WAAS:AppNavのトラブルシューティング

章：AppNavのトラブルシューティング

この記事では、AppNav展開のトラブルシューティング方法について説明します。

内容

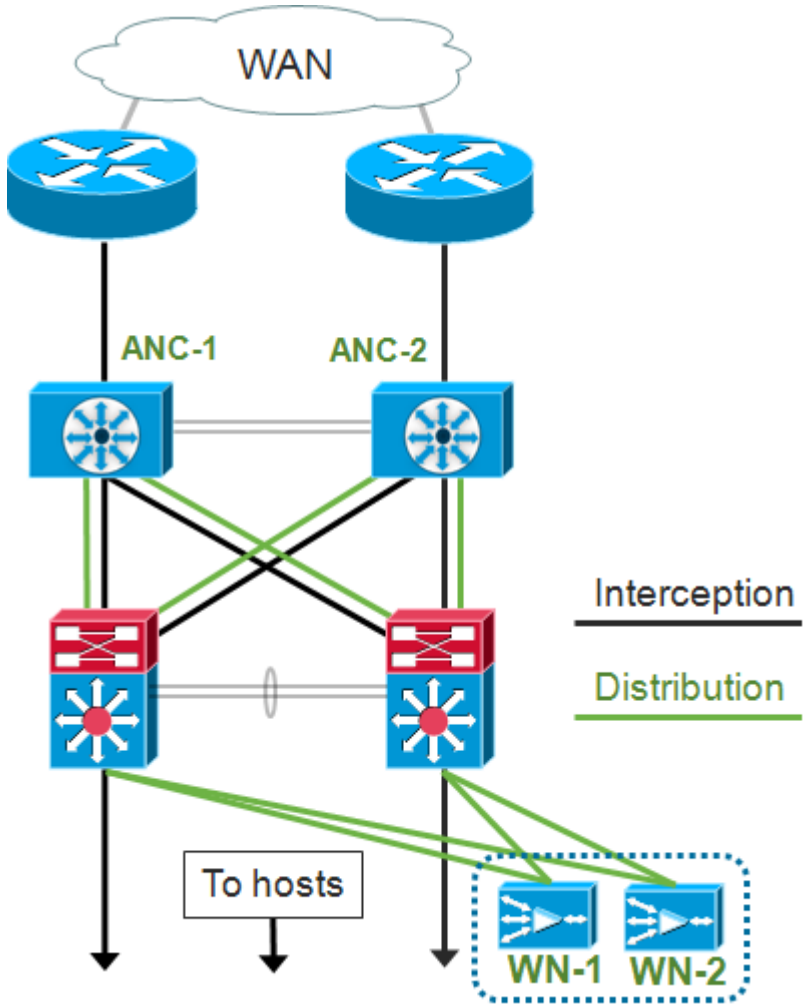
AppNavのトラブルシューティング

Cisco WAAS AppNavは、WAN最適化のネットワーク統合を簡素化し、AppNavコントローラ(ANC)を使用してWAASノード(WN)間でトラフィックを分散し、強力なクラスとポリシーメカニズムを使用して最適化することで、インターセプティングスイッチやルータへの依存をを削減します。WAASノード(WN)を使用して、サイトやアプリケーションに基づいてトラフィックを最適化できます。この記事では、AppNavのトラブルシューティング方法について説明します。

注：AppNav機能はWAASバージョン5.0.1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。

In-Path（インライン）代行受信

インラインモードでは、ANCはネットワークトラフィックのパスに配置され、パケットを代行受信してWNに配信します。



インライン展開のインターフェイス設定では、Cisco AppNavコントローラインターフェイスモジュール上の個別のインターフェイスに代行受信と配布のロールが割り当てられます。ブリッジグループインターフェイスは、インターセプションに必要で、2つ以上の物理インターフェイス、ポートチャネルインターフェイス、またはそれぞれが1つから構成されます。ブリッジグループインターフェイスは配線に失敗しません。つまり、デバイスの障害や電源の喪失の後にトラフィック

が機械的にブリッジングされないことが原因です。AppNavはクラスタリングを使用して、AppNavコントローラインターフェイスモジュール、リンクパス、またはAppNavコントローラインターフェイスモジュールへの接続が失われたか、電源障害が発生した場合に高可用性を提供します。

注：ブリッジインターフェイスはブリッジプロトコルデータユニット(BPDU)パケットをブロックせず、ループを作成する冗長インターフェイスの場合、いずれかのインターフェイスがスパニングツリープロトコルによってブロックされます。

インラインインターセプションのトラブルシューティングは、次の手順で行います。

- ネットワーク設計をチェックして、ANCの正しいインライン配置を確認します。必要に応じて、pingやtracerouteなどの基本的なツールや、レイヤ7ツールやアプリケーションを使用して、ネットワークトラフィックのパスが期待どおりに行われていることを確認します。ANCの物理的なケーブル接続を確認します。
- ANCがインラインインターセプションモードに設定されていることを確認します。
- ブリッジグループインターフェイスが正しく設定されていることを確認します。

最後の2つの手順は、Central Managerまたはコマンドラインで実行できます。ただし、Central Managerが推奨される方法であり、最初に説明します。

Central Managerで、[**Devices**] > [*AppNavController*]を選択して、[**Configure] > [Interception] > [Interception Configuration]を選択します**。[Interception Method]が[Inline]に設定されていることを確認します。

同じウィンドウで、ブリッジインターフェイスが設定されていることを確認します。ブリッジインターフェイスが必要な場合は、[ブリッジの作**成]をクリック**して作成します。ブリッジグループには、最大2つのメンバーインターフェイスを割り当てることができます。VLAN Calculatorを使用して、include操作またはexclude操作に基づいてVLANエントリを定義できます。ブリッジインターフェイスにIPアドレスが割り当てられていないことを確認します。

アラームパネルまたは**show alarm** execコマンドを使用して、デバイスでブリッジ関連のアラームが発生しているかどうかを確認します。bridge_downアラームは、ブリッジ内の1つ以上のメンバーインターフェイスがダウンしていることを示します。

CLIから、インライン操作を設定するには、次の手順を実行します。

1.代行受信方式をインラインに設定します。

```
wave# config
wave(config)# interception-method inline
```

2.ブリッジグループインターフェイスを作成します。

```
wave(config)# bridge 1 protocol interception
```

を選択します。（オプション）必要に応じて、インターセプトするVLANのリストを指定します。

```
wave(config)# bridge 1 intercept vlan-id all
```

4.ブリッジグループインターフェイスに2つの論理/物理インターフェイスを追加します。

```
wave(config)# interface GigabitEthernet 1/0
wave(config-if)# bridge-group 1
wave(config-if)# exit
wave(config)# interface GigabitEthernet 1/1
wave(config-if)# bridge-group 1
wave(config-if)# exit
```

show bridge execコマンドを使用して、ブリッジインターフェイスの動作ステータスを確認し、ブリッジの統計情報を表示できます。

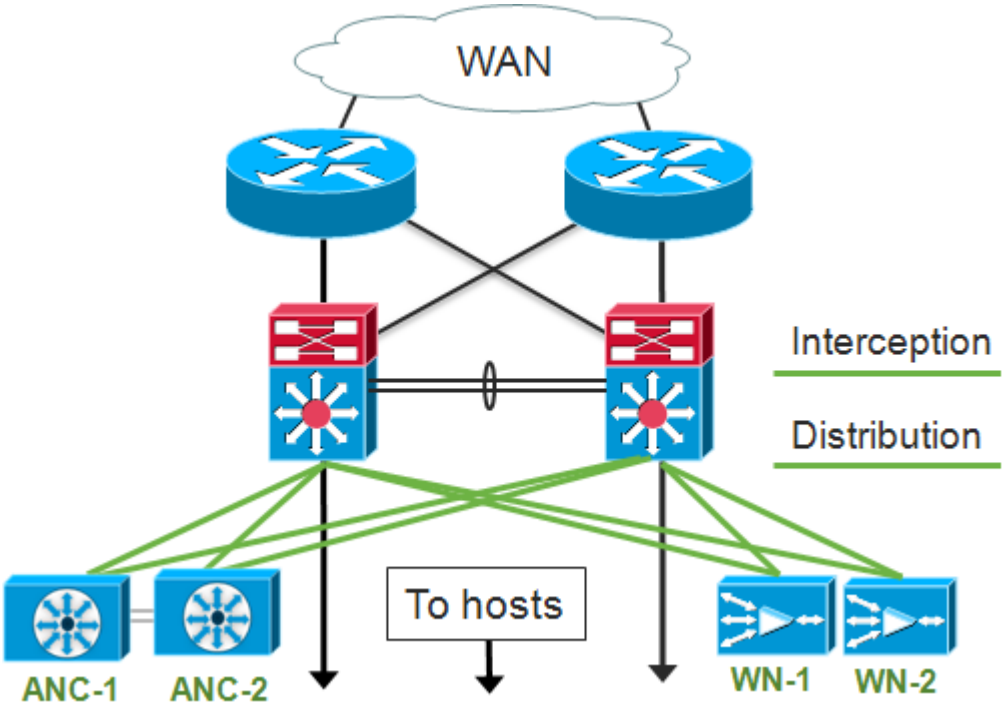
```
wave# show bridge 1
lsp: Link State Propagation
flow sync: AppNav Controller is in the process of flow sync
Member Interfaces:
 GigabitEthernet 1/0
 GigabitEthernet 1/1
Link state propagation: Enabled
VLAN interception:
 intercept vlan-id all                                                    <<< VLANs to intercept

Interception Statistics:
                              GigabitEthernet 1/0    GigabitEthernet 1/1
Operation State                  :   Down           Down(lsp)            <<< Down due to LSP
Input Packets Forwarded/Bridged  :   16188          7845
Input Packets Redirected         :   5068           0
Input Packets Punted             :   1208           605
Input Packets Dropped            :   0              0
Output Packets Forwarded/Bridged :   7843           21256
Output Packets Injected          :   301            301
Output Packets Dropped           :   2              0
```

上記の例では、Gig 1/0インターフェイスがダウンし、Gig 1/1インターフェイスもリンクステート伝搬(LSP)によりダウンしています。 Down(flow sync)が表示されることもあります。これは、ANCがクラスタに参加し、クラスタ内の他のANCとフロー情報を同期していることを意味します。既存のフローが正しく分散されるように、すべてのANCが同期されるまで、インターセプションパス (ブリッジインターフェイス) を約2分間閉じます。

出力の下部には、メンバーインターフェイスのトラフィック統計情報が表示されます。

オフパス(WCCP)代行受信

WCCPモードでは、WCCPルータは、パケットを代行受信し、オフパスにあるANCにリダイレクトするネットワークトラフィックのパスに配置されます。AppNavは、WAASアクセラレータ間の代行処理、インテリジェントなフロー分散、および負荷の考慮事項を処理するため、ルータのWCCP設定は大幅に簡素化されます。



オフパス展開のインターフェイス設定では、代行受信と配布のロールがCisco AppNav Controllerインターフェイスモジュールで同じインターフェイスを共有できますが、これは必須ではありません。

オフパスインターセプションのトラブルシューティングは、次の手順で行います。

- WCCPルータが最適化されたホストとの間を行き来するトラフィックのパスにあることを確認するために、正しい配置を確認します。**show run**または**show wccp**コマンドを使用して、これらがWCCP用に設定されているルータと同じであることを確認できます。必要に応じて、pingやtracerouteなどの基本的なツール、レイヤ7ツールやアプリケーションを使用して、最適化が必要なすべてのトラフィックがWCCPルータを通過することを確認します。
- Central Manager（推奨）またはCLIを使用して、WAAS ANCのWCCP設定を確認します。
- ルータCLIを使用して、リダイレクト側ルータのWCCP設定を確認します。

ANCのWCCP設定を確認するには、Central Managerで**[Devices] > [***AppNavController]を選択して*、**[Configure] > [Interception] > [Interception Configuration]を選択します**。

- [Interception Method]が[WCCP]に設定されていることを確認します。
- [Enable WCCP Service]チェックボックスがオンになっていることを確認します。
- [Use Default Gateway as WCCP Router]チェックボックスがオンになっているか、WCCPルータのIPアドレスが[WCCP Router]フィールドにリストされていることを確認します。
- ロードバランシングのマスクやリダイレクト方式などの他の設定が、導入に適切に設定されていることを確認します。

ルータのWCCPファームの一部であるANCのWCCP関連アラームを確認します。Central Managerで、画面下部の[Alarms]パネルをクリックするか、各デバイスで**show alarmコマンド**を使用してアラームを表示します。必要に応じてANCまたはルータの設定を変更して、アラーム状態を修正します。

CLIから、次の手順に従ってWCCP操作を設定します。

1.代行受信方式をwccpに設定します。

```
wave# config
wave(config)# interception-method wccp
```

2. WCCPルータリストを設定します。これには、WCCPファームに参加しているルータのIPアドレスが含まれます。

```
wave(config)# wccp router-list 1 10.10.10.21 10.10.10.22
```

3. WCCPサービスIDを設定します。AppNavでは1つのサービスIDが推奨されますが、2つのサービスIDがサポートされます。

```
wave(config)# wccp tcp-promiscuous 61
```

4.設定されたルータリストをWCCPサービスに関連付けます。

```
wave(config-wccp-service)# router-list-num 1
```

5. WCCP割り当て方式を設定します（ANCではマスク方式のみがサポートされます）。 dst-ip-maskまたはsrc-ip-maskオプションを指定しない場合、デフォルトの送信元IPマスクはfに設定され、宛先IPマスクは0に設定されます。

```
wave(config-wccp-service)# assignment-method mask
```

6. WCCPリダイレクトメソッドを設定します（出力メソッドとリターンメソッドは、リダイレクトメソッドに一致するように自動的に設定され、ANCでは設定できません）。 L2（デフォルト）またはGREを選択できます。L2では、ANCがルータとのレイヤ2接続を持ち、ルータもレイヤ2リダイレクション用に設定されている必要があります。

```
wave(config-wccp-service)# redirect-method gre
```

7. WCCPサービスを有効にします。

```
wave(config-wccp-service)# enable
```

show running-configコマンドを使用して、各ANCのWCCP代行受信を確認します。次の2つの例は、L2リダイレクトとGREリダイレクトの実行コンフィギュレーション出力を示しています。

Show running-config wccp（L2リダイレクト用）:

```
wave# sh run wccp
wccp router-list 1 10.10.10.21 10.10.10.22
wccp tcp-promiscuous service-pair 61
  router-list-num 1
  enable                                          <<< L2 redirect is default so is not shown in
running config
  exit
```

Show running-config wccp（GRE用）:

```
wave# sh run wccp
wccp router-list 1 10.10.10.21 10.10.10.22
wccp tcp-promiscuous service-pair 61
 router-list-num 1
 redirect-method gre                              <<< GRE redirect method is configured
 enable
 exit
```

show wccp statusコマンドを使用して、各ANCのWCCPステータスを確認します。

```
wave# show wccp routers
WCCP Interception :
Configured State :  Enabled                       <<< Shows Disabled if WCCP is not configured
Operational State : Enabled                       <<< Shows Disabled if WCCP is not enabled
 Services Enabled on this WAE:
        TCP Promiscuous 61                        <<< Shows NONE if no service groups are
configured
```

show wccp routersコマンドを使用して、WCCPファームのキープアライブメッセージに応答したルータを確認します。

```
wave# show wccp routers
Router Information for Service Id: 61

       Routers Seeing this Wide Area Engine(2)
       Router Id       Sent To                    <<< List of routers seen by this ANC
       192.168.1.1     10.10.10.21
       192.168.1.2     10.10.10.22
       Routers not Seeing this Wide Area Engine   <<< List of routers not seen by this ANC
               -NONE-
       Routers Notified of from other WAE's       <<< List of routers notified of but not
configured in router list
               -NONE-
```

show wccp clientsコマンドを使用して、WCCPファーム内の他のANCと、それぞれが到達可能なルータの各ANCのビューを確認します。

```
wave# show wccp clients
Wide Area Engine List for Service: 61
Number of WAE's in the Cache farm: 2                              <<< Number of ANCs in the farm
       IP address = 10.10.10.31   Lead WAE = NO   Weight = 0   <<< Entry for each ANC in the
farm
       Routers seeing this Wide Area Engine(2)
               192.168.1.1                                        <<< List of routers seeing this
ANC
               192.168.1.2

       IP address = 10.10.10.32   Lead WAE = YES  Weight = 0   <<< YES indicates ANC is serving
as the lead
       Routers seeing this Wide Area Engine(2)
               192.168.1.1                                        <<< List of routers seeing this
ANC
               192.168.1.2
```

show statistics wccpコマンドを使用して、ファーム内のルータから各ANCがパケットを受信していることを確認します。各ルータで送受信されたトラフィックの統計情報が表示されます。ファーム内のすべてのルータの累積統計情報が下部に表示されます。同様のコマンドは、show wccp

statisticsです。「OE」は、ここでANCデバイスを指します。

```
wave# sh statistics wccp

WCCP Stats for Router              : 10.10.10.21
 Packets Received from Router      : 1101954
 Bytes Received from Router        : 103682392
 Packets Transmitted to Router     : 1751072
 Bytes Transmitted to Router       : 2518114618
 Pass-thru Packets sent to Router  : 0
 Pass-thru Bytes sent to Router    : 0
 Redirect Packets sent to OE       : 1101954
 Redirect Bytes sent to OE         : 103682392

WCCP Stats for Router              : 10.10.10.22
 Packets Received from Router      : 75264
 Bytes Received from Router        : 10732204
 Packets Transmitted to Router     : 405193
 Bytes Transmitted to Router       : 597227459
 Pass-thru Packets sent to Router  : 0
 Pass-thru Bytes sent to Router    : 0
 Redirect Packets sent to OE       : 75264
 Redirect Bytes sent to OE         : 10732204

Cummulative WCCP Stats:
 Total Packets Received from all Routers : 1177218
 Total Bytes Received from all Routers : 114414596
 Total Packets Transmitted to all Routers : 2156265
 Total Bytes Transmitted to all Routers : 3115342077
 Total Pass-thru Packets sent to all Routers : 0
 Total Pass-thru Bytes sent to all Routers : 0
 Total Redirect Packets sent to OE : 1177218
 Total Redirect Bytes sent to OE   : 114414596
```

ルータでのWCCP代行受信の設定と確認

WCCPファームの各ルータでWCCP代行受信を設定するには、次の手順を実行します。

1. **ip wccp** routerコマンドを使用して、ルータのWCCPサービスを設定します。

```
Core-Router1 configure terminal
Core-Router1(config)# ip wccp 61
```

2.ルータのLANおよびWANインターフェイスでWCCP代行受信を設定します。ANCで1つのサービスIDを使用している場合は、両方のインターフェイスで同じサービスIDを設定できます。

```
Core-Router1(config)# interface GigabitEthernet0/0
Core-Router1(config-subif)# ip address 10.20.1.1 255.255.255.0
Core-Router1(config-subif)# ip wccp 61 redirect in
Core-Router1(config-subif)# ip router isis inline_wccp_pod
Core-Router1(config-subif)# exit

Core-Router1(config)# interface GigabitEthernet0/1
Core-Router1(config-subif)# ip address 10.19.1.1 255.255.255.0
Core-Router1(config-subif)# ip wccp 61 redirect in
Core-Router1(config-subif)# ip router isis inline_wccp_pod
```

```
Core-Router1(config-subif)# glbp 701 ip 10.19.1.254
Core-Router1(config-subif)# duplex auto
Core-Router1(config-subif)# speed auto
Core-Router1(config-subif)# media-type rj45
Core-Router1(config-subif)# exit
```

を選択します。（オプション）一般的なGRE出力を使用している場合は、トンネルインターフェイスを設定します（ANC WCCPリダイレクト方式にGREを選択した場合のみ）。

```
Core-Router1(config)# interface Tunnel1
Core-Router1(config-subif)# ip address 192.168.1.1 255.255.255.0
Core-Router1(config-subif)# no ip redirects
Core-Router1(config-subif)# tunnel source GigabitEthernet0/0.3702
Core-Router1(config-subif)# tunnel mode gre multipoint
```

show wccpコマンドを使用して、ファーム内の各ルータのWCCP設定を確認します。

```
Core-Router1 sh ip wccp 61 detail
WCCP Client information:
       WCCP Client ID:          10.10.10.31            <<< ANC IP address
       Protocol Version:        2.00
       State:                   Usable
       Redirection:             GRE                    <<< Negotiated WCCP parameters
       Packet Return:           GRE                    <<<
       Assignment:              MASK                   <<<
       Connect Time:            00:31:27
       Redirected Packets:
         Process:               0
         CEF:                   0
       GRE Bypassed Packets:
         Process:               0
         CEF:                   0
       Mask Allotment:          16 of 16 (100.00%)
       Assigned masks/values:   1/16

       Mask  SrcAddr    DstAddr    SrcPort DstPort
       ----  -------    -------    ------- -------
       0000: 0x0000000F 0x00000000 0x0000  0x0000      <<< Configured mask

       Value SrcAddr    DstAddr    SrcPort DstPort
       ----- -------    -------    ------- -------
       0000: 0x00000000 0x00000000 0x0000  0x0000      <<< Mask assignments
       0001: 0x00000001 0x00000000 0x0000  0x0000
       0002: 0x00000002 0x00000000 0x0000  0x0000
       0003: 0x00000003 0x00000000 0x0000  0x0000
       0004: 0x00000004 0x00000000 0x0000  0x0000
       0005: 0x00000005 0x00000000 0x0000  0x0000
       0006: 0x00000006 0x00000000 0x0000  0x0000
       0007: 0x00000007 0x00000000 0x0000  0x0000
       0008: 0x00000008 0x00000000 0x0000  0x0000
       0009: 0x00000009 0x00000000 0x0000  0x0000
       0010: 0x0000000A 0x00000000 0x0000  0x0000
       0011: 0x0000000B 0x00000000 0x0000  0x0000
       0012: 0x0000000C 0x00000000 0x0000  0x0000
       0013: 0x0000000D 0x00000000 0x0000  0x0000
       0014: 0x0000000E 0x00000000 0x0000  0x0000
       0015: 0x0000000F 0x00000000 0x0000  0x0000
```

追加情報

詳細については、次のドキュメントを参照してください。

- Cisco Catalyst 6500とのWCCPネットワーク統合：導入を成功させるためのベストプラクティスの推奨事項
- Cisco Wide Area Application Services(WAAS)Web Cache Communication Protocol Redirection:Ciscoルータプラットフォームのサポート
- Cisco *Wide Area Application Services*構成ガイドからルータの高度なWCCP機能を設定する
- WAEでのWCCPの設定(『*Cisco Wide Area Application Services Configuration Guide*』)

ネットワーク接続のトラブルシューティング

WAASのトラブルシューティングを行う際には、ネットワークがWAASを無効にしているときの動作を判断することが役立つ場合があります。これは、トラフィックの最適化に失敗するだけでなく、トラフィックの通過に失敗する場合に役立ちます。このような場合、問題がWAASに関連していないことが判明する可能性があります。トラフィックが通過している場合でも、この技術は、トラブルシューティングが必要なWAASデバイスを判別するのに役立ちます。

レイヤ3接続をテストする前に、AppNavコントローラインターフェイスモジュールが適切なスイッチポートに接続されていることを確認します。接続されたスイッチでCisco Discovery Protocol(CDP)がサポートされており、Cisco Discovery Protocol(CDP)が有効になっている場合は、**show cdp neighbors detailコマンドを実行して、ネットワークスイッチへの正しい接続を確認**します。

WAASの無効化は、すべてのケースで適用できるとは限りません。一部のトラフィックが最適化されていて、一部のトラフィックが最適化されていない場合、WAASを無効にすることは許容できない可能性があり、これにより、正常に最適化されているトラフィックが中断されます。このような場合、代行受信ACLまたはAppNavポリシーを使用して、問題が発生している特定のタイプのトラフィックを通過させることができます。詳細については、「特定のトラフィックを通過する」の項を参照してください。

WAASを無効にするには、オフパスモードとは異なる手順をインラインモードで実行します。

- インラインモードでは、インターセプションブリッジをパススルー状態にする必要があります。詳細については、「インラインANCの無効化」の項を参照してください。
- オフパスモードでは、WCCPプロトコルを無効にする必要があります。詳細については、「オフパスANCの無効化」の項を参照してください。

AppNav環境では、ANCだけを無効にする必要があります。WNは代行受信に参加しないため、無効にする必要はありません。

WAASが無効になったら、標準的な方法を使用してネットワーク接続を確認します。

- pingやtracerouteなどのツールを使用して、レイヤ3接続を確認します。
- アプリケーションの動作をチェックして、上位層の接続を判別する
- ネットワークでWAASが有効になっていたのと同じ接続の問題が発生している場合、問題はおそらくWAASに関係していない可能性があります。
- ネットワークがWAASが無効な状態で正常に動作しているが、WAASが有効になっている状態で接続に問題がある場合は、おそらく1つ以上のWAASデバイスに注意が必要です。次のステップでは、問題を特定のWAASデバイスに切り分けます。
- ネットワークでWAASが有効な状態と無効な状態の間に接続できるが、最適化が行われていない場合、おそらく1つ以上のWAASデバイスに注意が必要です。次のステップでは、問題を

特定のWAASデバイスに切り分けます。

WAASを有効にしてネットワークの動作を確認するには、次の手順を実行します。

1. WAAS ANCでWAAS機能を再度有効にし、必要に応じてWCCPルータを有効にします。

2. WAASに関連する問題があると判断した場合は、各AppNavクラスタまたはANCを個別に有効にして、問題が発生する潜在的な原因として切り分けます。

3.各ANCが有効になっているので、前の手順と同じ基本的なネットワーク接続テストを実行し、この特定のANCが正常に動作しているかどうかに注意してください。この段階では、個々のWNに関心を持たないでください。この段階の目標は、どのクラスタと、どの特定のANCで望ましい動作または望ましくない動作が発生しているかを判断することです。

4.各ANCが有効でテストされているため、再度無効にして、次のANCを有効にします。各ANCを有効にしてテストすると、トラブルシューティングを進める必要があるANCを判別できます。

このトラブルシューティング手法は、WAASの設定が最適化に失敗するだけでなく、通常のネットワーク接続の問題を引き起こす場合にも最も適しています。

特定のトラフィックの通過

特定のトラフィックをパススルーするには、インターセプションACLを使用するか、パススルー用にAppNavポリシーを設定します。

- 特定のトラフィックの通過を拒否し、その他すべてを許可するACLを作成します。この例では、HTTPトラフィック（宛先ポート80）をパススルーします。 ANC代行受信アクセスリストを定義されたACLに設定します。ポート80宛ての接続は通過します。**show statistics pass-through type appnav**コマンドを使用すると、PTインターセプトACLカウンタが増加していることを確認して、パススルーが発生していることを確認できます。

```
anc# config
anc(config)# ip access-list extended pt_http
anc(config-ext-nacl)# deny tcp any any eq 80
anc(config-ext-nacl)# permit ip any any
anc(config-ext-nacl)# exit
anc(config)# interception appnav-controller access-list pt_http
```

- 特定のクラスに一致するトラフィックを通過するようにANCポリシーを設定します。

```
class-map type appnav HTTP
   match tcp dest port 80

policy-map type appnav my_policy
.
.
.
class HTTP
   pass-through
```

インラインANCの無効化

インラインANCをパススルー状態にして無効にする方法は複数あります。

- 代行受信ブリッジVLANリストを[none]に設定します。Central ManagerでANCデバイスを選択し、[**Configure**] > [Interception] > [Interception Configuration] の順に選択します。ブリッジインタフェースを選択し、タスクバーの編集アイ**コンをク**リックします。[VLANs]フィールドの値を[none]に設定します。
- ANCを含むサービスコンテキストを無効にします。Central Managerでクラスタを選択し、[AppNav Controllers]タブをクリックしてANCを選択し、[Disable taskbar]アイコンを**クリック**します。
- 「すべて拒否」基準を使用して代行受信ACLを適用します。この方法が推奨されます。（最初の2つの方法は、既存の最適化された接続を中断させます）。 ACLをdeny ALL基準で定義します。Central ManagerでANCデバイスを選択し、**Configure > Interception > Interception Access List**の順に選択し、AppNav Controller Interception Access Listドロップダウンリストでdeny ALLアクセスリストを選択します。

CLIからACLによるインターセプションを無効にするには、次のコマンドを使用します。

```
anc# config
anc(config)# ip access-list standard deny
anc(config-std-nacl)# deny any
anc(config-std-nacl)# exit
anc(config)# interception appnav-controller access-list deny
```

ANCをパススルー状態にする：

- インターフェイスではなく、WAASインターセプションを無効にします。
- すべてのWAAS最適化を無効にします。
- すべてのトラフィックが影響を受けないようにします。

オフパスANCの無効化

オフパスモードで実行されているANCを無効にするには、ANCのWCCPプロトコルを無効にします。この操作は、ANCまたはリダイレクト側ルータ、あるいはその両方で実行できます。ANCでは、WCCPサービスを無効または削除したり、代行受信方式を削除したり、WCCPから別の方式に変更したりできます。

WCCP代行受信を無効にするには、Central ManagerでANCデバイスを選択し、[設定(Configure)] > [代行受信(Interception)] > [代行受信**設定(Interception Configuration)]を選択します**。[WCCPサービスを有効にする(Enable WCCP Service)]チェックボックスをオフにするか、[設定の削除(Remove Settings)]タスクバーアイコンをクリックして、WCCP代行受信設定を完全に削除します（失われます）。

CLIからWCCP代行受信を無効にするには、次のコマンドを使用します。

```
anc# config
anc(config)# wccp tcp-promiscuous service-pair 61
anc(config-wccp-service)# no enable
```

場合によっては、同じルータからリダイレクトされたトラフィックを受信する複数のANCが存在する場合があります。便宜上、ANCではなくルータでWCCPを無効にすることを選択できます。利点は、1つのステップでWCCPファームから複数のANCを削除できることです。欠点は、WAAS Central Managerからこれを実行できないことです。

ルータでWCCPを無効にするには、次の構文を使用します。

```
RTR1(config)# no ip wccp 61
RTR1(config)# no ip wccp 62    <<< Only needed if you are using two WCCP service IDs
```

ルータでWCCPを再度有効にするには、次の構文を使用します。

```
RTR1(config)# ip wccp 61
RTR1(config)# ip wccp 62       <<< Only needed if you are using two WCCP service IDs
```

各WCCPルータで、無効にするANCがWCCPクライアントとして表示されていないことを確認します。ルータでWCCPサービスが削除されると、次の出力が表示されます。

```
RTR1# show ip wccp 61
The WCCP service specified is not active.
```

AppNavクラスタのトラブルシューティング

AppNavクラスタのトラブルシューティングには、次のツールを使用できます。

- AppNavアラーム
- Central Managerモニタリング
- クラスタとデバイスのステータスを監視するためのAppNav CLIコマンド
- フロー分散統計情報を監視するためのAppNav CLIコマンド
- 接続トレース
- AppNavデバッグログ

AppNavアラーム

Cluster Membership Manager(CMM)では、エラー状態により次のアラームが発生します。

- [Degraded Cluster (Critical)]:ANC間の部分的な可視性。ANCは新しい接続を通過します。
- コンバージェンス失敗（重大）:ANCはANCとWNの安定したビューでのコンバージェンスに失敗しました。ANCは新しい接続を通過します。
- [ANC Join Failed (Critical)]:ANCは、クラスタがANC内で劣化する可能性があるため、既存のクラスタに参加できませんでした。
- [ANC混合ファーム（マイナー）(ANC Mixed Farm (Minor))]：クラスタ内のANCで実行されているクラスタプロトコルのバージョンは異なりますが、互換性があります。
- ANC到達不能（メジャー）：設定されたANCに到達できません。
- WN Unreachable (Major)：設定されたWNは到達不能です。このWNはトラフィックリダイレクションには使用されません。
- [WN除外（メジャー）(WN Excluded (Major))]：設定されたWNは到達可能ですが、1つ以上の他のANCがそれを認識できないため、除外されます。このWNは、トラフィックリダイレクション（新しい接続）には使用されません。

Central Managerの[アラーム]パネルでアラームを表示するか、デバイスで**show alarms** EXECコマンドを使用します。

注：CMMは、サービスコンテキストに関連付けられたAppNavクラスタへのANCとWNのグループ化を管理する内部AppNavコンポーネントです。

Central Managerモニタリング

Central Managerを使用して、AppNavクラスタの確認、監視、トラブルシューティングを行うことができます。Central Managerには、ネットワーク内のすべての登録済みWAASデバイスのグローバルビューがあり、ほとんどのAppNavの問題を迅速に特定できます。

[Central Manager]メニューから、[AppNav Clusters] > [*cluster-name*]を選択します。クラスタホームウィンドウには、クラスタトポロジ（WCCPおよびゲートウェイルータを含む）、クラスタ全体のステータス、デバイスステータス、デバイスグループのステータス、およびリンクステータスが表示されます。

まず、クラスタ全体のステータスが動作可能であることを確認します。

この図に示すANCおよびWNアイコンは、同じデバイス上に存在するため、同じデバイス名を持っていることに注意してください。WANとしてトラフィックを最適化するANCでは、これらの2つの機能がトポロジ図に個別のアイコンとして表示されます。

デバイスが過去30秒以内に応答しなかった（デバイスがオフラインまたは到達不能の可能性がある）ため、Central Managerが現在の情報を持っていないデバイスには、オレンジ色の三角形の警告インジケータが表示されます。

デバイスアイコンにカーソルを合わせると、ANCまたはWNデバイスの詳細な360度ステータスビューが表示されます。最初のタブには、デバイスのアラームが表示されます。適切なクラスタ動作を妨げているアラームを解決する必要があります。

各ANCでデバイスの代行受信方式を確認するには、[代行受信]タブをクリックします。

インターセプションがダウンしている場合、ステータスは次のように表示されます。

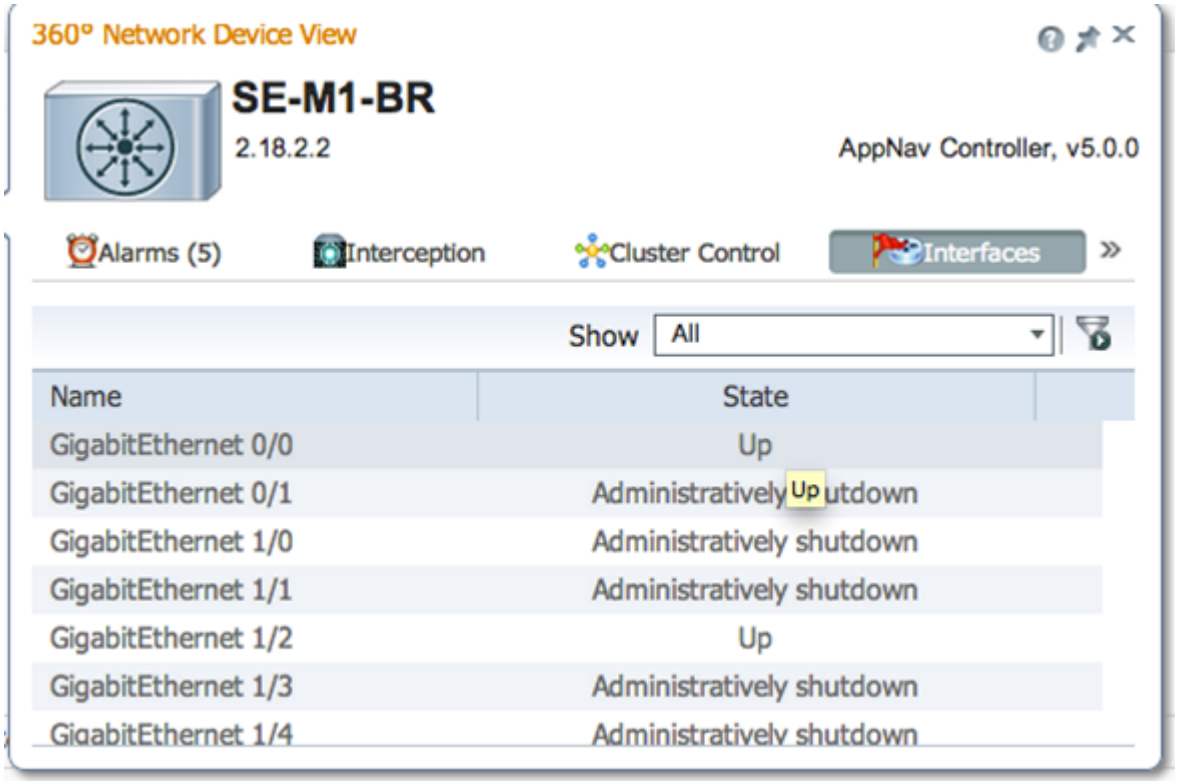
[クラスタ制御(Cluster Control)]タブをクリックして、このANCに表示されるクラスタ内の各デバイスのIPアドレスとステータスを確認します。クラスタ内の各ANCには、同じデバイスのリストが必要です。そうでない場合は、設定またはネットワークの問題を示します。

すべてのANCが互いに認識できない場合、クラスタは動作不能であり、クラスタがフローを同期できないため、すべてのトラフィックが通過します。

すべてのANCが接続されているが、WNのビューが異なる場合、クラスタはデグレード状態になります。トラフィックは引き続き分散されますが、すべてのANCによって認識されるWNのみに分散されます。

すべてのANCに表示されないWNは除外されます。

[Interfaces]タブをクリックして、ANCの物理インターフェイスと論理インターフェイスの状態を確認します。



クラスタ内の各WNの360度ビューを見て、[最適化]タブですべてのアクセラレータの緑のステータスを確認します。アクセラレータの黄色のステータスは、アクセラレータが動作しているが、新しい接続をサービスできないことを意味します。たとえば、過負荷状態になっている場合や、ライセンスが削除されている場合などです。赤のステータスは、アクセラレータが実行されていないことを示します。アクセラレータが黄色または赤色の場合は、これらのアクセラレータを個別にトラブルシューティングする必要があります。Enterpriseライセンスがない場合は、「System license has been revoked」という説明が表示されます。[Admin] > [History] > [License Management device]ページで、Enterpriseライセンスをインストールします。

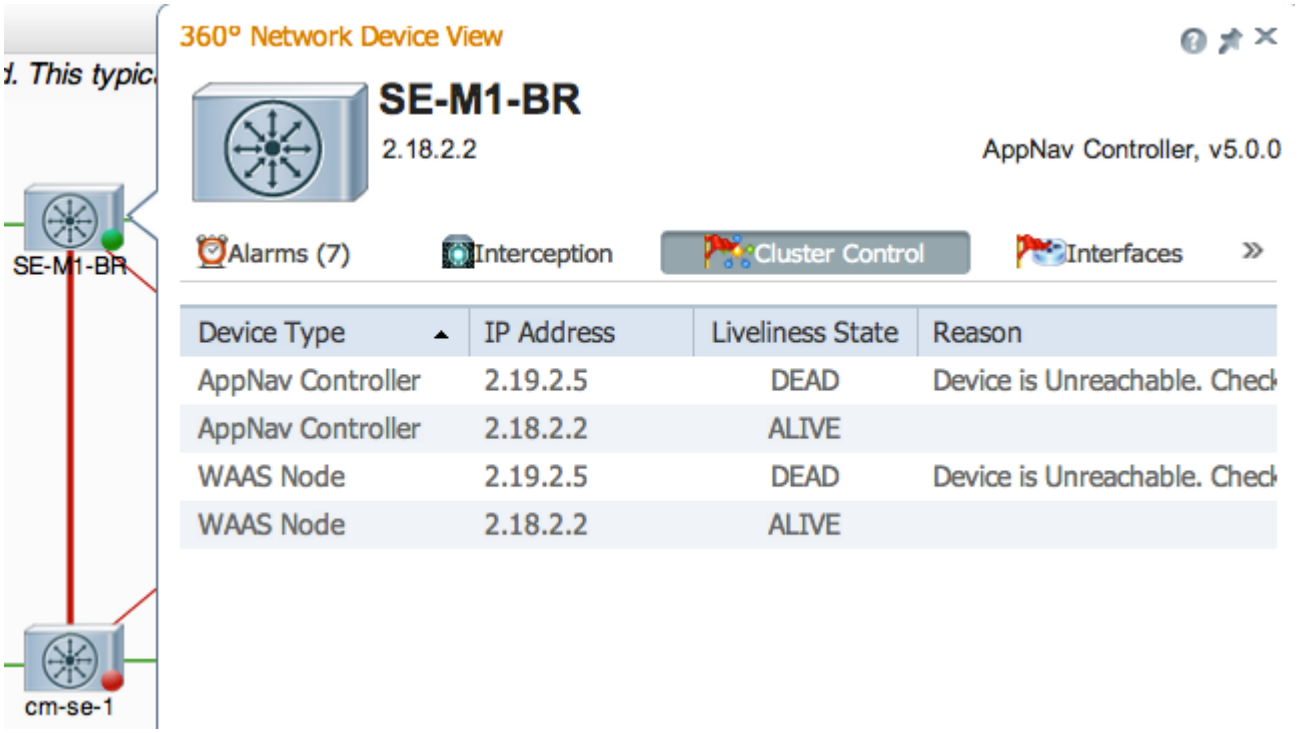
クラスタの分割は、クラスタ内のANC間の接続の問題によって発生します。Central Managerがすべてのと通信できる場合は、分割クラスタを検出できますが、一部のANCと通信できない場合は、分割を検出できません。Central Managerが任意のデバイスとの接続を失い、デバイスが

Central Managerでオフラインとして表示される場合、「Management status is offline」アラームが発生します。

データリンクがダウンしても管理接続を維持するには、管理インターフェイスをデータインターフェイスから分離するのが最適です。

スプリットクラスタでは、ANCの各サブクラスタは見えるWNGにフローを個別に分散しますが、サブクラスタ間のフローは調整されていないため、リセット接続が発生し、クラスタ全体のパフォーマンスが低下します。

各ANCの[Cluster Control]タブで、1つ以上のANCに到達できないかどうかを確認します。「Service controller is unreachable」アラームは、以前は相互に通信できる2つのANCが互いの間で接続を失った場合に発生しますが、これはスプリットクラスタの唯一の原因ではなく、各ANCの[Cluster Control]タブを確認するのが最善です。



ANCのステータスがグレーのライトになっている場合は、無効になっている可能性があります。トポロジダイアグラムの下にある[AppNav Controllers]タブをクリックして、すべてのANCが有効になっていることを確認します。ANCが有効になっていない場合は、[有効]状態は[いいえ]です。[タスクバーを有効にする]アイコンをクリックしてANCを有効にすることができます。

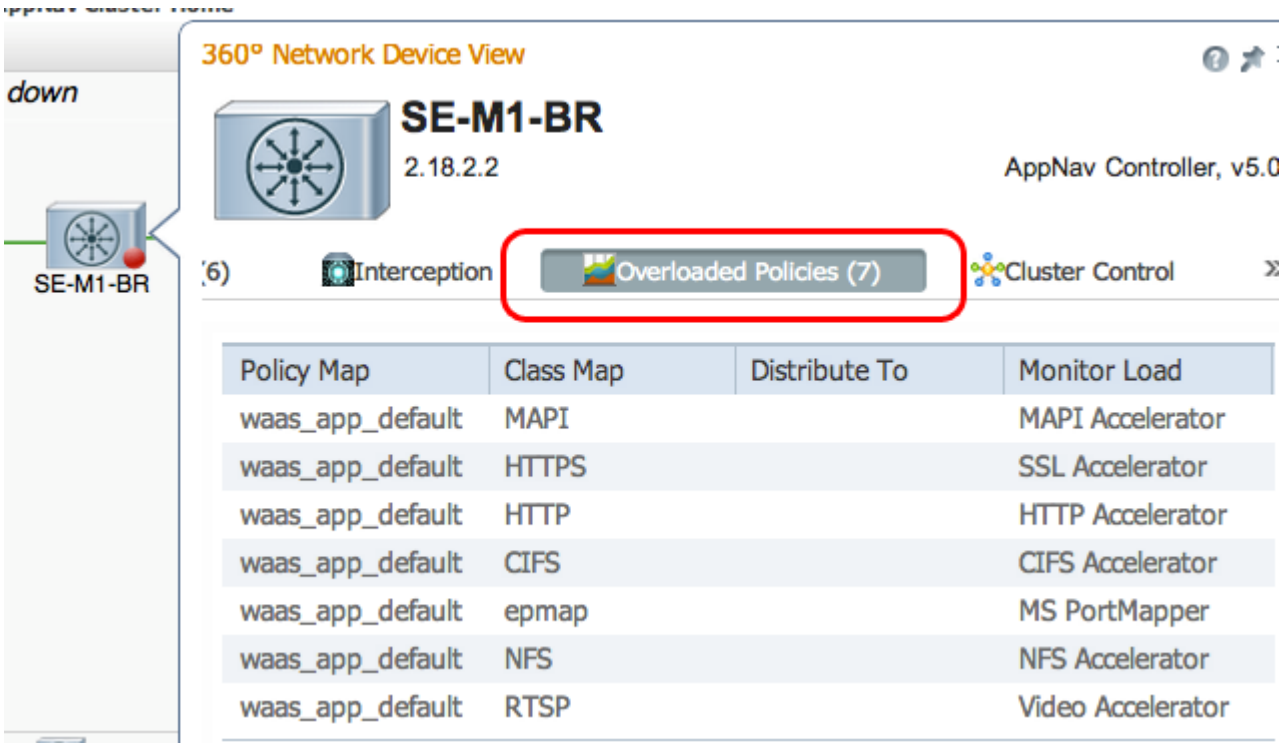
緑色のステータスライト以外の何らかのANCのAppNavポリシーを確認します。デバイスのステータスライトにカーソルを合わせると、ツールチップにステータスまたは問題（検出された場合）が表示されます。

定義されたポリシーを確認するには、Central Managerメニューから[Configure] > [AppNav Policies]を選択し、[Manage]ボタンをクリックします。

通常、クラスタ内のすべてのANCに割り当てられる1つのポリシーが必要です。デフォルトのポリシー名はappnav_defaultです。ポリシーの横にあるオプションボタンを選択し、[タスクバーの編集]アイコンをクリックします。[AppNavポリシー(AppNav Policy)]ペインには、選択したポリシーが適用されるANCが表示されます。すべてのANCにチェックマークが付いていない場合は、チェックマークが付いていない各ANCの横にあるチェックボックスをクリックして、ポリシーを割り当てます。[OK]をクリックして、変更を保存します。

ポリシーの割り当てを確認した後、表示されたままの[AppNav Policies]ページでポリシールールを確認できます。任意のポリシー規則を選択し、[タスクバーの編集]アイコンをクリックして定義を変更します。

1つ以上のポリシーが過負荷の場合、ANCのステータスが黄色または赤色になる場合があります。360度デバイスビューの[Overload Policies]タブをチェックして、過負荷になっている監視対象ポリシーのリストを確認します。



ANCがクラスタに参加している場合は、黄色のステータスライトと参加ステータスが表示されます。

360度のデバイスビューの[代行受信]タブには、結合状態が原因で代行受信パスがダウンしていることが示されます。代行受信は、ANCが他のANCとフローテーブルを同期し、トラフィックを受け入れる準備が整うまで停止されます。通常、このプロセスには2分を超える時間はかかりません。

クラスタからANCを削除しても、トポロジ図に数分間表示され、[クラスタ制御(Cluster Control)]タブに表示され、すべてのANCが新しいクラスタトポロジに同意するまで表示されます。この状態では、新しいフローは受信されません。

クラスタとデバイスのステータスを監視するためのAppNav CLIコマンド

ANCでのトラブルシューティングには、次のようなCLIコマンドが役立ちます。

- **show run service-insertion**
- **show service-insertion service-context**
- **show service-insertion appnav-controller-group**
- **show service-insertion service-node-group all**
- **show service-insertion appnav-controller** *ip-address*
- **show service-insertion service-node** [*ip-address*]
- **show service-insertion service-node-group** *group-name*

WNで次のコマンドを使用します。

- show run service-insertion
- show service-insertion service-node

ANCでshow service-insertion service-contextコマンドを使用すると、サービスコンテキストのステータスとクラスタ内のデバイスの安定した表示を確認できます。

```
ANC# show service-insertion service-context
Service Context                              : test
Service Policy                               : appnav_default              <<< Active AppNav
policy
Cluster protocol ICIMP version               : 1.1
Cluster protocol DMP version                 : 1.1
Time Service Context was enabled             : Wed Jul 11 02:05:23 2012
Current FSM state                            : Operational                 <<< Service context
status
Time FSM entered current state               : Wed Jul 11 02:05:55 2012
Last FSM state                               : Converging
Time FSM entered last state                  : Wed Jul 11 02:05:45 2012
Joining state                                : Not Configured
Time joining state entered                   : Wed Jul 11 02:05:23 2012
Cluster Operational State                    : Operational                 <<< Status of this
ANC
Interception Readiness State                 : Ready
Device Interception State                    : Not Shutdown                <<< Interception is
not shut down by CMM

Stable AC View:                                                            <<< Stable view of
converged ANCs
       10.1.1.1         10.1.1.2
Stable SN View:                                                            <<< Stable view of
converged WNs
       10.1.1.1         10.1.1.2
Current AC View:
       10.1.1.1         10.1.1.2
Current SN View:
       10.1.1.1         10.1.1.2         10.1.1.3
```

[Device Interception State]フィールド（上記）に[Shutdown]と表示されている場合は、このANCがトラフィックフローを受信する準備ができていないため、CMMがシャットダウン済みであることを意味します。たとえば、ANCはまだ参加プロセスにあり、クラスタのフローがまだ同期されていない可能性があります。

[安定表示(Stable View)]フィールド（上記）には、クラスタの最後の統合ビューで、このANCデバイスによって表示されるANCおよびWNのIPアドレスがリストされます。これは、ディストリビューション操作に使用されるビューです。[Current View]フィールドには、このANCによってアドバタイズされたデバイスがハートビートメッセージにリストされます。

ANCでshow service-insertion appnav-controller-groupコマンドを使用すると、ANCグループ内の各ANCのステータスを確認できます。

```
ANC# show service-insertion appnav-controller-group
All AppNav Controller Groups in Service Context
Service Context                              : test
Service Context configured state             : Enabled
```

```
AppNav Controller Group : scg
Member AppNav Controller count : 2
   Members:
       10.1.1.1        10.1.1.2

AppNav Controller                           : 10.1.1.1
AppNav Controller ID                        : 1
Current status of AppNav Controller         : Alive                     <<< Status of this ANC
Time current status was reached             : Wed Jul 11 02:05:23 2012
Joining status of AppNav Controller         : Joined                    <<< Joining means ANC
is still joining
Secondary IP address                        : 10.1.1.1                  <<< Source IP used in
cluster protocol packets
Cluster protocol ICIMP version              : 1.1
Cluster protocol Incarnation Number         : 2
Cluster protocol Last Sent Sequence Number  : 0
Cluster protocol Last Received Sequence Number: 0

Current AC View of AppNav Controller:                                    <<< ANC and WN
devices advertised by this ANC
       10.1.1.1        10.1.1.2
Current SN View of AppNav Controller:
       10.1.1.1        10.1.1.2

AppNav Controller                           : 10.1.1.2 (local)           <<< local indicates
this is the local ANC
AppNav Controller ID                        : 1
Current status of AppNav Controller         : Alive
Time current status was reached             : Wed Jul 11 02:05:23 2012
Joining status of AppNav Controller         : Joined
Secondary IP address                        : 10.1.1.2
Cluster protocol ICIMP version              : 1.1
Cluster protocol Incarnation Number         : 2
Cluster protocol Last Sent Sequence Number  : 0
Cluster protocol Last Received Sequence Number: 0

Current AC View of AppNav Controller:                                    <<< ANC and WN
devices advertised by this ANC
       10.1.1.1        10.1.1.2
Current SN View of AppNav Controller:
       10.1.1.1        10.1.1.2        10.1.1.3
```

ANCのステータスと参加ステータスのリストについては、『*Cisco Wide Area Application Servicesコマンドレファレンス*』のshow service-insertionコマンドを参照してください。

ANCでshow service-insertion service-nodeコマンドを使用すると、クラスタ内の特定のWNのステータスを確認できます。

```
ANC# show service-insertion service-node 10.1.1.2
Service Node:                               : 20.1.1.2
Service Node belongs to SNG                 : sng2
Service Context                             : test
Service Context configured state            : Enabled

Service Node ID                             : 1
Current status of Service Node              : Alive                     <<< WN is visible
Time current status was reached             : Sun May  6 11:58:11 2011
Cluster protocol DMP version                : 1.1
Cluster protocol incarnation number         : 1
Cluster protocol last sent sequence number  : 1692060441
Cluster protocol last received sequence number: 1441393061
```

```
AO state
--------
AO               State            For
--               -----            ---
tfo              GREEN            3d 22h 11m 17s                          <<< Overall/TFO state
reported by WN
epm              GREEN            3d 22h 11m 17s                          <<< AO states
reported by WN
cifs             GREEN            3d 22h 11m 17s
mapi             GREEN            3d 22h 11m 17s
http             RED              3d 22h 14m 3s
video            RED              11d 2h 2m 54s
nfs              GREEN            3d 22h 11m 17s
ssl              YELLOW           3d 22h 11m 17s
ica              GREEN            3d 22h 11m 17s
```

ANCでshow service-insertion service-node-groupコマンドを使用すると、クラスタ内の特定のWNGのステータスを確認できます。

```
ANC# show service-insertion service-node-group sng2
Service Node Group name   : sng2
Service Context             : scxt1
       Member Service Node count   : 1
       Members:
       10.1.1.1       10.1.1.2

Service Node:                                 : 10.1.1.1
Service Node belongs to SNG                   : sng2
Current status of Service Node                : Excluded                    <<< WN status
Time current status was reached               : Sun Nov  6 11:58:11 2011
Cluster protocol DMP version                  : 1.1
Cluster protocol incarnation number           : 1
Cluster protocol last sent sequence number    : 1692061851
Cluster protocol last received sequence number: 1441394001

AO state
--------
AO               State            For
--               -----            ---
tfo              GREEN            3d 22h 12m 52s
epm              GREEN            3d 22h 12m 52s
cifs             GREEN            3d 22h 12m 52s
mapi             GREEN            3d 22h 12m 52s
http             RED              3d 22h 15m 38s
video            RED              11d 2h 4m 29s
nfs              GREEN            3d 22h 12m 52s
ssl              YELLOW           3d 22h 12m 52s
ica              GREEN            3d 22h 12m 52s

Service Node:                                 : 10.1.1.2
Service Node belongs to WNG                   : sng2
Current status of Service Node                : Alive                       <<< WN status
Time current status was reached               : Sun Nov  6 11:58:11 2011
Cluster protocol DMP version                  : 1.1
Cluster protocol incarnation number           : 1
Cluster protocol last sent sequence number    : 1692061851
Cluster protocol last received sequence number: 1441394001

AO state
--------
```

```
AO              State           For
--              -----           ---
tfo             GREEN           3d 22h 12m 52s
epm             GREEN           3d 22h 12m 52s
cifs            GREEN           3d 22h 12m 52s
mapi            GREEN           3d 22h 12m 52s
http            RED             3d 22h 15m 38s
video           RED             11d 2h 4m 29s
nfs             GREEN           3d 22h 12m 52s
ssl             YELLOW          3d 22h 12m 52s
ica             GREEN           3d 22h 12m 52s

SNG Availability per AO                                    <<< AO status for entire
WNG
----------------------
AO              Available       Since
--              ---------       -----
tfo             Yes             3d 22h 12m 52s
epm             Yes             3d 22h 12m 52s
cifs            Yes             3d 22h 12m 52s
mapi            Yes             3d 22h 12m 52s
http            No              3d 22h 15m 38s
video           No              11d 2h 4m 29s
nfs             Yes             3d 22h 12m 52s
ssl             No              11d 2h 4m 29s
ica             Yes             3d 22h 12m 52s
```

上の例の最初のWNのステータスは[Excluded]です。これは、WNがANCに表示されますが、1つ以上の他のANCが表示できないため、クラスタから除外されることを意味します。

AOごとのSNG可用性の表は、各AOが新しい接続をサービスできるかどうかを示しています。AOは、WNGの少なくとも1つのWNがAOの緑色のステータスを持つ場合に使用できます。

WNでshow service-insertion service-nodeコマンドを使用すると、WNのステータスを確認できます。

```
WAE# show service-insertion service-node
Cluster protocol DMP version      : 1.1
Service started at                : Wed Jul 11 02:05:45 2012
Current FSM state                 : Operational                    <<< WN is responding to
health probes
Time FSM entered current state    : Wed Jul 11 02:05:45 2012
Last FSM state                    : Admin Disabled
Time FSM entered last state       : Mon Jul  2 17:19:15 2012
Shutdown max wait time:
               Configured        : 120
               Operational       : 120

Last 8 AppNav Controllers
-------------------------
AC IP             My IP            DMP Version  Incarnation  Sequence        Tim
e Last Heard
-----             -----            -----------  -----------  --------        ---
------------

Reported state                                                <<< TFO and AO reported states
--------------
Accl              State    For              Reason
----              -----    ---              ------
```

```
TFO (System)     GREEN    43d 7h 45m 8s
EPM              GREEN    43d 7h 44m 40s
CIFS             GREEN    43d 7h 44m 41s
MAPI             GREEN    43d 7h 44m 43s
HTTP             GREEN    43d 7h 44m 45s
VIDEO            GREEN    43d 7h 44m 41s
NFS              GREEN    43d 7h 44m 44s
SSL              RED      43d 7h 44m 21s
ICA              GREEN    43d 7h 44m 40s

Monitored state of Accelerators                                    <<< TFO and AO actual states
------------------------------
TFO (System)
       Current State: GREEN
       Time in current state: 43d 7h 45m 8s
EPM
       Current State: GREEN
       Time in current state: 43d 7h 44m 40s
CIFS
       Current State: GREEN
       Time in current state: 43d 7h 44m 41s
MAPI
       Current State: GREEN
       Time in current state: 43d 7h 44m 43s
HTTP
       Current State: GREEN
       Time in current state: 43d 7h 44m 45s
VIDEO
       Current State: GREEN
       Time in current state: 43d 7h 44m 41s
NFS
       Current State: GREEN
       Time in current state: 43d 7h 44m 44s
SSL
       Current State: RED
       Time in current state: 43d 7h 44m 21s
       Reason:
       AO is not configured
ICA
       Current State: GREEN
       Time in current state: 43d 7h 44m 40s
```

アクセラレータのモニタ状態は実際の状態ですが、報告される状態はシステム状態またはアクセラレータ状態の低さであるため異なる場合があります。

WNでの最適化のトラブルシューティングの詳細は、「最適化のトラブルシューティング」および「アプリケーションアクセラレーションのトラブルシューティング」の記事を参照してください。

フロー分散統計情報を監視するためのAppNav CLIコマンド

ANCのポリシーとフロー分散のトラブルシューティングには、次のCLIコマンドが役立ちます。

- **show policy-map type appnav** *policymap-name*：ポリシーマップ内の各クラスのポリシールールとヒットカウントを表示します。
- **show class-map type appnav** *class-name*：クラスマップ内の各一致条件の一致基準とヒットカウントを表示します。
- **show policy-sub-class type appnav** *level1-class-name level2-class-name*：ネストされたAppNavポリシーマップ内のクラスマップ内の各一致条件の一致基準とヒットカウントを表示

します。

- **show statistics class-map type appnav** *class-name*：クラスマップのトラフィック代行受信と分散統計情報を表示します。
- **show statistics policy-sub-class type appnav** *level1-class-name level2-class-name*：ネストされたAppNavポリシーマップ内のクラスマップに対するトラフィックの代行受信および分散統計情報を表示します。
- **show statistics pass-through type appnav**：各パススルー理由のAppNavトラフィック統計情報を表示します。
- **show appnav-controller flow-distribution**：定義されたポリシーおよび動的負荷条件に基づいて、特定の仮想フローがANCによってどのように分類および分散されるかを示します。このコマンドは、特定のフローがANCでどのように処理され、どのクラスに属するかを確認するのに役立ちます。

フロー分散のトラブルシューティングを行うには、WNで次のコマンドを使用します。

- **show statistics service-insertion service-node** *ip-address*：アクセラレータとWNに分散されたトラフィックの統計情報を表示します。
- **show statistics service-insertion service-node-group name** *group-name*：アクセラレータとWNGに配信されるトラフィックの統計情報を表示します。

show statistics class-map type appnav *class-name*コマンドをANCで使用して、フロー分散のトラブルシューティングを行い、たとえば、特定のクラスでトラフィックが遅くなる理由を判別できます。これは、HTTPなどのアプリケーションクラスマップである可能性があります。また、ブランチへのすべてのトラフィックが遅いと思われる場合は、ブランチアフィニティクラスマップである可能性があります。HTTPクラスの例を次に示します。

```
ANC# show statistics class-map type appnav HTTP
Class Map                         From Network to SN   From SN to Network
                                  ------------------   ------------------
HTTP
 Redirected Client->Server:
   Bytes                                    3478104             11588180
   Packets                                    42861                102853
 Redirected Server->Client:
   Bytes                                 1154109763              9842597
   Packets                                   790497                60070

Connections
-----------
   Intercepted by ANC                                          4        <<< Are connections
being intercepted?
   Passed through by ANC                                       0        <<< Passed-through
connections
   Redirected by ANC                                           4        <<< Are connections
being distributed to WNs?
   Accepted by SN                                              4        <<< Connections accepted
by WNs
   Passed through by SN (on-Syn)                               0        <<< Connections might be
passed through by WNs
   Passed through by SN (post-Syn)                             0        <<< Connections might be
passed through by WNs


Passthrough Reasons                    Packets            Bytes        <<< Why is ANC passing
through connections?
```

```
------------------                      -------          -----
Collected by ANC:
  PT Flow Learn Failure                        0              0      <<< Asymmetric
connection; interception problem
  PT Cluster Degraded                          0              0      <<< ANCs cannot
communicate
  PT SNG Overload                              0              0      <<< All WNs in the WNG
are overloaded
  PT AppNav Policy                             0              0      <<< Connection policy is
pass-through
  PT Unknown                                   0              0      <<< Unknown passthrough

Indicated by SN:                                                    <<< Why are WNs passing
through connections?
  PT No Peer                                   0              0      <<< List of WN pass-
through reasons
  ...
```

[Indicated by SN]セクションのWNパススルーの理由は、パススルーオフロードがWNに設定されている場合にのみ増加します。そうしないと、ANCはWNが接続を通過していることを認識せず、カウントしません。

[Connections:ANCカウンタによってインターセプトされたパケットは増加しておらず、インターセプトの問題があります。WAAS TcpTracerouteユーティリティを使用すると、ネットワーク内でのANCの配置のトラブルシューティング、非対称パスの検索、接続に適用されるポリシーの決定を行うことができます。詳細については、「接続トレース」の項を参照してください。

接続をデバッグするためのAppNav CLIコマンド

ANC上の個々の接続または一連の接続をデバッグするには、**show statistics appnav-controller connection**コマンドを使用してアクティブな接続リストを表示します。

```
anc# show statistics appnav-controller connection
Collecting Records. Please wait...
Optimized Flows:
------------------------
Client                Server               SN-IP                AC Owned

2.30.5.10:38111       2.30.1.10:5004       2.30.1.21            Yes
2.30.5.10:38068       2.30.1.10:5003       2.30.1.21            Yes
2.30.5.10:59861       2.30.1.10:445        2.30.1.21            Yes
2.30.5.10:59860       2.30.1.10:445        2.30.1.21            Yes
2.30.5.10:43992       2.30.1.10:5001       2.30.1.5             Yes
2.30.5.10:59859       2.30.1.10:445        2.30.1.21            Yes
2.30.5.10:59858       2.30.1.10:445        2.30.1.21            Yes
2.30.5.10:59857       2.30.1.10:445        2.30.1.21            Yes
2.30.5.10:59856       2.30.1.10:445        2.30.1.21            Yes

Passthrough Flows:
------------------------
Client                Server               Passthrough Reason
2.30.5.10:41911       2.30.1.10:5002       PT Flowswitch Policy
```

クライアントまたはサーバーのIPアドレスまたはポートオプションを指定してリストをフィルタし、**detail**キーワードを指定して接続に関する詳細な統計を表示できます。

```
anc# show statistics appnav-controller connection server-ip 2.30.1.10 detail
```

```
Collecting Records. Please wait...

Optimized Flows
--------------------------
Client: 2.30.5.10:55330
Server: 2.30.1.10:5001
AppNav Controller Owned: Yes        <<< This ANC is seeing activity on this connection
Service Node IP:2.30.1.5            <<< Connection is distributed to this SN
Classifier Name: se_policy:p5001    <<< Name of matched class map
Flow association: 2T:No,3T:No       <<< Connection is associated with dynamic app or session
(MAPI and ICA only)?
Application-ID: 0                   <<< AO that is optimizing the connection
Peer-ID: 00:14:5e:84:41:31          <<< ID of the optimizing peer

Client: 2.30.5.10:55331
Server: 2.30.1.10:5001
AppNav Controller Owned: Yes
Service Node IP:2.30.1.5
Classifier Name: se_policy:p5001
Flow association: 2T:No,3T:No
Application-ID: 0
Peer-ID: 00:14:5e:84:41:31
...
```

集約オプションを指定すると、アクティブな分散接続とパススルー接続の数を表示できます。

```
anc# show statistics appnav-controller connection summary
Number of optimized flows    = 2
Number of pass-through flows = 17
```

接続トレース

AppNavフローのトラブルシューティングを支援するために、Central Managerの接続トレースツールを使用できます。このツールは、特定の接続に関する次の情報を表示します。

- 接続がWNGを通過したか、WNGに配布された場合
- パススルーの理由（該当する場合）
- 接続が配布されたWNGとWN
- 接続を監視するアクセラレータ
- クラスマップを適用

接続トレースツールを使用するには、次の手順を実行します。

1. Central Managerメニューから、[AppNav Clusters] > [*cluster-name]を選択*し、[Monitor] > [Tools] > [Connection Trace]を選択します。

2. ANC、ピアWAASデバイスを選択し、接続一致基準を指定します。

3. [トレース]をクリックして、一致する接続を表示します。

WAAS TCP Tracerouteは、非対称パスを含むネットワークおよび接続の問題のトラブルシューティングに役立つAppNav固有のツールではありません。これを使用して、クライアントとサーバの間のWAASノードのリスト、および接続に対して設定および適用された最適化ポリシーを検索できます。Central Managerから、tracerouteを実行するWAASネットワーク内の任意のデバイスを選択できます。WAAS Central Manager TCP Tracerouteツールを使用するには、次の手順を実行します。

1. WAAS Central Managerメニューから、**[Monitor] > [Troubleshoot] > [WAAS Tcptraceroute]を選択します**。または、最初にデバイスを選択してから、このメニュー項目を選択して、そのデバイスからtracerouteを実行することもできます。

2. [WAAS Node]ドロップダウンリストから、tracerouteを実行するWAASデバイスを選択します。（デバイスコンテキスト内の場合、この項目は表示されません）。

3. [Destination IP]および[Destination Port]フィールドに、tracerouteを実行する宛先のIPアドレスとポートを入力します

4. [Run TCPTraceroute]をクリ**ックし、**結果を表示します。

トレースされたパスのWAASノードが、フィールドの下の表に表示されます。このユーティリティは、**waas-tcptrace**コマンドを使用してCLIから実行することもできます。

AppNavデバッグログ

AppNavクラスタマネージャの問題のトラブルシューティングには、次のログファイルを使用できます。

- デバッグログファイル：/local1/errorlog/cmm-errorlog.current（およびcmm-errorlog.*）

AppNavクラスタマネージャのデバッグログを設定および有効にするには、次のコマンドを使用します。

注：デバッグロギングはCPUに負荷がかかり、大量の出力を生成する可能性があります。実稼働環境では慎重に慎重に使用してください。

ディスクへの詳細な口ギングを有効にできます。

```
WAE(config)# logging disk enable
WAE(config)# logging disk priority detail
```

クラスタマネージャデバッグ(5.0.1以降)のオプションは次のとおりです。

```
WAE# debug cmm ?
 all      enable all CMM debugs
 cli      enable CMM cli debugs
 events   enable CMM state machine events debugs
 ipc      enable CMM ipc messages debugs
 misc     enable CMM misc debugs
 packets  enable CMM packet debugs
 shell    enable CMM infra debugs
 timers   enable CMM state machine timers debugs
```

クラスタマネージャのデバッグロギングを有効にして、デバッグエラーログの最後を次のように表示できます。

```
WAE# debug cmm all
WAE# type-tail errorlog/cmm-errorlog.current follow
```

次のコマンドを使用して、フロー分散マネージャ(FDM)またはフロー分散エージェント(FDA)のデバッグロギングを有効にすることもできます。

```
WAE# debug fdm all
WAE# debug fda all
```

FDMは、WNのポリシーおよび動的ロード条件に基づいて、フローの配布場所を決定します。FDAはWNロード情報を収集します。FDMおよびFDAの問題のトラブルシューティングには、次のログ・ファイルを使用できます。

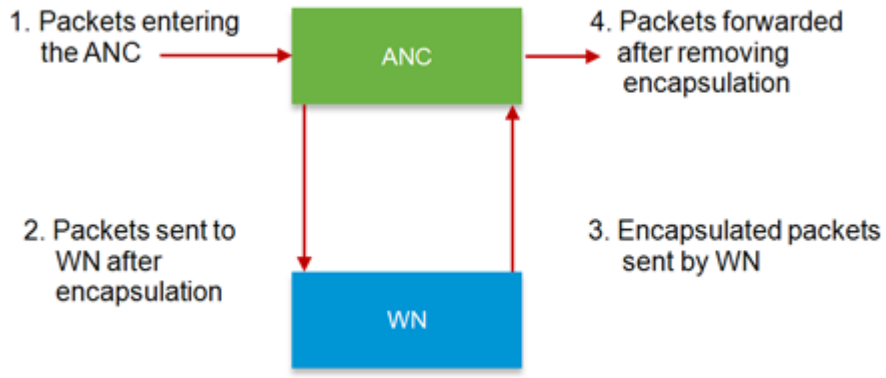
- デバッグログファイル：/local1/errorlog/fdm-errorlog.current（およびfdm-errorlog.*）
- デバッグログファイル：/local1/errorlog/fda-errorlog.current（およびfda-errorlog.*）

AppNavパケットキャプチャ

Cisco AppNavコントローラのインターフェースモジュールのインターフェイスでデータパケットをキャプチャできるように、新しいpacket-captureコマンドが導入されました。このコマンドは、他のインターフェイスのパケットをキャプチャしたり、パケットキャプチャファイルをデコードしたりすることもできます。**packet-captureコマンド**は、Cisco AppNavコントローラインターフェイスモジュールでパケットをキャプチャできない、非推奨のコマンド**tcpdump**および**ethereal**よりも優先されます。コマンド構文の詳細については、*『Cisco Wide Area Application Servicesコマンドレフェレンス』*を参照してください。

注：パケットキャプチャまたはデバッグキャプチャはアクティブにできますが、両方を同時にアクティブにすることはできません。

次の図に示すように、ANCとWNの間で送信されるデータパケットはカプセル化されます。



図のポイント1または4でパケットをキャプチャすると、カプセル化は解除されます。ポイント2または3でパケットをキャプチャすると、カプセル化されます。

カプセル化パケットキャプチャの出力例を次に示します。

```
anc# packet-capture appnav-controller interface GigabitEthernet 1/0 access-list all
Packet-Capture: Setting virtual memory/file size limit to 419430400
Running as user "admin" and group "root". This could be dangerous.
Capturing on eth14
 0.000000    2.58.2.11 -> 2.1.6.122    TCP https > 2869 [ACK] Seq=1 Ack=1 Win=65535 Len=0
 4.606723   2.58.2.175 -> 2.43.64.21   TELNET Telnet Data ...
...
 37.679587    2.58.2.40 -> 2.58.2.35    GRE Encapsulated 0x8921 (unknown)
 37.679786    2.58.2.35 -> 2.58.2.40    GRE Encapsulated 0x8921 (unknown)
```

カプセル化されていないパケットキャプチャの出力例を次に示します。

```
anc# packet-capture appnav-controller access-list all non-encapsulated
Packet-Capture: Setting virtual memory/file size limit to 419430400
Running as user "admin" and group "root". This could be dangerous.
Capturing on eth14
0.751567   2.58.2.175 -> 2.43.64.21   TELNET Telnet Data ...
1.118363   2.58.2.175 -> 2.43.64.21   TELNET Telnet Data ...
1.868756   2.58.2.175 -> 2.43.64.21   TELNET Telnet Data ...
...
```

パケットキャプチャガイドライン：

- パケットキャプチャACLは、WCCP-GREおよびSIAカプセル化パケットの内部IPパケットに常に適用されます。
- パケットキャプチャ用のANCインターフェイスが提供されていない場合、すべてのANCインターフェイスでパケットキャプチャが実行されます。

WNインターフェイスでのパケットキャプチャの出力例を次に示します。

```
anc# packet-capture interface GigabitEthernet 0/0 access-list 10
Packet-Capture: Setting virtual memory/file size limit to 419430400
Running as user "admin" and group "root". This could be dangerous.
Capturing on eth0
  0.000000      2.1.8.4 -> 2.64.0.6     TELNET Telnet Data ...
  0.000049     2.64.0.6 -> 2.1.8.4      TELNET Telnet Data ...
  0.198908      2.1.8.4 -> 2.64.0.6     TCP 18449 > telnet [ACK] Seq=2 Ack=2 Win=3967 Len=0
  0.234129      2.1.8.4 -> 2.64.0.6     TELNET Telnet Data ...
  0.234209     2.64.0.6 -> 2.1.8.4      TELNET Telnet Data ...
```

パケットキャプチャファイルをデコードする例を次に示します。

```
anc# packet-capture decode /local1/se_flow_add.cap
Running as user "admin" and group "root". This could be dangerous.  1   0.000000
     100.1.1.2 -> 100.1.1.1    GRE Encapsulated SWIRE  2   0.127376
     100.1.1.2 -> 100.1.1.1    GRE Encapsulated SWIRE
```

パケットをフィルタリングするために、src-ip/dst-ip/src-port/dst-portを指定できます。

anc# packet-capture decode source-ip 2.64.0.33 /local1/hari_pod_se_flow.cap

```
Running as user "admin" and group "root". This could be dangerous.
3   0.002161    2.64.0.33 -> 2.64.0.17    TCP 5001 > 33165 [SYN, ACK] Seq=0 Ack=1
Win=5792 Len=0 MSS=1460 TSV=326296092 TSER=326296080 WS=4
4   0.002360    2.64.0.33 -> 2.64.0.17    TCP 5001 > 33165 [SYN, ACK] Seq=0 Ack=1
Win=5792 Len=0 MSS=1406 TSV=326296092 TSER=326296080 WS=4
```