAE in the farm will handle a particular request by using the **show ip wccp** ***service*** **hash** ***dst-ip src-ip dst-port src-port*** hidden IOS command on the router as follows:

```
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
```

On routers where WCCP redirection is performed in the hardware, continue by verifying WCCPv2 interception on the router by using the **show ip wccp 61 detail** IOS command as follows:

```
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 platf
   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)
```

You want to see the Mask assignment method for routers that are capable of hardware redirection.

In order to save TCAM resources on the router, consider altering the default WCCP mask to suit your network environment. Consider these recommendations:

- Use the smallest number of mask bits possible when using WCCP redirect ACL. A smaller number of mask bits when used in conjunction with Redirect ACL results in lower TCAM utilization. If there are 1-2 WCCP clients in a cluster, use one bit. If there are 3-4 WCCP clients, use 2 bits. If there are 5-8 WCCP clients, then use 3 bits and so on.
- We do not recommend using the WAAS default mask (0x1741). For data center deployments, the goal is to load balance the branch sites into the data center rather than clients or hosts. The right mask minimizes data center WAE peering and hence scales storage. For example, use 0x100 to 0x7F00 for retail data centers that have /24 branch networks. For large enterprises with a /16 per business, use 0x10000 to 0x7F0000 to load balance the businesses into the enterprise data center. In the branch office, the goal is to balance the clients that obtain their IP addresses via DHCP. DHCP generally issues client IP addresses incrementing from the lowest IP address in the subnet. To best balance DHCP assigned IP addresses with mask, use 0x1 to 0x7F to only consider the lowest order bits of the client IP address to achieve the best distribution.

The TCAM resources consumed by a WCCP redirect access-list is a product of the content of that ACL multiplied against the configured WCCP bit mask. Therefore, there is contention between the number of WCCP buckets (which are created based on the mask) and the number of entries in the redirect ACL. For example, a mask of 0xF (4 bits) and a 200 line redirect permit ACL may result in 3200 (2^4 x 200) TCAM entries. Reducing the mask to 0x7 (3 bits) reduces the TCAM usage by 50% (2^3 x 200 = 1600).

Catalyst 6500 series and Cisco 7600 series platforms are capable of handling WCCP redirection in both the software and hardware. If packets are inadvertently being redirected in software, when you expect hardware redirection, it could result in overly high router CPU use.

You can inspect the TCAM information to determine if redirection is being handled in the software or the hardware. Use the **show tcam** IOS command as follows:

```
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" matches represent requests not handled in the hardware. This situation could be caused by the following errors:

- Hash assignment instead of mask
- Outbound redirection instead of inbound
- Redirect exclude in
- Unknown WAE MAC address
- Using a loopback address for the generic GRE tunnel destination

In the following example, the policy-route entries show that the router is doing full hardware redirection:

```
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 hard
   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)
```

The Here I Am (HIA) from the WAE must enter the same interface that the WAE MAC is known through. We recommend that you use a loopback interface and not a directly connected interface in the WAE router list.

Troubleshooting WCCP on the ASR 1000 Series Routers

The commands for troubleshooting WCCP on the Cisco ASR 1000 Series routers are different from the other routers. This section shows commands that you can use to get WCCP information on the ASR 1000.

To display route processor WCCP information, use the **show platform software wccp rp active** commands as follows:

```
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 retur
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
```

The following example shows additional commands that you can use to examine forwarding processor information:

```
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>
```

To display redirected packet statistics for each interface, use the **show platform software wccp interface**

counters command as follows:

```
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
```

Use the **show platform software wccp web-cache counters** command to display WCCP cache information as follows:

```
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
```

To display low level details, use the following commands:

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

For more information, see the white paper "Deploying and Troubleshooting Web Cache Control Protocol Version 2 on Cisco ASR 1000 Series Aggregation Services Routers"

Troubleshooting WCCP on the WAE

Begin troubleshooting on the WAE by using the **show wccp services** command. You want to see both services 61 and 62 configured, as follows:

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

Next check the WCCP status by using the **show wccp status** command. You want to see that WCCP version 2 is enabled and active as follows:

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

Look at the WCCP farm information by using the **show wccp wide-area-engine** command. This command shows the number of WAEs in the farm, their IP addresses, which one is the lead WAE, routers that can see the WAEs, and other information, as follows:

```
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
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
. . .
```

Look at the router information by using the **show wccp routers** command. Verify that there is bidirectional communication with WCCP-enabled routers and all routers show the same KeyIP and KeyCN (change number), as follows:

```
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
       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 cases where the WAE is not Layer 2-adjacent to the router, or a loopback address is used, either static routes or a default gateway is required to support WCCP.

To examine the hash bucket distribution in the service group, use the **show wccp flows tcp-promiscuous** command as follows:

```
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
```

Alternatively, you can use the summary version of the command to see similar information, as well as bypass flow information:

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

Use the **show wccp gre** command to display GRE packet statistics as follows:

```
WAE-612# show wccp gre
Transparent GRE packets received:              5531561         <-----Increments for WCCP GRE redir
Transparent non-GRE packets received:          0               <-----Increments for WCCP L2 redire
Transparent non-GRE non-WCCP packets received: 0               <-----Increments for ACE or PBR red
Total packets accepted:                        5051            <-----Accepted for optimization; pe
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
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--
```

If WCCP redirection is working, either of the first two counters should be incrementing.

The Transparent non-GRE packets received counter increments for packets that are redirected using the WCCP Layer 2 redirect forwarding method.

The Transparent non-GRE non-WCCP packets received counter increments for packets that are redirected by a non-WCCP interception method (such as ACE or PBR).

The Total packets accepted counter indicates packets that are accepted for optimization because auto-discovery found a peer WAE.

The GRE packets sent to router (not bypass) counter indicates packets that were handled using the WCCP negotiated return egress method.

The packets sent to another WAE counter indicates that flow protection is occurring when another WAE is added to the service group and begins handling a bucket assignment that was previously being handled by another WAE.

Verify that the egress methods that are being used are the expected ones by using the **show egress-methods** command as follows:

```
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
```

Egress method mismatches can occur under the following conditions:

- The negotiated return egress method is configured, but WCCP negotiates the Layer 2 return method and only GRE return is supported by WAAS.
- The generic GRE egress method is configured, but the interception method is Layer 2 and only WCCP GRE is supported as the interception method when generic GRE egress is configured.

In either of these cases, a minor alarm is raised and is cleared when the mismatch is resolved by changing the egress method or the WCCP configuration. Until the alarm is cleared, the default IP forwarding egress method is used.

The following example shows the command output when a mismatch exists:

```
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 mism
               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 mism
               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.
```

For Catalyst 6500 Sup720 or Sup32 routers, we recommend using the generic GRE egress method, which is processed in hardware. Additionally, we recommend using one multipoint tunnel for ease of configuration, instead of one point-to-point tunnel for each WAE. For tunnel configuration details, refer to the section Configuring a GRE Tunnel Interface on a Router in the *Cisco Wide Area Application Services Configuration Guide*.

To view the GRE tunnel statistics for each intercepting router, use the **show statistics generic-gre** command as follows:

```
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
```

Failure to ensure that egress packets from a WAE are not reintercepted can lead to a redirection loop. If a WAE detects its own ID returned in the TCP options field, a redirection loop has occurred and results in the following syslog message:

```
%WAAS-SYS-3-900000: 137.34.79.11:1192 - 137.34.77.196:139 - opt_syn_rcv: Routing Loop detected - P
```

You can search the syslog.txt file for instances of this error by using the **find** command as follows:

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

This error also shows up in the TFO flow statistics available in the **show statistics filtering** command as follows:

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

If you are doing outbound redirection on the router, as traffic leaves the router it will get redirected back to the WAE, which will reroute the packet out the router, causing a routing loop. If the data center WAE and servers are on different VLANs and the branch WAE and the clients are on different VLANS, you can avoid a routing loop by using the following router configuration on the WAE VLAN:

```
ip wccp redirect exclude in
```

If the WAE shares the same VLAN with its adjacent clients or servers, you can avoid routing loops by using the negotiated return method, or generic GRE return for platforms where WCCP redirection is performed in the hardware. When using generic GRE return, the WAE uses a GRE tunnel to return traffic to the router.

Troubleshooting Configurable Service IDs and Variable Timeouts in Version 4.4.1

NOTE: The WCCP configurable service IDs and variable failure detection timeout features were introduced in WAAS version 4.4.1. This section is not applicable to earlier WAAS versions.

All WAEs in a WCCP farm must use the same pair of WCCP service IDs (the default is 61 and 62), and these IDs must match all routers that are supporting the farm. A WAE with different WCCP service IDs than those configured on the routers is not allowed to join the farm and the existing "Router Unreachable" alarm is raised. Likewise, all WAEs in a farm must use the same value for the failure detection timeout. A WAE raises an alarm if you configure it with a mismatching value.

If you see an alarm that a WAE is not able to join a WCCP farm, check that the WCCP service IDs configured on the WAE and the routers in the farm match. On the WAEs, use the **show wccp wide-area-engine** command to check the configured service IDs. On the routers, you can use the **show ip wccp** IOS command.

To check if the WAE has connectivity to the router, use the **show wccp services detail** and **show wccp router detail** commands.

Additionally, you can enable WCCP debug output on the WAE by using the **debug ip wccp event** or **debug ip wccp packet** commands.

If you see a "Router Unusable" minor alarm for a WAE, it could mean that the variable failure detection timeout value set on the WAE is not supported by the router. Use the **show alarm minor detail** command to check if the reason for the alarm is "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 r
mismatch with router                                                                 <-----
```

On the WAE, check the configured failure detection timeout as follows:

```
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 timec
. . .
```

On the router, check if the IOS version supports variable failure detection timeout. If so, you can check the configured setting by using the **show ip wccp *xx* detail** command, where *xx* is the WCCP service ID. There are three possible results:

- WAE is using default failure detection timeout of 30 seconds and router is configured the same or does not support variable timeout: The router output shows no details about the timeout setting. This configuration operates fine.
- WAE is using non-default failure detection timeout of 9 or 15 seconds and router does not support variable timeout: State field shows "NOT Usable" and the WAE cannot use the router. Change the WAE failure detection timeout to the default value of 30 seconds by using the **wccp tcp failure-detection 30** global configuration command.
- WAE is using non-default failure detection timeout of 9 or 15 seconds and router supports variable timeout: Client timeout field shows the configured failure detection timeout, which matches the WAE. This configuration operates fine.

If the WCCP farm is unstable due to link flapping, it could be because the WCCP failure detection timeout is too low.