WAAS:WCCPのトラブルシューティング

章：WCCPのトラブルシューティング

この記事では、WCCPの問題をトラブルシューティングする方法について説明します。

内容

次の症状は、WCCPの問題の可能性を示しています。

- WAEがトラフィックを受信していない（WCCPの設定ミスが原因である可能性がある）
- エンドユーザがサーバアプリケーションにアクセスできない（トラフィックのブラックホール化が原因である可能性がある）
- WCCPが有効な場合のネットワークの速度低下（ルータによるパケットのドロップまたはル

ータのCPU使用率の上昇が原因の可能性）
- ルータのCPU使用率が過度に高い（ハードウェアではなくソフトウェアでのリダイレクションが原因である可能性がある）

WCCPの問題は、ルータの問題（またはデバイスのリダイレクト）またはWAEデバイスの問題によって発生する可能性があります。ルータとWAEデバイスの両方のWCCP設定を確認する必要があります。まず、ルータのWCCP設定を確認し、次にWAEのWCCP設定を確認します。

ルータのWCCPのトラブルシューティング

このセクションでは、次のデバイスのトラブルシューティングについて説明します。

- Catalyst 6500シリーズスイッチ、ISRおよび3700シリーズルータ
- Cisco ASR 1000 シリーズ ルータ

Catalyst 6500シリーズスイッチ、ISRおよび3700シリーズルータでのWCCPのトラブルシューティング

次のようにshow ip wccp IOSコマンドを使用して、スイッチまたはルータのWCCPv2代行受信を確認して、トラブルシューティングを開始します。

```
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--
```

ソフトウェアベースのリダイレクションを使用するプラットフォームでは、上記のコマンド出力でTotal Packets s/w Redirectedカウンタが増加していることを確認します。ハードウェアベースのリダイレクションを使用するプラットフォームでは、これらのカウンタはそれほど増加しません。これらのカウンタがハードウェアベースのプラットフォームで大幅に増加している場合は、ルータでWCCPが誤って設定されているか（WCCP GREはデフォルトでソフトウェアで処理されます）、またはTCAMリソースの枯渇などのハードウェアリソースの問題によりルータが再送されます。ハードウェアベースのプラットフォームでこれらのカウンタが増加し、CPU使用率が高

くなる可能性がある場合は、さらに調査が必要です。

Total Packets Denied Redirectカウンタは、サービスグループに一致するものの、リダイレクトリストに一致しないパケットに対して増分されます。

Total Authentication failuresカウンタは、誤ったサービスグループパスワードで受信されたパケットに対して増分されます。

ソフトウェアでWCCPリダイレクションが実行されているルータでは、**show ip wccp 61 detail IOSコマンドを使用して、ルータのWCCPv2代行受信を確認し**て、次の手順を続行します。

```
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
```

サービスグループ61のWAE状態が[Usable]であることを確認します。[Hash Allotment]フィールドで、ハッシュバケットがWAEに割り当てられていることを確認します。パーセンテージは、このWAEによって処理される合計ハッシュバケットの数を示します。WAEがサービスグループに属していた時間は、[Connect Time]フィールドに報告されます。ハッシュ割り当て方式は、ソフトウェアベースのリダイレクションで使用する必要があります。

次のように、ルータで**show ip wccp *service hash dst-ip src-ip dst-port src-port src-port* hidden IOSコマンドを使用して、ファーム内のどのWAEが特定の要求を処理するかを確認できます。**

```
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
```

WCCPリダイレクションがハードウェアで実行されるルータで、**show ip wccp 61 detail IOSコマンドを使用して、ルータのWCCPv2代受信を確認し**て、次の手順を続行します。

```
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)
```

ハードウェアリダイレクションが可能なルータのマスク割り当て方式を確認する。

ルータのTCAMリソースを保存するには、ネットワーク環境に合わせてデフォルトのWCCPマスクを変更することを検討してください。次の推奨事項を検討してください。

- WCCPリダイレクトACLを使用する場合は、できるだけ少ない数のマスクビットを使用します。リダイレクトACLと組み合わせて使用すると、マスクビットの数が少なくなり、TCAM使用率が低下します。クラスタに1 ~ 2個のWCCPクライアントがある場合は、1ビットを使用します。3 ~ 4個のWCCPクライアントがある場合は、2ビットを使用します。5 ~ 8個のWCCPクライアントがある場合は、3ビットなどを使用します。
- WAASデフォルトマスク(0x1741)の使用はお勧めしません。 データセンターの導入の目標は、クライアントやホストではなく、ブランチサイトをデータセンターにロードバランシングすることです。右側のマスクは、データセンターのWAEピアリングを最小限に抑え、ストレージを拡張します。たとえば、/24のブランチネットワークを持つ小売データセンターには、0x100 ~ 0x7F00を使用します。1ビジネスあたり/16の大企業では、0x10000 ~ 0x7F0000を使用して、企業をエンタープライズデータセンターにロードバランシングします。ブランチオフィスでは、DHCPを使用してIPアドレスを取得するクライアントのバランスを取ることが目標です。DHCPは通常、サブネット内で最も小さいIPアドレスから増加するクライアントIPアドレスを発行します。DHCPによって割り当てられたIPアドレスとマスクのバランスを最適にするには、0x1 ~ 0x7Fを使用して、クライアントのIPアドレスの最下位ビットだけを考慮し、最適な分散を実現します。

WCCPリダイレクトアクセスリストによって消費されるTCAMリソースは、そのACLの内容を設定済みのWCCPビットマスクに乗算した結果になります。したがって、WCCPバケット（マスクに基づいて作成される）の数とリダイレクトACLのエントリの数の間に競合があります。たとえば、0xF（4ビット）のマスクと200ラインリダイレクト許可ACLを使用すると、3200(2^4 x 200)のTCAMエントリが生成される場合があります。マスクを0x7（3ビット）に減らすと、TCAMの使用率が50 %低下します(2^3 x 200 = 1600)。

Catalyst 6500シリーズおよびCisco 7600シリーズプラットフォームは、ソフトウェアとハードウェアの両方でWCCPリダイレクションを処理できます。パケットが誤ってソフトウェアでリダイレクトされている場合、ハードウェアリダイレクションが予想されると、ルータのCPU使用率が過度に高くなる可能性があります。

TCAM情報を調べて、ソフトウェアまたはハードウェアでリダイレクションが処理されているかどうかを確認できます。次のように**show tcam** IOSコマンドを使用します。

```
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
```

「パント」一致は、ハードウェアで処理されない要求を表します。この状況は、次のエラーが原因で発生する可能性があります。

- マスクではなくハッシュ割り当て
- インバウンドではなくアウトバウンドリダイレクション
- Redirect exclude in
- 不明なWAE MACアドレス
- 汎用GREトンネルの宛先にループバックアドレスを使用する

次の例では、policy-routeエントリは、ルータが完全なハードウェアリダイレクションを実行していることを示しています。

```
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)
```

WAEからのHere I Am(HIA)は、WAE MACが認識しているインターフェイスと同じインターフェイスを入力する必要があります。WAEルータリストでは、直接接続されたインターフェイスではなく、ループバックインターフェイスを使用することを推奨します。

ASR 1000シリーズルータでのWCCPのトラブルシューティング

Cisco ASR 1000シリーズルータのWCCPをトラブルシューティングするコマンドは、他のルータ

とは異なります。このセクションでは、ASR 1000のWCCP情報を取得するために使用できるコマンドを示します。

ルートプロセッサのWCCP情報を表示するには、次のように**show platform software wccp rp activeコマンド**を使用します。

```
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
```

次の例は、フォワーディングプロセッサ情報を調べるために使用できる追加コマンドを示しています。

```
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>
```

各インターフェイスのリダイレクトされたパケットの統計情報を表示するには、次のように**show platform software wccp interface countersコマンド**を使用します。

```
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
```

show platform software wccp web-cache countersコマンドを使用して、WCCPキャッシュ情報を次のように表示します。

```
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
```

詳細レベルを表示するには、次のコマンドを使用します。

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

詳細については、ホワイトペーパー『Deploying and Troubleshooting Web Cache Control Protocol Version 2 on Cisco ASR 1000 Series Aggregation Services Routers』を参照してください。

WAEでのWCCPのトラブルシューティング

show wccp servicesコマンドを使用して、WAEのトラブルシューティングを開始します。次のように、サービス61とサービス62の両方が設定されていることを確認します。

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

次に、**show wccp status**コマンドを使用して、WCCPのステータスを確認します。WCCPバージョン2が有効で、次のようにアクティブであることを確認します。

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

show wccp wide-area-engineコマンドを使用して、WCCPファーム情報を調べます。このコマンドは、ファーム内のWAEの数、そのIPアドレス（リードWAE、WAEを確認できるルータ、およびその他の情報）を次のように表示します。

```
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
. . .
```

show wccp routersコマンドを使用して、ルータ情報を調べてください。WCCP対応ルータとの双方向通信があり、すべてのルータが同じKeyIP(IP)とKeyCN（変更番号）を示していることを次のように確認します。

```
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-
. . .
```

WAEがルータにレイヤ2隣接していない場合、またはループバックアドレスが使用されている場合は、WCCPをサポートするためにスタティックルートまたはデフォルトゲートウェイが必要です。

サービスグループのハッシュバケット分布を調べるには、show wccp flows tcp-promiscuousコマンドを次のように使用します。

```
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
```

または、コマンドの要約バージョンを使用して、同様の情報を表示したり、フロー情報をバイパスしたりできます。

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

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

BYP  = 0

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

AWAY = 0

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

show wccp greコマンドを使用して、GREパケットの統計情報を次のように表示します。

```
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--
```

WCCPリダイレクションが機能している場合は、最初の2つのカウンタのいずれかが増加している必要があります。

WCCPレイヤ2リダイレクト転送方式を使用してリダイレクトされたパケットのTransparent non-GRE packets receivedカウンタが増加します。

Transparent non-GRE non-WCCP packets receivedカウンタは、非WCCP代行受信方式（ACEやPBRなど）によってリダイレクトされるパケットに対して増分されます。

Total packets acceptedカウンタは、自動検出によってピアWAEが検出されたため、最適化のために受け入れられたパケットを示します。

ルータ（バイパスではなく）に送信されたGREパケットは、WCCPネゴシエーテッドリターン出力方式を使用して処理されたパケットを示します。

別のWAEカウンタに送信されたパケットは、別のWAEがサービスグループに追加され、別のWAEによって以前に処理されていたバケット割り当ての処理を開始したときにフロー保護が行われていることを示します。

次のように**show egress-methods**コマンドを使用して、使用されている出力方式が予想される出力方式であることを確認します。

```
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
```

出力方式のミスマッチは、次の状況で発生する可能性があります。

- ネゴシエートされたリターンの出力方式が設定されていますが、WCCPはレイヤ2リターンの方式をネゴシエートし、WAASでサポートされるのはGREリターンだけです。
- 一般的なGRE出力方式が設定されていますが、一般的なGRE出力が設定されている場合、代行受信方式としてサポートされているのはレイヤ2であり、WCCP GREだけです。

いずれの場合も、出力方式またはWCCP設定を変更してミスマッチを解決すると、マイナーアラームが発生し、クリアされます。アラームがクリアされるまで、デフォルトのIP転送出力方式が使用されます。

次の例は、不一致が存在する場合のコマンド出力を示しています。

```
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.
```

Catalyst 6500 Sup720またはSup32ルータの場合は、ハードウェアで処理される一般的なGRE出力方式を使用することを推奨します。また、設定を容易にするために、WAEごとに1つのポイントツーポイントトンネルではなく、1つのマルチポイントトンネルを使用することを推奨します。トンネルの設定の詳細については、『*Cisco Wide Area Application Services設定ガイド*』の「*ルータでのGREトンネルインターフェイスの設定*」の項を参照してください。

各インターセプティングルータのGREトンネル統計情報を表示するには、**show statistics generic-greコマンドを次のように**使用します。

```
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
```

WAEからの出力パケットが再インターセプトされていないことを確認しないと、リダイレクションループが発生する可能性があります。WAEがTCPオプションフィールドで返された独自のIDを検出すると、リダイレクションループが発生し、次のsyslogメッセージが表示されます。

```
%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.
```

次のように**find**コマンドを使用して、syslog.txtファイルでこのエラーのインスタンス**を検索**できます。

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

このエラーは、**show statistics filtering**コマンドで使用可能なTFOフロー統計情報にも次のように表示されます。

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

ルータでアウトバウンドリダイレクションを実行している場合、トラフィックがルータから出るときに、WAEにリダイレクトされてルータからパケットが再ルーティングされ、ルーティングループが発生します。データセンターのWAEとサーバが異なるVLANにあり、ブランチのWAEとクライアントが異なるVLANにある場合は、WAE VLANで次のルータ設定を使用することで、ルーティングループを回避できます。

```
ip wccp redirect exclude in
```

WAEが隣接するクライアントまたはサーバと同じVLANを共有する場合、ハードウェアでWCCPリダイレクションが実行されるプラットフォームに対して、ネゴシエートされたリターン方式または汎用GREリターンを使用することで、ルーティングループを回避できます。一般的なGREリターンを使用する場合、WAEはGREトンネルを使用してトラフィックをルータに返します。

バージョン4.4.1の設定可能なサービスIDおよび変数タイムアウトのトラブルシューティング

注：WCCP設定可能なサービスIDおよび可変障害検出タイムアウト機能は、WAASバージョン4.4.1で導入されました。このセクションは、以前のWAASバージョンには適用されません。

WCCPファーム内のすべてのWAEは、同じWCCPサービスIDのペア（デフォルトは61と62）を使用する必要があり、これらのIDは、ファームをサポートしているすべてのルータと一致する必要があります。ルータに設定されているWCCPサービスIDとは異なるWAEがファームに参加することは許可されず、既存の「Router Unreachable」アラームが発生します。同様に、ファーム内のすべてのWAEは、障害検出タイムアウトに同じ値を使用する必要があります。WAEは、値の不一致を設定するとアラームを発生します。

WAEがWCCPファームに参加できないというアラームが表示された場合は、WAEに設定されているWCCPサービスIDとファーム内のルータが一致していることを確認します。WAEで**show wccp wide-area-engine**コマンドを使用して、設定されたサービスIDを確認します。ルータでは、**show ip wccp** IOSコマンドを使用できます。

WAEがルータに接続されているかどうかを確認するには、**show wccp services detail**コマンドと**show wccp router detail**コマンドを使用します。

さらに、**debug ip wccp event**コマンドまたは**debug ip wccp packet**コマンドを使用して、WAEでWCCPデバッグ出力を有効にします。

WAEの「Router Unusable」マイナーアラームが表示される場合は、WAEに設定されている可変障害検出タイムアウト値がルータでサポートされていないことが原因である可能性があります。**show alarm minor detail**コマンドを使用して、アラームの原因が「Timer interval mismatch with router」であるかどうかを確認します。

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

WAEで、設定されている障害検出タイムアウトを次のように確認します。

```
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
. . .
```

ルータで、IOSバージョンが可変障害検出タイムアウトをサポートしているかどうかを確認します。設定されている場合は、**show ip wccp *xx* *detail***コマンドを使用して設定を確認できます。ここで、*xx*はWCCPサービスIDです。次の3つの結果が考えられます。

- WAEはデフォルトの障害検出タイムアウトである30秒を使用しており、ルータは同じ設定になっているか、変数タイムアウトをサポートしていません。ルータの出力には、タイムアウト設定の詳細は表示されません。この設定は正常に動作します。
- WAEはデフォルト以外の障害検出タイムアウトである9または15秒を使用しており、ルータは可変タイムアウトをサポートしていません。状態フィールドに「NOT Usable」と表示され、WAEはルータを使用できません。wccp tcp failure-detection 30グローバルコンフィギュレーションコマンドを使用して、WAE障害検出タイムアウトをデフォルト値の30秒に変更します。
- WAEはデフォルト以外の障害検出タイムアウトである9または15秒を使用しており、ルータは可変タイムアウトをサポートしています。[Client timeout]フィールドには、WAEに一致する設定された障害検出タイムアウトが表示されます。この設定は正常に動作します。

リンクフラッピングが原因でWCCPファームが不安定な場合は、WCCP障害検出タイムアウトが低すぎる可能性があります。