Cisco WAAS-Fehlerbehebungsleitfaden für Version 4.1.3 und höher

Kapitel: Fehlerbehebung AppNav

In diesem Artikel wird die Fehlerbehebung bei einer AppNav-Bereitstellung beschrieben.

Inhalt

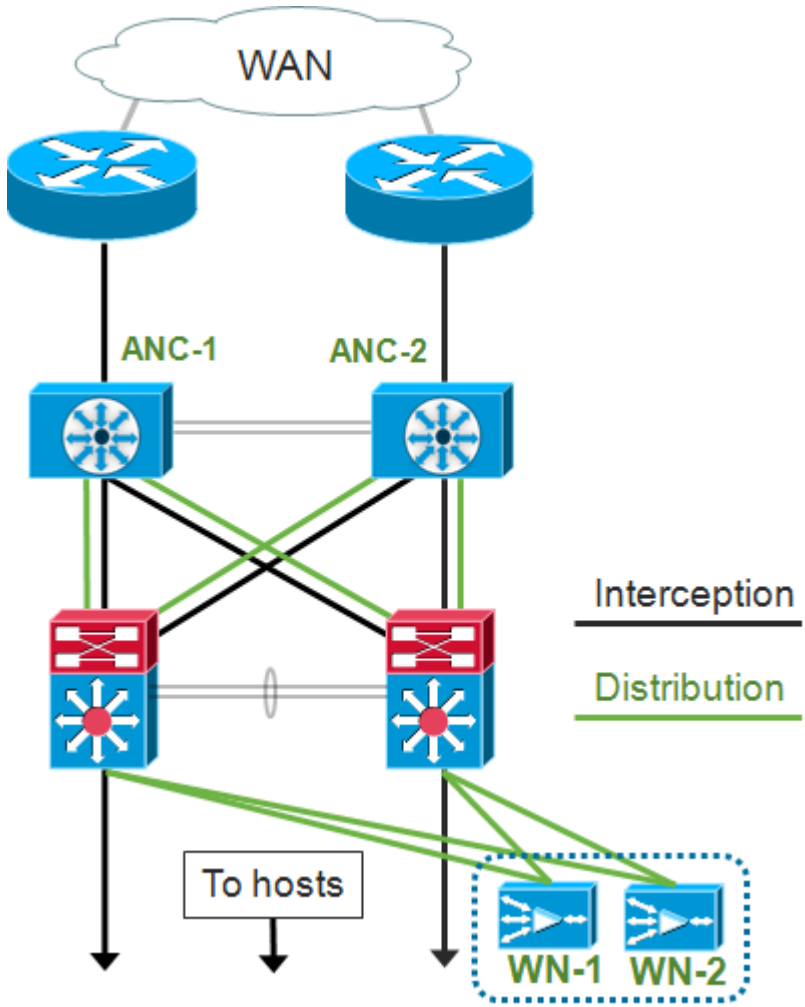
AppNav-Fehlerbehebung

Cisco WAAS AppNav vereinfacht die Netzwerkintegration der WAN-Optimierung und reduziert die Abhängigkeit vom Intercepting-Switch oder -Router durch die Verwendung von AppNav-Controllern (ANCs) für die Verteilung des Datenverkehrs zwischen WAAS-Nodes (WNs) zur Optimierung mithilfe eines leistungsstarken Klassen- und Richtlinienmechanismus. Sie können WAAS-Knoten (WNs) verwenden, um den Datenverkehr basierend auf Standorten und/oder Anwendungen zu optimieren. In diesem Artikel wird die Fehlerbehebung für AppNav beschrieben.

HINWEIS: Die AppNav-Funktion wurde in WAAS Version 5.0.1 eingeführt. Dieser Abschnitt gilt nicht für frühere WAAS-Versionen.

In-Path-Interception (Inline)

Im Inline-Modus sind ANCs im Pfad des Netzwerkverkehrs positioniert, wo sie Pakete abfangen und an WNs verteilen.



Bei der Schnittstellenkonfiguration für eine Inline-Bereitstellung werden die Interception- und Verteilungsrollen separaten Schnittstellen im Cisco AppNav-Controller-Schnittstellenmodul zugewiesen. Für das Abfangen ist eine Bridge-Group-Schnittstelle erforderlich, die aus zwei oder mehr physischen oder Port-Channel-Schnittstellen oder jeweils einer besteht. Die Bridge-Group-

Schnittstelle bietet keine Möglichkeit zum Verdrahten. d. h., der Datenverkehr wird nach einem Geräteausfall oder Stromausfall nicht mechanisch überbrückt. AppNav stellt mithilfe von Clustering eine hohe Verfügbarkeit bereit, wenn das AppNav-Controller-Schnittstellenmodul, der Verbindungspfad oder die Verbindung zum AppNav-Controller-Schnittstellenmodul verloren gehen oder ein Stromausfall vorliegt.

Hinweis: Bridge-Schnittstellen blockieren keine BPDU-Pakete (Bridge Protocol Data Unit). Bei redundanten Schnittstellen, die Schleifen erstellen, wird eine der Schnittstellen durch das Spanning Tree Protocol blockiert.

Die Fehlerbehebung bei Inline-Interception besteht aus den folgenden Schritten:

- Überprüfen Sie das Netzwerkdesign, um die korrekte Inline-Platzierung des ANC zu überprüfen. Verwenden Sie bei Bedarf grundlegende Tools wie Ping und Traceroute oder Layer-7-Tools oder -Anwendungen, um sicherzustellen, dass der Netzwerkverkehrspfad wie erwartet verläuft. Prüfen Sie die physische Verkabelung des ANC.
- Stellen Sie sicher, dass der ANC auf den Inline-Abfangmodus eingestellt ist.
- Überprüfen Sie, ob die Bridge-Group-Schnittstelle richtig konfiguriert ist.

Die beiden letzten Schritte können entweder in Central Manager oder in der Befehlszeile ausgeführt werden, wobei der Central Manager die bevorzugte Methode ist und zuerst beschrieben wird.

Wählen Sie im Central Manager **Devices >** AppNavController aus, und wählen Sie **Configure > Interception > Interception Configuration aus**. Überprüfen Sie, ob die Interception-Methode auf Inline eingestellt ist.

Überprüfen Sie im gleichen Fenster, ob eine Bridge-Schnittstelle konfiguriert ist. Wenn eine Bridge-Schnittstelle erforderlich ist, klicken Sie auf **Create Bridge (Bridge erstellen)**, um sie zu erstellen. Sie können der Bridge-Gruppe bis zu zwei Mitgliedsschnittstellen zuweisen. Sie können den VLAN-Rechner verwenden, um die VLAN-Einträge auf Basis von Einschließen- oder Ausschlussvorgängen zu definieren. Beachten Sie, dass der Bridge-Schnittstelle keine IP-Adresse zugewiesen wird.

Verwenden Sie den Befehl Alarm Panel oder **show alarm** exec, um zu überprüfen, ob Bridge-Alarme auf dem Gerät ausgelöst werden. Ein bridge_down-Alarm gibt an, dass eine oder mehrere Mitgliedschnittstellen in der Bridge inaktiv sind.

Führen Sie über die CLI die folgenden Schritte aus, um den Inline-Betrieb zu konfigurieren:

1. Legen Sie die Interception-Methode auf inline fest:

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

2. Erstellen Sie die Bridge-Group-Schnittstelle:

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

3. (Optional) Geben Sie die Liste der VLANs an, die bei Bedarf abgefangen werden sollen:

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

4. Fügen Sie der Bridge-Gruppen-Schnittstelle zwei logische/physische Schnittstellen hinzu:

```
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
```

Sie können den Betriebsstatus der Bridge-Schnittstelle mit dem Befehl **show bridge** exec überprüfen und Statistiken zur Bridge anzeigen.

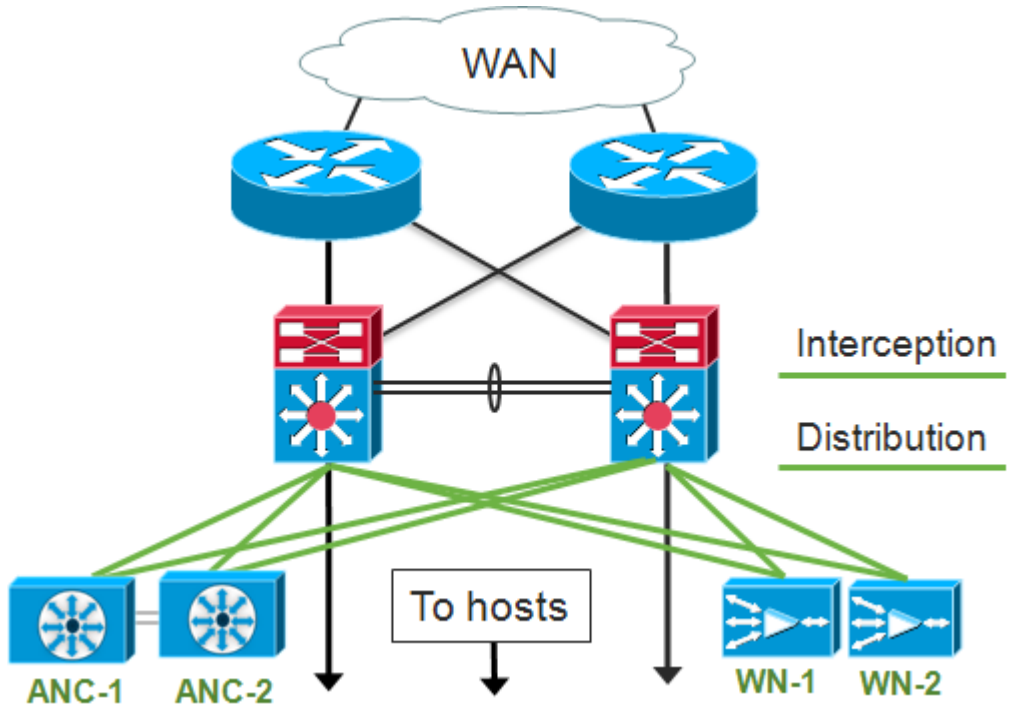
```
wave# show bridge 1
lsp: Link State Propagation
flow sync: AppNav Controller is in the process of flow sync
Member Interfaces:
 GigabitEthernet 1/0
 GigabitEthernet 1/1
Link state propagation: Enabled
VLAN interception:
 intercept vlan-id all                                                    <<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

Im obigen Beispiel ist die Gig 1/0-Schnittstelle ausgefallen, und die Gig 1/1-Schnittstelle ist aufgrund der Link State Propagation (LSP) ebenfalls inaktiv. Sie können auch Down (Flow Sync) sehen, was bedeutet, dass die ANC einem Cluster beitritt und Flow-Informationen mit anderen ANCs im Cluster synchronisiert. Der Abfangpfad (Bridge-Schnittstelle) bleibt etwa zwei Minuten lang geschlossen, bis alle ANCs synchronisiert sind, sodass bestehende Datenflüsse korrekt verteilt werden können.

Der untere Teil der Ausgabe zeigt Datenverkehrsstatistiken für die Mitgliedschnittstellen.

Off-Path (WCCP)-Interception

Im WCCP-Modus sind WCCP-Router im Pfad des Netzwerkverkehrs positioniert, wo sie Pakete abfangen und an ANCs umleiten, die sich außerhalb des Pfades befinden. Da AppNav die Interception-Verarbeitung, die intelligente Flussverteilung und Lastüberlegung zwischen WAAS-Beschleunigern übernimmt, wird die WCCP-Konfiguration auf den Routern erheblich vereinfacht.



In der Schnittstellenkonfiguration für eine Off-Path-Bereitstellung können die Interception- und Verteilungsrollen dieselben Schnittstellen auf dem Cisco AppNav-Controller-Schnittstellenmodul verwenden, dies ist jedoch nicht erforderlich.

Die Fehlerbehebung bei der Off-Path-Interception besteht aus den folgenden Schritten:

- Überprüfen Sie die korrekte Platzierung der WCCP-Router, um sicherzustellen, dass sie sich im Pfad des Datenverkehrs zu und von den optimierten Hosts befinden. Sie können die Befehle **show run** oder **show wccp** verwenden, um zu überprüfen, ob es sich um dieselben Router handelt, die für WCCP konfiguriert sind. Verwenden Sie bei Bedarf grundlegende Tools wie Ping und Traceroute oder Layer-7-Tools oder -Anwendungen, um sicherzustellen, dass der gesamte Datenverkehr, der optimiert werden muss, über die WCCP-Router geleitet wird.
- Überprüfen Sie die WCCP-Konfiguration auf den WAAS-ANCs mithilfe der zentralen Verwaltungsschnittstelle (bevorzugt) oder der CLI.
- Überprüfen Sie die WCCP-Konfiguration auf den umleitenden Routern mithilfe der Router-CLI.

Um die WCCP-Konfiguration auf den ANCs zu überprüfen, wählen Sie im zentralen Manager **Geräte >** AppNavController aus, und wählen Sie **Configure > Interception > Interception Configuration aus**.

- Stellen Sie sicher, dass die Interception Method auf WCCP festgelegt ist.
- Überprüfen Sie, ob das Kontrollkästchen WCCP-Dienst aktivieren aktiviert ist.
- Stellen Sie sicher, dass das Kontrollkästchen Default Gateway als WCCP-Router verwenden aktiviert ist oder dass die IP-Adressen des WCCP-Routers im Feld WCCP-Router aufgeführt sind.
- Überprüfen Sie, ob die anderen Einstellungen, z. B. die Load Balancing Maske und die Umleitungsmethode, für Ihre Bereitstellung korrekt konfiguriert sind.

Prüfen Sie, ob WCCP-Alarme auf den ANCs vorhanden sind, die Teil der Router-WCCP-Farm sind. Klicken Sie in der zentralen Verwaltungsschnittstelle unten im Bildschirm auf den Bereich Alarme, oder verwenden Sie den Befehl **show alarm** auf jedem Gerät, um Alarme anzuzeigen. Korrigieren Sie alle Alarmbedingungen, indem Sie die Konfiguration auf dem ANC oder Router

nach Bedarf ändern.

Führen Sie in der CLI die folgenden Schritte aus, um den WCCP-Betrieb zu konfigurieren:

1. Legen Sie die Abfangmethode auf wccp fest.

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

2. Konfigurieren Sie die WCCP-Routerliste, die die IP-Adressen der Router enthält, die zur WCCP-Farm gehören.

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

3. Konfigurieren Sie die WCCP-Dienst-ID. Eine einzige Service-ID wird für AppNav bevorzugt, obwohl zwei Service-IDs unterstützt werden.

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

4. Ordnen Sie die konfigurierte Routerliste dem WCCP-Dienst zu.

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

5. Konfigurieren Sie die WCCP-Zuweisungsmethode (nur die Maskenmethode wird von einem ANC unterstützt). Wenn Sie die Optionen dst-ip-mask oder src-ip-mask nicht angeben, wird die IP-Standardmaske für die Quelle auf f und die IP-Zielmaske auf 0 gesetzt.

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

6. Konfigurieren Sie die WCCP-Umleitungsmethode (die Egress- und die Return-Methode werden automatisch auf die Umleitungsmethode festgelegt und können nicht für eine ANC konfiguriert werden). Sie können L2 (Standard) oder GRE auswählen. L2 erfordert, dass das ANC über eine Layer-2-Verbindung mit dem Router verfügt und der Router auch für die Layer-2-Umleitung konfiguriert ist.

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

7. Aktivieren Sie den WCCP-Dienst.

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

Überprüfen Sie die WCCP-Interception für jede ANC mithilfe des Befehls **show running-config**. Die beiden folgenden Beispiele zeigen die aktuelle Konfigurationsausgabe für die L2-Umleitung und die GRE-Umleitung.

show running-config wccp (für L2-Umleitung):

```
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 (für GRE):

```
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
```

Überprüfen Sie den WCCP-Status für jede ANC mit dem Befehl **show wccp status**.

```
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
```

Überprüfen Sie die Router, die auf die Keepalive-Nachrichten in der WCCP-Farm reagiert haben, mithilfe des Befehls **show wccp routers**.

```
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-
```

Überprüfen Sie die Ansicht der anderen ANCs in der WCCP-Farm und der von den einzelnen ANCs erreichbaren Router mithilfe des Befehls **show wccp clients**.

```
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
```

Stellen Sie sicher, dass alle ANCs Pakete von den Routern in der Farm erhalten, indem Sie den Befehl **show statistics wccp** verwenden. Es werden Statistiken für Datenverkehr angezeigt, der von den einzelnen Routern empfangen, weitergeleitet und an diese gesendet wird. Die kumulativen Statistiken für alle Router in der Farm sind unten aufgeführt. Ein ähnlicher Befehl ist **show wccp statistics**. Beachten Sie, dass "OE" sich hier auf die ANC-Geräte bezieht.

```
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
```

Konfigurieren und Überprüfen des WCCP-Interception auf dem Router

Führen Sie die folgenden Schritte aus, um die WCCP-Interception auf jedem Router in der WCCP-Farm zu konfigurieren.

1. Konfigurieren Sie den WCCP-Dienst auf dem Router mithilfe des Befehls **ip wccp** router.

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

2. Konfigurieren der WCCP-Interception an den Router-LAN- und WAN-Schnittstellen Sie können

auf beiden Schnittstellen dieselbe Service-ID konfigurieren, wenn Sie eine einzige Service-ID für die ANCs verwenden.

```
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
```

3. (Optional) Konfigurieren Sie eine Tunnelschnittstelle, wenn Sie generische GRE-Ausgänge verwenden (nur wenn Sie GRE für die ANC WCCP-Umleitungsmethode ausgewählt haben).

```
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
```

Überprüfen Sie die WCCP-Konfiguration auf jedem Router in der Farm mithilfe des Befehls **show wccp**.

```
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
```

Zusätzliche Informationen

Weitere Informationen finden Sie in den folgenden Dokumenten:

- WCCP-Netzwerkintegration mit Cisco Catalyst 6500: Best Practice-Empfehlungen für erfolgreiche Bereitstellungen
- Umleitung des Cisco Wide Area Application Services Web Cache Communication Protocol: Unterstützung der Cisco Router-Plattform
- Konfigurieren erweiterter WCCP-Funktionen auf Routern im *Cisco Wide Area Application Services Configuration Guide*
- Konfigurieren von WCCP auf WAEs im *Cisco Wide Area Application Services Configuration Guide*

Fehlerbehebung bei Netzwerkverbindungen

Bei der Fehlerbehebung für WAAS kann es hilfreich sein, festzustellen, wie sich das Netzwerk verhält, wenn WAAS deaktiviert ist. Dies ist hilfreich, wenn der Datenverkehr nicht nur nicht optimiert, sondern überhaupt nicht erreicht wird. In diesen Fällen stellt sich möglicherweise heraus, dass das Problem nicht mit WAAS zusammenhängt. Selbst bei eingehenden Datenverkehrsströmen kann diese Technik helfen festzustellen, welche WAAS-Geräte eine Fehlerbehebung erfordern.

Überprüfen Sie vor dem Testen der Layer-3-Konnektivität, ob das AppNav-Controller-Schnittstellenmodul mit den richtigen Switch-Ports verbunden ist. Wenn der verbundene Switch das Cisco Discovery Protocol (CDP) unterstützt und aktiviert ist, führen Sie den Befehl **show cdp neighbors detail aus,** um die ordnungsgemäße Verbindung zum Netzwerk-Switch zu überprüfen.

Eine Deaktivierung von WAAS ist möglicherweise nicht in allen Fällen möglich. Wenn ein Teil des Datenverkehrs optimiert wird und andere nicht, kann es inakzeptabel sein, WAAS zu deaktivieren und damit den Datenverkehr zu unterbrechen, der erfolgreich optimiert wurde. In einem solchen Fall kann die Abfangen-ACL oder die AppNav-Richtlinie verwendet werden, um den spezifischen Typ des Datenverkehrs zu durchlaufen, bei dem Probleme auftreten. Weitere Informationen finden Sie im Abschnitt Durchlaufen eines bestimmten Datenverkehrs.

Zum Deaktivieren von WAAS werden für den Inline-Modus andere Schritte als für den Off-Path-Modus ausgeführt:

- Im Inline-Modus muss die Interception Bridge in den Pass-Through-Zustand versetzt werden. Weitere Informationen finden Sie im Abschnitt Deaktivieren einer Inline-ANC.
- Für den Off-Path-Modus muss das WCCP-Protokoll deaktiviert werden. Weitere Informationen finden Sie im Abschnitt Deaktivieren eines Off-Path-ANC.

In AppNav-Umgebungen müssen nur die ANCs deaktiviert werden. WNs müssen nicht deaktiviert werden, da sie nicht am Abfangen teilnehmen.

Wenn WAAS deaktiviert ist, überprüfen Sie die Netzwerkverbindung mit Standardmethoden.

- Überprüfen Sie die Layer-3-Konnektivität mithilfe von Tools wie Ping und Traceroute.
- Überprüfen Sie das Anwendungsverhalten, um Verbindungen auf höherer Ebene zu ermitteln.
- Wenn im Netzwerk dieselben Verbindungsprobleme auftreten wie bei aktivierter WAAS, ist das Problem höchstwahrscheinlich nicht mit WAAS in Zusammenhang zu bringen.
- Wenn das Netzwerk mit deaktivierter WAAS-Funktion einwandfrei arbeitet, aber Verbindungsprobleme mit aktivierter WAAS aufwies, gibt es möglicherweise ein oder mehrere WAAS-Geräte, die Ihre Aufmerksamkeit erfordern. Der nächste Schritt besteht darin, das Problem auf bestimmte WAAS-Geräte zu isolieren.
- Wenn das Netzwerk über Verbindungen mit und ohne WAAS-Aktivierung verfügt, jedoch keine Optimierung erfolgt, sind wahrscheinlich ein oder mehrere WAAS-Geräte zu beachten. Der nächste Schritt besteht darin, das Problem auf bestimmte WAAS-Geräte zu isolieren.

Um das Netzwerkverhalten bei aktivierter WAAS zu überprüfen, gehen Sie wie folgt vor:

1. Aktivieren Sie die WAAS-Funktionalität auf den WAAS-ANCs und ggf. den WCCP-Routern wieder.

2. Wenn Sie festgestellt haben, dass ein WAAS-bezogenes Problem vorliegt, aktivieren Sie jeden AppNav-Cluster und/oder ANC einzeln, um dieses als potenzielle Ursache des beobachteten Problems zu isolieren.

3. Wenn jede ANC aktiviert ist, führen Sie die gleichen grundlegenden Netzwerkverbindungstests wie in früheren Schritten durch, und stellen Sie fest, ob diese spezielle ANC ordnungsgemäß zu funktionieren scheint. Machen Sie sich derzeit nicht mit individuellen WNs beschäftigt. In dieser Phase soll ermittelt werden, welche Cluster und welche spezifischen ANCs ein erwünschtes oder unerwünschtes Verhalten erleben.

4. Wenn jede ANC aktiviert und getestet ist, deaktivieren Sie sie erneut, damit die nächste aktiviert werden kann. Durch die Aktivierung und das Testen jeder ANC wiederum können Sie bestimmen, welche weitere Fehlerbehebung erforderlich sind.

Dieses Verfahren zur Fehlerbehebung ist vor allem in Situationen anzuwenden, in denen die WAAS-Konfiguration nicht nur nicht optimiert werden kann, sondern auch Probleme mit der normalen Netzwerkverbindung verursacht.

Weiterleitung durch bestimmten Datenverkehr

Sie können bestimmten Datenverkehr durchlaufen, indem Sie entweder eine Abhörkontrollliste verwenden oder die AppNav-Richtlinie für die Weiterleitung konfigurieren.

- Erstellen Sie eine ACL, die den zu durchgebenden Datenverkehr blockiert und alle anderen Vorgänge zulässt. In diesem Beispiel möchten wir den HTTP-Datenverkehr (Ziel-Port 80) weiterleiten. Legen Sie die ACL für die ACL für die ACL-Interception-Zugriffsliste fest. Verbindungen, die für Port 80 bestimmt sind, werden weitergeleitet. Sie können den Befehl **show statistics pass-through type appnav** verwenden, um zu überprüfen, ob der Passthrough-Vorgang stattfindet, indem Sie überprüfen, ob die Zähler für die PT-Intercept-ACL

inkrementiert sind.

```
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
```

- Konfigurieren Sie die ANC-Richtlinie so, dass Datenverkehr, der bestimmten Klassen entspricht, weitergeleitet wird.

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

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

Deaktivieren einer Inline-ANC

Es gibt mehrere Möglichkeiten, eine Inline-ANC zu deaktivieren, indem sie in den Pass-Through-Zustand versetzt wird:

- Legen Sie die VLAN-Liste der Interception Bridge auf none fest. Wählen Sie in Central Manager ein ANC-Gerät aus, und wählen Sie **Configure > Interception > Interception Configuration aus**. Wählen Sie die Bridge-Schnittstelle aus, und klicken Sie auf das Symbol **Edit** taskbar. Legen Sie im Feld VLANs den Wert "none" fest.
- Deaktivieren Sie den Dienstkontext, der die ANC enthält. Wählen Sie in der zentralen Verwaltungsschnittstelle einen Cluster aus, klicken Sie dann auf die Registerkarte AppNav-Controller, wählen Sie eine ANC aus, und klicken Sie auf das Symbol **Disable** taskbar.
- Wenden Sie eine Abhörkontrollliste mit den Kriterien "ALLE ablehnen" an. Diese Methode wird bevorzugt. (Die ersten beiden Methoden stören vorhandene optimierte Verbindungen.) Definieren Sie eine ACL mit den Kriterien "Ablehnen ALLE". Wählen Sie in der zentralen Verwaltungsschnittstelle ein ANC-Gerät aus, wählen Sie dann **Configure > Interception > Interception Access List aus**, und wählen Sie in der Dropdown-Liste AppNav Controller Interception Access List (Zugriffsliste für AppNav-Controller-Interception) die Option Deny ALL Access List (ALLE Zugriff verweigern) aus.

Um das Abfangen mit einer ACL über die CLI zu deaktivieren, verwenden Sie die folgenden Befehle:

```
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
```

Festlegen einer ANC im Pass-Through-Zustand:

- Deaktiviert WAAS-Interception, nicht die Schnittstellen.
- Deaktiviert die gesamte WAAS-Optimierung.
- Verhindert, dass der gesamte Datenverkehr unbeeinträchtigt verläuft.

Deaktivieren einer Off-Path-ANC

Um eine ANC zu deaktivieren, die im Off-Path-Modus ausgeführt wird, deaktivieren Sie das WCCP-Protokoll für die ANC. Sie können diese Aktion auf dem ANC oder auf dem Umleitungs-Router oder auf beiden durchführen. Auf der ANC können Sie die WCCP-Dienste deaktivieren oder löschen, oder Sie können die Abfangmethode entfernen oder von WCCP in eine andere Methode ändern.

Um die WCCP-Überwachung zu deaktivieren, wählen Sie im zentralen Manager ein ANC-Gerät aus, und wählen Sie dann **Configure > Interception > Interception Configuration**. Deaktivieren Sie das Kontrollkästchen WCCP-Dienst aktivieren, oder klicken Sie auf das Taskleistensymbol "Einstellungen entfernen", um die WCCP-Interception-Einstellungen vollständig zu entfernen (sie gehen verloren).

Verwenden Sie die folgenden Befehle, um die WCCP-Interception über die CLI zu deaktivieren:

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

In einigen Fällen können mehrere ANCs den umgeleiteten Datenverkehr vom gleichen Router empfangen. Aus Gründen der Einfachheit können Sie WCCP am Router deaktivieren, statt die ANCs zu verwenden. Der Vorteil besteht darin, dass Sie mehrere ANCs in einem einzigen Schritt aus einer WCCP-Farm entfernen können. Der Nachteil ist, dass Sie dies nicht über den WAAS Central Manager tun können.

Um WCCP am Router zu deaktivieren, verwenden Sie die folgende Syntax:

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

Um WCCP am Router erneut zu aktivieren, verwenden Sie die folgende Syntax:

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

Stellen Sie bei jedem WCCP-Router sicher, dass die ANCs, die Sie deaktiviert haben, nicht als WCCP-Clients angezeigt werden. Die folgende Ausgabe wird angezeigt, wenn die WCCP-Dienste auf dem Router gelöscht wurden.

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

AppNav-Cluster-Fehlerbehebung

Zur Fehlerbehebung in einem AppNav-Cluster können Sie die folgenden Tools verwenden:

- AppNav-Alarme
- Überwachung des zentralen Managers
- AppNav CLI-Befehle für die Überwachung von Cluster- und Gerätestatus
- AppNav CLI-Befehle für die Überwachung von Flow Distribution Statistics
- Verbindungsverfolgung
- AppNav-Debug-Protokollierung

AppNav-Alarme

Der Cluster Membership Manager (CMM) löst aufgrund von Fehlerzuständen folgende Alarme aus:

- Degraded Cluster (Critical) - Teilweise Transparenz zwischen ANCs. ANC durchläuft neue Verbindungen.
- Konvergenz fehlgeschlagen (entscheidend) - ANC konnte keine stabile Ansicht der ANCs und WNs herstellen. ANC durchläuft neue Verbindungen.
- ANC Join Failed (Critical) (ANC-Join fehlgeschlagen) (Kritisch)) - ANC konnte einem vorhandenen Cluster nicht beitreten, da der Cluster möglicherweise mit der ANC in diesem Cluster abgebaut wurde.
- ANC Mixed Farm (Nebenprodukte) - ANCs im Cluster führen verschiedene, aber kompatible Versionen des Clusterprotokolls aus.
- ANC Unreachable (Major) (AnC nicht erreichbar (Major) - Eine konfigurierte ANC ist nicht erreichbar.
- WN Unreachable (Major) (WN nicht erreichbar) - Ein konfiguriertes WN ist nicht erreichbar. Dieser WN wird nicht für die Umleitung von Datenverkehr verwendet.
- WN Excluded (Major) (WN ausgeschlossen (Major)) - Ein konfiguriertes WN ist erreichbar, aber ausgeschlossen, da ein oder mehrere andere ANCs ihn nicht sehen können. Dieser WN wird nicht für die Umleitung des Datenverkehrs (neue Verbindungen) verwendet.

Sie können Alarme im Fenster Central Manager Alarms (Alarme) oder mit dem Befehl **show alarm** EXEC auf einem Gerät sehen.

Hinweis: Der CMM ist eine interne AppNav-Komponente, die die Gruppierung von ANCs und WNs in einem AppNav-Cluster verwaltet, das mit einem Dienstkontext verknüpft ist.

Überwachung des zentralen Managers

Sie können AppNav-Cluster mit dem Central Manager überprüfen, überwachen und beheben. Der Central Manager bietet eine globale Übersicht über alle registrierten WAAS-Geräte in Ihrem Netzwerk und kann Ihnen bei der schnellen Identifizierung der meisten AppNav-Probleme helfen.

Wählen Sie im Menü Central Manager (Zentrale Verwaltungsschnittstelle) **AppNav Clusters >** *Clustername aus*. Im Hauptfenster des Clusters werden die Cluster-Topologie (einschließlich WCCP und Gateway-Router), der allgemeine Cluster-Status, der Gerätestatus, der Gerätegruppenstatus und der Verbindungsstatus angezeigt.

Überprüfen Sie zunächst, ob der Gesamtstatus des Clusters betriebsbereit ist.

Beachten Sie, dass die in diesem Diagramm gezeigten ANC- und WN-Symbole denselben Gerätenamen haben, da sie sich auf demselben Gerät befinden. Auf einem ANC, der auch den Datenverkehr als WN optimiert, werden diese beiden Funktionen im Topologiediagramm als separate Symbole angezeigt.

Auf jedem Gerät, für das der Central Manager möglicherweise nicht über aktuelle Informationen verfügt, wird eine orangefarbene Dreieckswarnung angezeigt, da das Gerät innerhalb der letzten 30 Sekunden nicht geantwortet hat (das Gerät ist möglicherweise offline oder nicht erreichbar).

Wenn Sie den Mauszeiger über das Symbol des Geräts bewegen, können Sie eine detaillierte Statusansicht für jedes ANC- oder WN-Gerät mit 360 Grad anzeigen. Auf der ersten Registerkarte werden Alarme auf dem Gerät angezeigt. Sie sollten alle Alarme beheben, die den ordnungsgemäßen Cluster-Betrieb behindern.

Klicken Sie auf die Registerkarte Interception (Interception), um die Methode zum Abfangen von Geräten für jede ANC zu überprüfen.

Wenn die Interception nicht verfügbar ist, wird der Status wie folgt angezeigt:

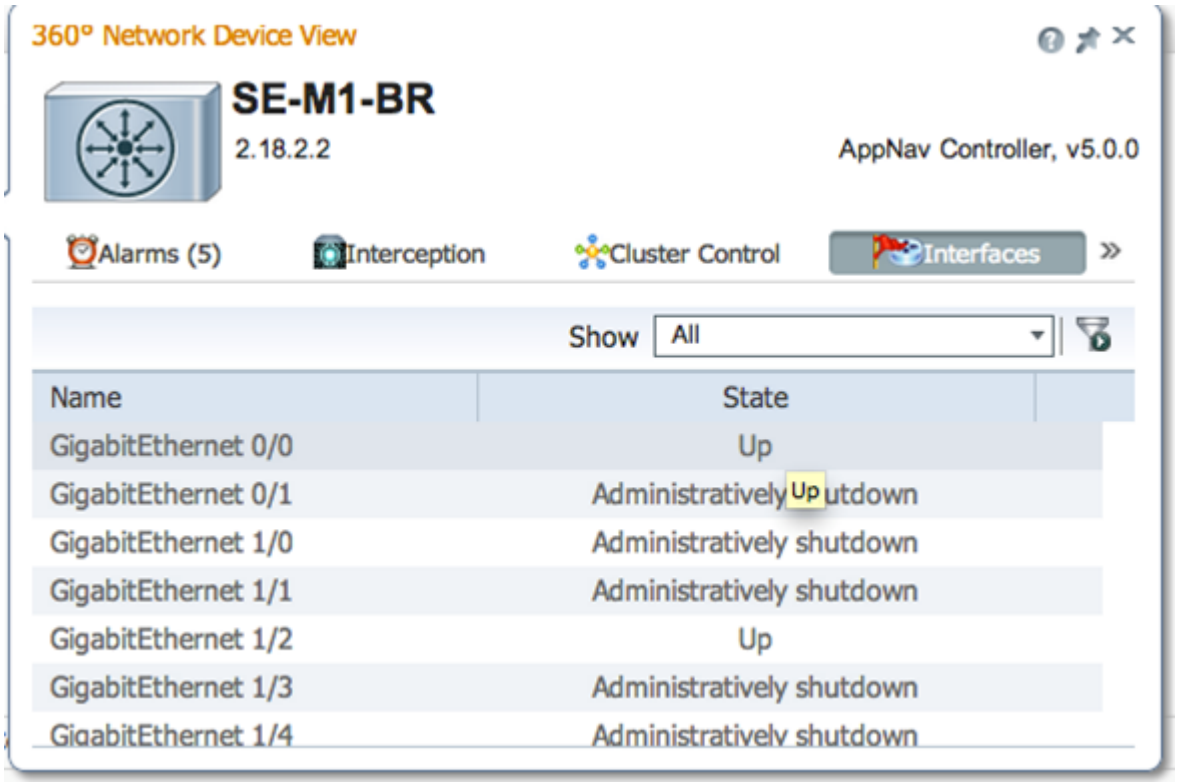
Klicken Sie auf die Registerkarte Cluster Control (Clustersteuerung), um die IP-Adresse und den Status der einzelnen Geräte im Cluster anzuzeigen, die diese ANC-Adresse anzeigen kann. Jede ANC im Cluster sollte über dieselbe Geräteliste verfügen. Ist dies nicht der Fall, weist dies auf ein Konfigurations- oder Netzwerkproblem hin.

Wenn sich nicht alle ANCs gegenseitig sehen können, ist der Cluster nicht betriebsbereit, und der gesamte Datenverkehr wird durchlaufen, da der Cluster nicht in der Lage ist, die Datenflüsse zu synchronisieren.

Wenn alle ANCs verbunden sind, aber unterschiedliche Ansichten zu den WNs haben, befindet sich der Cluster in einem verschlechterten Zustand. Der Datenverkehr wird weiterhin verteilt, jedoch nur an die WNs, die von allen ANCs angezeigt werden.

Alle WNs, die nicht von allen ANCs erkannt werden, sind ausgeschlossen.

Klicken Sie auf das Register Schnittstellen, um den Zustand der physischen und logischen Schnittstellen auf dem ANC zu überprüfen.



Überprüfen Sie in der 360-Grad-Ansicht jedes WN im Cluster den grünen Status aller Accelerators auf der Registerkarte Optimierung. Ein gelber Status für einen Accelerator bedeutet, dass der

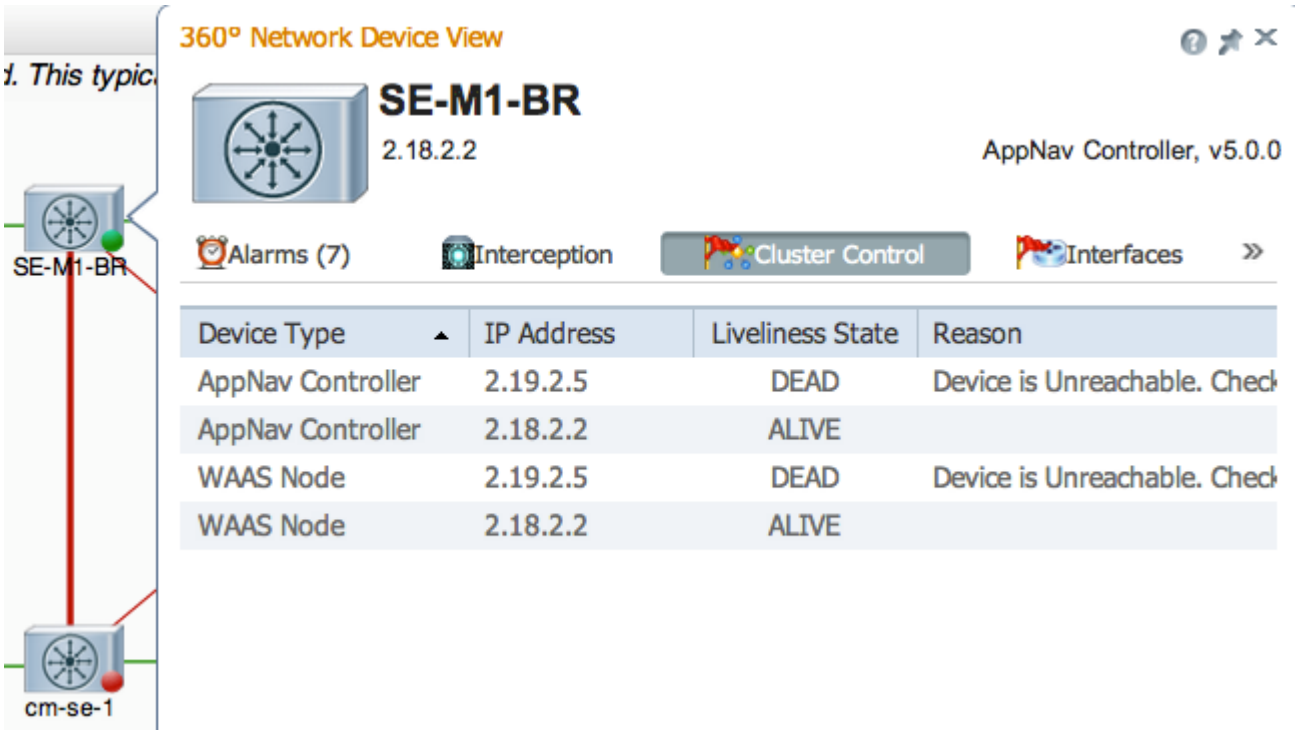
Accelerator ausgeführt wird, aber keine neuen Verbindungen bedienen kann, z. B. weil er überladen ist oder weil seine Lizenz entfernt wurde. Ein roter Status zeigt an, dass der Accelerator nicht ausgeführt wird. Wenn Accelerators gelb oder rot sind, müssen Sie diese Accelerators separat beheben. Wenn die Enterprise-Lizenz fehlt, lautet die Beschreibung Systemlizenz wurde widerrufen. Installieren Sie die Enterprise-Lizenz auf der Seite **Admin > History > License Management** Device (**Admin > Verlauf > Lizenzmanagement-**Gerät).

Ein geteilter Cluster resultiert aus Verbindungsproblemen zwischen ANCs im Cluster. Wenn der Central Manager mit allen ANCs kommunizieren kann, kann er ein geteiltes Cluster erkennen. Wenn er jedoch nicht mit einigen ANCs kommunizieren kann, kann er die Aufteilung nicht erkennen. Der Alarm "Management status is offline" (Verwaltungsstatus ist offline) wird ausgelöst, wenn der Central Manager die Verbindung mit einem beliebigen Gerät verliert und das Gerät im Central Manager als offline angezeigt wird.

Die Managementschnittstellen sollten von den Datenschnittstellen getrennt werden, um die Management-Konnektivität auch dann aufrechtzuerhalten, wenn eine Datenverbindung nicht verfügbar ist.

In einem geteilten Cluster verteilt jeder Untercluster von ANCs unabhängig die Flüsse an die WNGs, die er sehen kann. Da jedoch die Flüsse zwischen den Unterclustern nicht koordiniert werden, kann dies zu Reset-Verbindungen führen und die Gesamtleistung des Clusters verringert werden.

Überprüfen Sie auf der Registerkarte "Clusterkontrolle" jeder ANC, ob eine oder mehrere ANCs nicht erreichbar sind. Der Alarm "Service Controller is unreachable" (Service-Controller ist nicht erreichbar) wird ausgelöst, wenn zwei ANCs, die einmal miteinander kommunizieren konnten, die Verbindung untereinander verlieren. Dies ist jedoch nicht die einzige Ursache für einen Split-Cluster. Daher empfiehlt es sich, die Registerkarte "Cluster-Steuerung" jeder ANC zu überprüfen.



Wenn eine ANC eine graue Statusanzeige hat, kann sie deaktiviert werden. Überprüfen Sie, ob alle ANCs aktiviert sind, indem Sie unter dem Topologiediagramm auf die Registerkarte AppNav-Controller klicken. Wenn eine ANC nicht aktiviert ist, lautet ihr Aktivierungsstatus Nein. Sie können auf das Symbol **Enable** taskbar klicken, um eine ANC zu aktivieren.

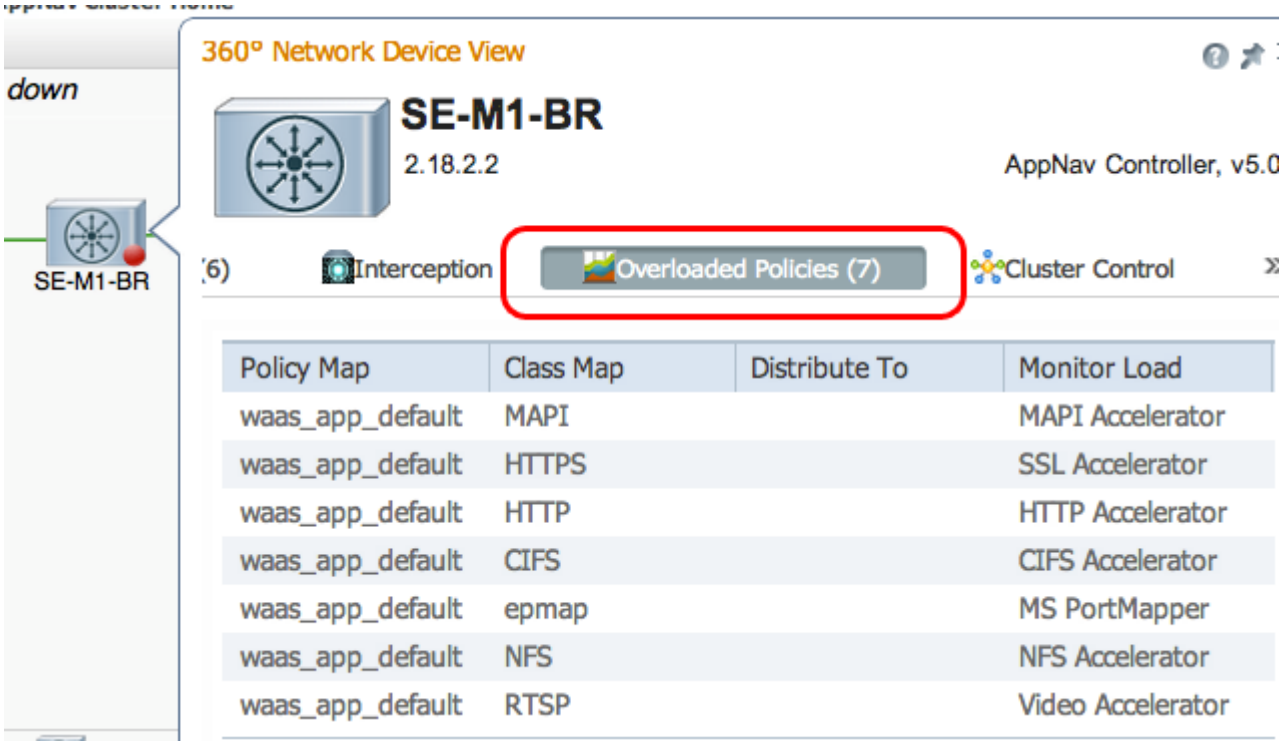
Überprüfen Sie die AppNav-Richtlinie für jede ANC, die über eine andere als eine grüne Statusanzeige verfügt. Wenn Sie den Mauszeiger über die Statusanzeige eines Geräts bewegen, werden Sie über einen QuickInfo über den Status oder das Problem informiert, wenn ein solches erkannt wird.

Um die definierten Richtlinien zu überprüfen, wählen Sie im Menü Central Manager **Configure > AppNav Policies (Konfigurieren > AppNav-Richtlinien)** und klicken Sie dann auf die **Schaltfläche Manage (Verwalten)**.

Im Allgemeinen sollte allen ANCs im Cluster eine einzige Richtlinie zugewiesen werden. Die Standardrichtlinie heißt "appnav_default". Wählen Sie das Optionsfeld neben einer Richtlinie aus, und klicken Sie auf das Symbol **Edit** taskbar. Im Bereich AppNav-Richtlinie werden die ANCs angezeigt, auf die die ausgewählte Richtlinie angewendet wird. Wenn nicht alle ANCs mit einem Häkchen angezeigt werden, klicken Sie auf das Kontrollkästchen neben jeder nicht markierten ANC, um die Richtlinie dieser zuzuweisen. Klicken Sie auf **OK**, um die Änderungen zu speichern.

Nachdem Sie die Richtlinienzuweisungen überprüft haben, können Sie die Richtlinienregeln auf der Seite AppNav-Richtlinien überprüfen, die weiterhin angezeigt wird. Wählen Sie eine Policy-Regel aus, und klicken Sie auf das Symbol **Edit** taskbar (Taskleiste bearbeiten)**,** um die Definition zu ändern.

Eine ANC kann eine gelbe oder rote Statusleuchte aufweisen, wenn eine oder mehrere Richtlinien überladen werden. Auf der Registerkarte Overloaded Policies (Überladene Richtlinien) der 360-Grad-Geräteansicht können Sie eine Liste der überladenen überwachten Richtlinien anzeigen.



Wenn eine ANC dem Cluster beitritt, wird sie mit einer gelben Statusleuchte und einem Beitrittsstatus angezeigt.

Die Registerkarte Interception der 360-Grad-Geräteansicht zeigt an, dass der Abhörpfad aufgrund des Zusammenschaltzustands heruntergefahren ist. Die Abhörfunktion wird so lange ausgesetzt, bis die ANC ihre Flow-Tabellen mit den anderen ANCs synchronisiert hat und Datenverkehr annehmen kann. Dieser Vorgang dauert in der Regel maximal zwei Minuten.

Wenn Sie eine ANC aus einem Cluster entfernen, wird sie im Topologiediagramm für einige Minuten und in der Registerkarte "Clustersteuerung" als aktiv angezeigt, bis sich alle ANCs auf die neue Cluster-Topologie einigen. In diesem Zustand werden keine neuen Ströme empfangen.

AppNav CLI-Befehle für die Überwachung von Cluster- und Gerätestatus

Mehrere CLI-Befehle sind für die Fehlerbehebung auf einem ANC nützlich:

- **Show Run Service Insertion**
- **Anzeigen des Service-Insertion-Service-Kontexts**
- **show service Insertion appnav-controller-group**
- **show service-Insertion service-node-group all**
- **Anzeige von Service Insertion Appnav-Controller** *IP-Adresse*
- **show service-Insertion service-node** [*ip-address*]
- **show service-Insertion service-node-group** *Gruppenname*

Verwenden Sie diese Befehle in einem WN:

- **Show Run Service Insertion**
- **Service-Insertion Service-Node anzeigen**

Sie können den Befehl **show service-Insertion service-context** auf einem ANC verwenden, um den Service-Kontext-Status und die stabile Ansicht der Geräte im Cluster anzuzeigen:

```
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
```

Wenn im Feld Device Interception State (oben) Shutdown (Herunterfahren des Geräts) angezeigt wird, bedeutet dies, dass der CMM die Abfangfunktion deaktiviert hat, da dieser ANC nicht bereit ist, Datenverkehrsflüsse zu empfangen. Beispielsweise befindet sich das ANC möglicherweise noch im Verbindungsprozess, und das Cluster hat noch keine synchronisierten Datenflüsse.

In den Feldern "Stabile Ansicht" (oben) werden die IP-Adressen der ANCs und WNs aufgeführt, die dieses ANC-Gerät in seiner letzten konvergenten Ansicht des Clusters gesehen hat. Diese Ansicht wird für Verteilungsvorgänge verwendet. Die Felder Aktuelle Ansicht enthalten die Geräte, die von diesem ANC in seinen Heartbeat-Nachrichten angekündigt werden.

Sie können den Befehl **show service-Insertion appnav-controller-group** auf einem ANC verwenden, um den Status jeder ANC in der ANC-Gruppe anzuzeigen:

```
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
```

Eine Liste möglicher ANC-Status und Join-Status finden Sie im Befehl **show service-Insertion** in der *Befehlsreferenz für Cisco Wide Area Application Services*.

Sie können den Befehl **show service-Insertion service-node** auf einem ANC verwenden, um den Status eines bestimmten WN im Cluster anzuzeigen:

```
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
```

Sie können den Befehl **show service-Insertion service-node-group** auf einem ANC verwenden, um den Status einer bestimmten WNG im Cluster anzuzeigen:

```
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
```

Das erste WN im obigen Beispiel hat den Status Excluded (Ausgeschlossen), d. h., das WN ist für

die ANC sichtbar, aber vom Cluster ausgeschlossen, da es von einem oder mehreren anderen ANCs nicht angezeigt wird.

Die SNG-Verfügbarkeitstabelle pro AO zeigt, ob jede AO neue Verbindungen bedienen kann. Ein AO ist verfügbar, wenn mindestens ein WN in der WNG einen GRÜNEN Status für das AO hat.

Sie können den Befehl **show service-Insertion service-node** auf einem WN verwenden, um den Status des WN anzuzeigen:

```
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
```

Der überwachte Zustand eines Beschleunigers ist der tatsächliche Zustand, der gemeldete Zustand kann jedoch abweichen, da er der niedrigere Status des Systems oder des Beschleunigers ist.

Weitere Informationen zur Fehlerbehebung in einem WN finden Sie in den Artikeln Fehlerbehebungsoptimierung und Problembehandlung bei Anwendungsbeschleunigung.

AppNav CLI-Befehle für die Überwachung von Flow Distribution Statistics

Mehrere CLI-Befehle sind nützlich für die Fehlerbehebung von Richtlinien und die Flussverteilung auf einem ANC:

- **show policy-map type appnav** *policymap name* - Zeigt die Richtlinienregeln und Trefferzähler für jede Klasse in der Richtlinienzuordnung an.
- **show class-map type appnav** *class-name* - Zeigt die Anpassungskriterien und Trefferzähler für jede Übereinstimmung-Bedingung in der Klassenzuordnung an.
- **show policy-sub-class type appnav** *level1-class-namelevel2-class-name* - Zeigt die Abgleichskriterien und Trefferzählungen für jede Übereinstimmung-Bedingung in einer Klassenzuordnung in einer geschachtelten AppNav-Richtlinienzuordnung.
- **show statistics class-map type appnav** *class-name* - Zeigt Datenverkehrsabfangen und Verteilungsstatistiken für eine Klassenzuordnung an.
- **show statistics policy-sub-class type appnav** *level1-class-namelevel2-class-name* - Zeigt Datenverkehrs-Interception- und Verteilungsstatistiken für eine Klassenzuordnung in einer geschachtelten AppNav-Richtlinienzuordnung.
- **show statistics pass-through type appnav** - Zeigt AppNav-Datenverkehrsstatistiken für jeden Pass-Through-Grund an.
- **show appnav-controller flow-distribution** - Zeigt, wie ein bestimmter hypothetischer Datenfluss von einem ANC klassifiziert und verteilt wird, basierend auf den definierten Richtlinien und dynamischen Lastbedingungen. Dieser Befehl kann hilfreich sein, um zu überprüfen, wie ein bestimmter Datenfluss auf einem ANC behandelt wird und zu welcher Klasse er gehört.

Verwenden Sie die folgenden Befehle in einem WN, um Fehler bei der Flussverteilung zu beheben:

- **show Statistics Service-Insertion Service-Node** *ip-address*: Zeigt Statistiken zu Accelerators und Datenverkehr an, der an das WN verteilt wird.
- **show statistics service-Insertion service-node-group name** *group-name* - Zeigt Statistiken für Accelerators und Datenverkehr, der an die WNG verteilt wird.

Sie können den Befehl **show statistics class-map type appnav** *class-name* auf einem ANC

verwenden, um die Datenflussverteilung zu beheben, um beispielsweise zu ermitteln, warum der Datenverkehr für eine bestimmte Klasse langsam sein kann. Dabei kann es sich um eine Anwendungsklassenzuordnung wie HTTP handeln. Wenn der gesamte Datenverkehr zu einer Zweigstelle langsam scheint, kann es sich um eine Klassenzuordnung für Zweigstellen handeln. Hier ein Beispiel für die HTTP-Klasse:

```
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
  ...
```

Die WN-Passthrough-Gründe im Abschnitt Indicated by SN (Nach SN angegeben) erhöhen sich nur, wenn die Pass-Through-Offload auf einem WN konfiguriert ist. Andernfalls weiß die ANC nicht, dass das WN eine Verbindung durchläuft, und zählt es nicht.

Wenn Verbindungen: Der ANC-Zähler fängt nicht an, es besteht ein Abhörproblem. Sie können das WAAS TcpTraceroute-Dienstprogramm verwenden, um die Platzierung des ANC im Netzwerk zu beheben, asymmetrische Pfade zu finden und die auf eine Verbindung angewendete Richtlinie

zu bestimmen. Weitere Informationen finden Sie im Abschnitt Verbindungsverfolgung.

AppNav CLI-Befehle zum Debuggen von Verbindungen

Um eine einzelne Verbindung oder einen Verbindungssatz auf einem ANC zu debuggen, können Sie den Befehl **show statistics appnav-controller connection** verwenden, um die Liste der aktiven Verbindungen anzuzeigen.

```
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
```

Sie können die Liste filtern, indem Sie die Client- oder Server-IP-Adresse und/oder die Port-Optionen angeben, und Sie können detaillierte Statistiken über Verbindungen anzeigen, indem Sie das **Detail-**Schlüsselwort angeben.

```
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
...
```

Sie können die Zusammenfassungsoption angeben, um die Anzahl der aktiven verteilten und

Pass-Through-Verbindungen anzuzeigen.

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

Verbindungsverfolgung

Um die Fehlerbehebung für AppNav-Flows zu unterstützen, können Sie das Connection Trace-Tool im Central Manager verwenden. Dieses Tool zeigt die folgenden Informationen für eine bestimmte Verbindung an:

- Wenn die Verbindung an eine WNG weitergeleitet oder an diese verteilt wurde
- ggf. Grund für die Durchreise
- WNG und WN, an die die Verbindung verteilt wurde
- Der Accelerator wird für die Verbindung überwacht.
- Klassenzuordnung angewendet

Um das Connection Trace-Tool zu verwenden, gehen Sie wie folgt vor:

1. Wählen Sie im Menü Central Manager (Zentrale Verwaltungsschnittstelle) **AppNav Clusters >** *Clustername aus*, und wählen Sie **Monitor > Tools > Connection Trace (Überwachung > Tools > Verbindungsverfolgung)**.

2. Wählen Sie die ANC und das Peer-WAAS-Gerät aus, und geben Sie die Kriterien für die Übereinstimmung der Verbindung an.

3. Klicken Sie auf **Trace**, um passende Verbindungen anzuzeigen.

WAAS TCP Traceroute ist ein weiteres Tool, das nicht spezifisch für AppNav ist und Ihnen bei der Behebung von Netzwerk- und Verbindungsproblemen, einschließlich asymmetrischer Pfade, helfen kann. Sie können damit eine Liste von WAAS-Knoten zwischen Client und Server sowie die konfigurierten und angewendeten Optimierungsrichtlinien für eine Verbindung finden. Über den Central Manager können Sie jedes Gerät im WAAS-Netzwerk auswählen, von dem aus die Traceroute ausgeführt werden soll. Um das TCP-Traceroute-Tool von WAAS Central Manager zu verwenden, gehen Sie wie folgt vor:

1. Wählen Sie im Menü WAAS Central Manager **Monitor > Troubleshoot > WAAS Tcptraceroute aus**. Alternativ können Sie zuerst ein Gerät auswählen und dann dieses Menüelement auswählen, um die Traceroute von diesem Gerät aus auszuführen.

2. Wählen Sie in der Dropdown-Liste WAAS Node (WAAS-Knoten) ein WAAS-Gerät aus, von dem die Traceroute ausgeführt werden soll. (Dieses Element wird nicht angezeigt, wenn Sie sich im Gerätekontext befinden.)

3. Geben Sie in den Feldern Ziel-IP und Ziel-Port die IP-Adresse und den Port des Ziels ein, an das Sie die Traceroute ausführen möchten.

4. Klicken Sie auf **TCPTraceroute ausführen**, um die Ergebnisse anzuzeigen.

WAAS-Knoten im Pfad mit Ablaufverfolgung werden in der Tabelle unter den Feldern angezeigt. Sie können dieses Dienstprogramm auch über die CLI mit dem Befehl **waas-tcptrace** ausführen.

AppNav-Debug-Protokollierung

Die folgende Protokolldatei ist verfügbar, um Probleme mit dem AppNav Cluster Manager zu beheben:

- Debugging-Protokolldateien: /local1/errorlog/cmm-errorlog.current (und cmm-errorlog.*)

Verwenden Sie die folgenden Befehle, um die Debug-Protokollierung des AppNav-Cluster-Managers einzurichten und zu aktivieren.

HINWEIS: Die Debug-Protokollierung ist CPU-intensiv und kann eine große Menge an Ausgabe generieren. Verwenden Sie sie sorgfältig und sparsam in einer Produktionsumgebung.

Sie können die detaillierte Protokollierung auf dem Datenträger aktivieren:

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

Die Optionen für das Debuggen von Cluster-Managern (ab Version 5.0.1) sind wie folgt:

```
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
```

Sie können die Debug-Protokollierung für den Cluster-Manager aktivieren und dann das Ende des Debug-Fehlerprotokolls wie folgt anzeigen:

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

Sie können die Debug-Protokollierung für den Flow Distribution Manager (FDM) oder den Flow Distribution Agent (FDA) mithilfe der folgenden Befehle aktivieren:

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

Der FDM bestimmt, wo die Datenflüsse basierend auf den Richtlinien und den dynamischen Lastbedingungen der WNs verteilt werden. Die FDA sammelt Informationen zum WN-Laden. Zur Fehlerbehebung bei FDM- und FDA-Problemen stehen die folgenden Protokolldateien zur Verfügung:

- Debugging-Protokolldateien: /local1/errorlog/fdm-errorlog.current (und fdm-errorlog.*)
- Debugging-Protokolldateien: /local1/errorlog/fda-errorlog.current (und fda-errorlog.*)

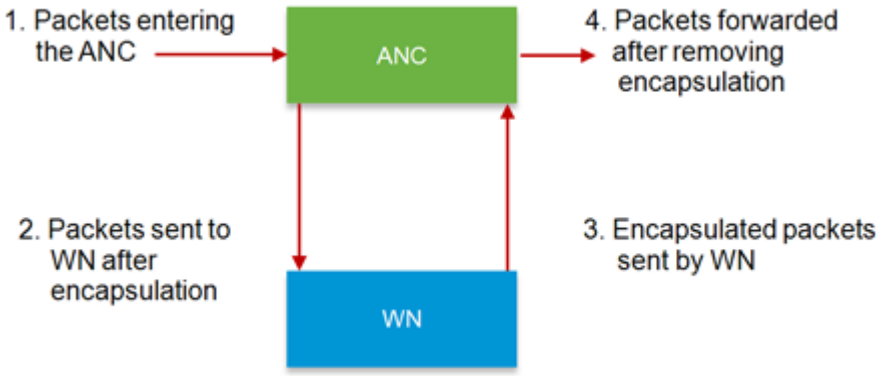
AppNav-Paketerfassung

Ein neuer Befehl zur **Paketerfassung** wird eingeführt, um die Erfassung von Datenpaketen an Schnittstellen auf dem Cisco AppNav-Controller-Schnittstellenmodul zu ermöglichen. Mit diesem Befehl können auch Pakete auf anderen Schnittstellen erfasst und Paketerfassungsdateien

decodiert werden. Der Befehl **zur Paketerfassung** wird gegenüber den veralteten Befehlen **tcpdump** und **tethereal** bevorzugt, die keine Pakete auf dem Cisco AppNav-Controller-Schnittstellenmodul erfassen können. Weitere Informationen zur Befehlssyntax finden Sie unter *Cisco Wide Area Application Services Command Reference*.

Hinweis: Die Paketerfassung oder die Debugging-Erfassung können aktiv sein, aber nicht beide gleichzeitig.

Datenpakete, die zwischen ANCs und WNs gesendet werden, werden gekapselt, wie im folgenden Diagramm gezeigt.



Wenn Sie Pakete an Punkt 1 oder 4 des Diagramms erfassen, werden sie nicht gekapselt. Wenn Sie Pakete an Punkt 2 oder 3 erfassen, werden sie gekapselt.

Im Folgenden finden Sie eine Beispielausgabe für eine gekapselte Paketerfassung:

```
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)
```

Im Folgenden finden Sie eine Beispielausgabe für eine nicht gekapselte Paketerfassung:

```
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 ...
...
```

Richtlinien zur Paketerfassung:

- Eine Paketerfassungs-ACL wird immer auf interne IP-Pakete für WCCP-GRE- und SIA-gekapselte Pakete angewendet.
- Die Paketerfassung wird auf allen ANC-Schnittstellen durchgeführt, wenn die ANC-

Schnittstelle für die Paketerfassung nicht bereitgestellt wird.

Die folgende Beispielausgabe für eine Paketerfassung an einer WN-Schnittstelle ist folgt:

```
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 ...
```

Hier ein Beispiel für die Decodierung einer Paketerfassungsdatei:

```
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
```

Sie können eine src-ip/dst-ip/src-port/dst-port zum Filtern der Pakete angeben:

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
```