

# WAAS - AppNav故障排除

## 章節：AppNav故障排除

本文描述如何對AppNav部署進行故障排除。

指南

[主頁](#)

[瞭解](#)

[WAAS](#)

[故障](#)

[應用](#)

[排除](#)

[排除](#)

[排除](#)

[排除](#)

[排除](#)

[影片](#)

[通用](#)

[過重](#)

[WCCP](#)

[App](#)

[磁碟](#)

[串列](#)

[vW](#)

[WAAS](#)

[排除](#)

## 目錄

- [1 AppNav故障排除](#)
  - [1.1 路徑內 \( 內嵌 \) 偵聽](#)
  - [1.2 Off-Path\(WCCP\)攔截](#)
    - [1.2.1 在路由器上配置和檢驗WCCP攔截](#)
    - [1.2.2 其他資訊](#)
  - [1.3 網路連線故障排除](#)
    - [1.3.1 通過特定流量](#)
    - [1.3.2 禁用內聯ANC](#)
    - [1.3.3 禁用非路徑ANC](#)
  - [1.4 AppNav群集故障排除](#)
    - [1.4.1 AppNav警報](#)
    - [1.4.2 Central Manager監控](#)
    - [1.4.3 用於監控集群和裝置狀態的AppNav CLI命令](#)
    - [1.4.4 用於監控流分佈統計資訊的AppNav CLI命令](#)
    - [1.4.5 用於調試連線的AppNav CLI命令](#)
    - [1.4.6 連線跟蹤](#)
    - [1.4.7 AppNav調試日誌記錄](#)

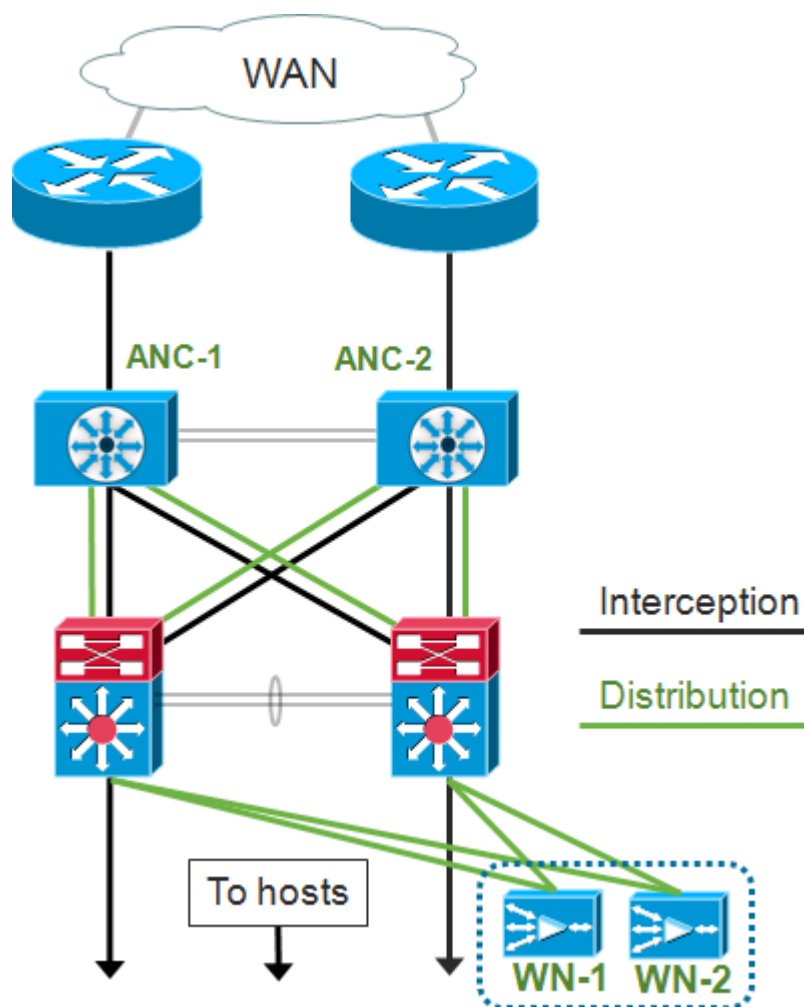
## AppNav故障排除

Cisco WAAS AppNav使用AppNav控制器(ANC)在WAAS節點(WN)之間分配流量，使用功能強大的類和策略機制進行最佳化，從而簡化了WAN最佳化的網路整合，並大大降低了對攔截交換機或路由器的依賴性。您可以使用WAAS節點(WN)根據站點和/或應用最佳化流量。本文描述如何對AppNav進行故障排除。

**附註：** AppNav功能是在WAAS 5.0.1版中引入的。本節不適用於較早的WAAS版本。

### 路徑內（內嵌）偵聽

在內聯模式下，ANC位於網路流量的路徑中，在此路徑中它們會攔截資料包並將它們分發到WN。



內聯部署的介面配置將偵聽和分發角色分配給Cisco AppNav控制器介面模組上的獨立介面。需要網橋組介面進行攔截，該介面由兩個或多個物理或埠通道介面或每個介面之一組成。網橋組介面沒有連線故障功能；也就是說，在裝置故障或斷電後，它不會開啟並機械橋接流量。如果AppNav控制器介面模組、連結路徑或與AppNav控制器介面模組的連線丟失或電源故障，AppNav使用群集功能來提供高可用性。

**附註：** 橋接器介面不會封鎖橋接通訊協定資料單元(BPDU)封包，而且在有產生回圈的備援介面的情況下，其中一個介面會遭到跨距樹狀目錄通訊協定的封鎖。

內嵌偵聽故障排除包括下列步驟：

- 通過檢查網路設計驗證ANC的正確內聯位置。如有必要，請使用ping和traceroute等基本工具或

第7層工具或應用來確認網路流量路徑是否與預期相符。檢查ANC的物理佈線。

- 驗證ANC已設定為內聯偵聽模式。
- 驗證是否已正確配置網橋組介面。

最後兩個步驟既可以在Central Manager中執行，也可以在命令列中執行，儘管Central Manager是首選方法，並且會首先進行說明。

在Central Manager中，選擇**Devices > AppNavController**，然後選擇**Configure > Interception > Interception Configuration**。驗證攔截方法是否設定為**Inline**。

在同一視窗中，檢驗是否已配置網橋介面。如果需要網橋介面，請按一下**Create Bridge**建立該介面。最多可以為網橋組分配兩個成員介面。您可以使用VLAN計算器根據包括或排除操作定義VLAN條目。請注意，沒有為網橋介面分配IP地址。

使用Alarm面板或**show alarm exec**命令檢查裝置上是否出現任何與網橋相關的警報。**bridge\_down**警報表示網橋中的一個或多個成員介面已關閉。

在CLI中，按照以下步驟配置內嵌操作：

1.將偵聽方法設定為內聯：

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

2.建立網橋組介面：

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

3. ( 可選 ) 根據需要指定要攔截的VLAN清單：

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

4.向網橋組介面新增兩個邏輯/物理介面：

```
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
```

您可以使用**show bridge exec**命令驗證網橋介面運行狀態並檢視網橋統計資訊。

```
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:

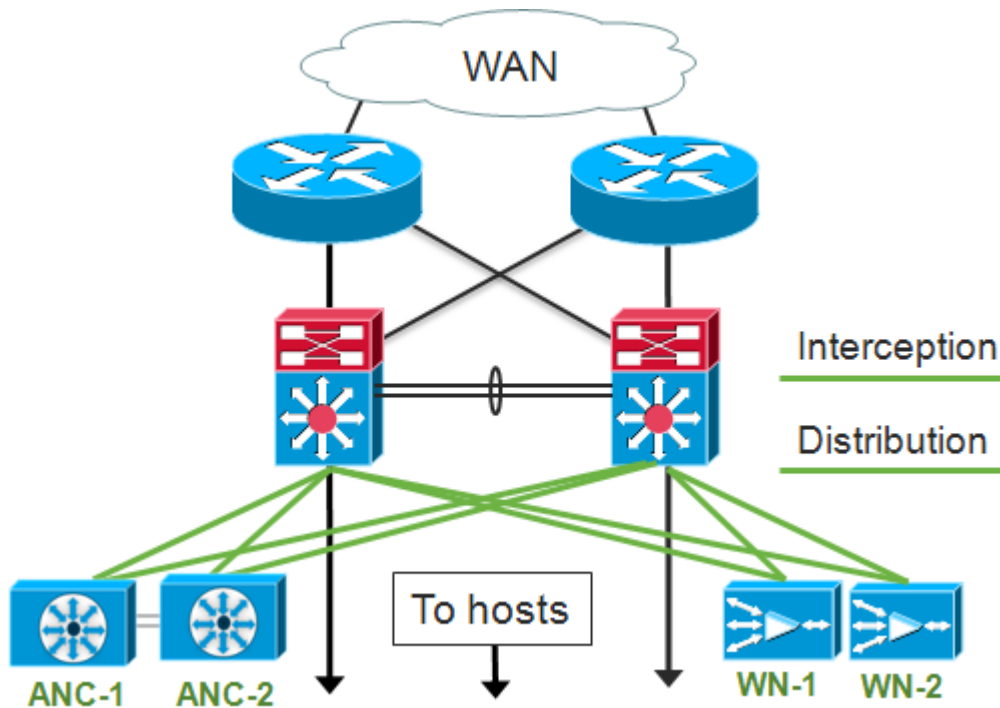
	GigabitEthernet 1/0	GigabitEthernet 1/1	
Operation State	: Down	Down(lsp)	<<< Down due to LSP
Input Packets Forwarded/Bridged	: 16188	7845	
Input Packets Redirected	: 5068	0	
Input Packets Punted	: 1208	605	
Input Packets Dropped	: 0	0	
Output Packets Forwarded/Bridged	: 7843	21256	
Output Packets Injected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

在上方範例中，Gig 1/0介面關閉，Gig 1/1介面也因為連結狀態傳播(LSP)而關閉。您可能還會看到Down (流同步)，這意味著ANC正在加入群集，並且正在將流資訊與群集中的其他ANC同步。它使偵聽路徑 (網橋介面) 保持關閉大約兩分鐘，直到所有ANC同步，以便可以正確分發現有流。

輸出的下方顯示了成員介面的流量統計資訊。

### Off-Path(WCCP)攔截

在WCCP模式中，WCCP路由器位於網路流量的路徑中，在網路流量中，WCCP路由器會攔截資料包，並將資料包重定向到位於路徑之外的ANC。由於AppNav處理偵聽處理、智慧流量分配以及WAAS加速器之間的負載考慮，因此路由器上的WCCP配置大大簡化。



在脫離路徑部署的介面配置中，偵聽和分發角色可以在Cisco AppNav控制器介面模組上共用相同的介面，但不需要這樣做。

排除路徑外攔截故障包括以下步驟：

- 檢驗WCCP路由器的正確位置，以確保它們處於進出最佳化主機的流量路徑中。您可以使用 **show run** 或 **show wccp** 命令驗證這些路由器是否與為WCCP配置的路由器相同。如有必要，使用ping和traceroute等基本工具，或第7層工具或應用來確認需要最佳化的所有流量都通過WCCP路由器。
- 使用中央管理器 (首選) 或CLI驗證WAAS ANC上的WCCP配置。
- 使用路由器CLI檢驗重定向路由器上的WCCP配置。

要驗證ANC上的WCCP配置，請在中央管理器中選擇**Devices > AppNavController**，然後選擇**Configure > Interception > Interception Configuration**。

- 驗證攔截方法是否設定為WCCP。
- 驗證是否已選中Enable WCCP Service覈取方塊。
- 確認已選中Use Default Gateway as WCCP Router覈取方塊或在WCCP Router欄位中列出WCCP路由器IP地址。
- 驗證其他設定（如負載平衡掩碼和重定向方法）是否針對您的部署進行了正確配置。

在路由器WCCP場中的ANC上檢查任何WCCP相關警報。在Central Manager上，按一下螢幕底部的Alarms面板，或在每台裝置上使用**show alarm**命令檢視警報。根據需要，通過更改ANC或路由器上的配置來更正任何警報條件。

在CLI中，按照以下步驟配置WCCP操作：

1.將攔截方法設定為wccp。

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

2.配置WCCP路由器清單，該清單包含參與WCCP場的路由器的IP地址。

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

3.配置WCCP服務ID。對於AppNav，單一服務ID是首選的，但支援兩個服務ID。

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

4.將配置的路由器清單與WCCP服務相關聯。

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

5.配置WCCP分配方法（ANC僅支援掩碼方法）。如果不指定dst-ip-mask或src-ip-mask選項，則預設源IP掩碼設定為f，目標IP掩碼設定為0。

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

6.配置WCCP重定向方法（出口和返回方法會自動設定為與重定向方法匹配，並且不能為ANC配置）。您可以選擇L2（預設）或GRE。L2要求ANC與路由器建立第2層連線，並且路由器也配置為進行第2層重定向。

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

7.啟用WCCP服務。

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

使用**show running-config**命令檢驗每個ANC上的WCCP攔截。以下兩個範例顯示L2 redirect和GRE

redirect的執行組態輸出。

Show running-config wccp ( 用於L2重定向 ) :

```
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
running config
exit
```

<<< L2 redirect is default so is not shown in

Show running-config wccp ( 用於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
  enable
exit
```

<<< GRE redirect method is configured

使用show wccp status命令檢驗每個ANC上的WCCP狀態。

```
wave# show wccp routers
WCCP Interception :
Configured State : Enabled
Operational State : Enabled
  Services Enabled on this WAE:
    TCP Promiscuous 61
configured
```

<<< Shows Disabled if WCCP is not configured  
<<< Shows Disabled if WCCP is not enabled  
<<< Shows NONE if no service groups are

使用show wccp routers命令檢驗WCCP場中響應了keep-alive消息的路由器。

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

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

<<< List of routers seen by this ANC  
<<< List of routers not seen by this ANC  
<<< List of routers notified of but not

使用show wccp clients命令檢驗每個ANC對WCCP群中其他ANC以及它們各自可訪問的路由器的檢視。

```
wave# show wccp clients
Wide Area Engine List for Service: 61
Number of WAE's in the Cache farm: 2
IP address = 10.10.10.31  Lead WAE = NO  Weight = 0
```

<<< Number of ANCs in the farm  
<<< 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

```

使用**show statistics wccp**命令檢驗每個ANC是否從場中的路由器接收資料包。圖中顯示了從每台路由器接收、通過和傳送到每台路由器的流量的統計資訊。伺服器場中所有路由器的累積統計資料顯示在底部。類似命令是**show wccp statistics**。請注意，「OE」是指這裡的ANC裝置。

```

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

```

## 在路由器上配置和檢驗WCCP攔截

要在WCCP場中的每個路由器上配置WCCP攔截，請執行以下步驟。

- 1.使用**ip wccp router**命令在路由器上配置WCCP服務。

```

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

```

- 2.在路由器LAN和WAN介面上配置WCCP攔截。如果您在ANC上使用單個服務ID，則可以在兩個介

面上配置相同的服務ID。

```
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. ( 可選 ) 如果使用通用GRE輸出，請配置隧道介面 ( 僅當您為ANC WCCP重定向方法選擇GRE時 )。

```
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
```

使用show wccp命令檢驗場中每台路由器上的WCCP配置。

```
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
```

## 其他資訊

有關其他資訊，請參閱以下檔案：

- [WCCP網路與Cisco Catalyst 6500的整合：成功部署的最佳實踐建議](#)
- [Cisco廣域應用程式服務Web快取通訊協定重新導向：思科路由器平台支援](#)
- [在路由器上配置高級WCCP功能，請參閱思科廣域應用服務配置指南](#)
- [在WAE上配置WCCP，請參閱思科廣域應用服務配置指南](#)

## 網路連線故障排除

在對WAAS進行故障排除時，在禁用WAAS的情況下確定網路的運行方式可能會有所幫助。當流量不僅無法最佳化，而且根本無法通過時，這很有幫助。在這些情況下，問題可能與WAAS無關。即使在流量通過的情況下，此技術也有助於確定需要故障排除的WAAS裝置。

測試第3層連線之前，請驗證AppNav控制器介面模組是否連線到正確的交換機埠。如果所連線的交換機支援並啟用了Cisco Discovery Protocol(CDP)，請運行`show cdp neighbors detail`命令以驗證與網路交換機的正确連線。

禁用WAAS可能不適用於所有情況。如果正在最佳化某些流量，而某些流量未最佳化，則禁用WAAS可能是無法接受的，從而中斷正在成功最佳化的流量。在這種情況下，偵聽ACL或AppNav策略可用於通過遇到問題的特定流量型別。有關詳細資訊，請參閱[通過特定流量](#)部分。

要禁用WAAS，對內聯模式執行的步驟與對離開路徑模式執行的步驟不同：

- 內嵌模式要求將攔截橋置於傳遞狀態。有關詳細資訊，請參閱[禁用內聯ANC](#)部分。
- 關閉路徑模式要求禁用WCCP協定。有關詳細資訊，請參閱[禁用路徑外ANC](#)部分。

在AppNav環境中，僅需要禁用ANC。WN不需要禁用，因為它們不參與攔截。

禁用WAAS後，使用標準方法檢查網路連線。

- 使用ping和traceroute等工具檢查第3層連線。
- 檢查應用行為以確定上層連線
- 如果網路遇到與啟用WAAS時相同的連線問題，則問題很可能與WAAS無關。
- 如果禁用WAAS後網路運行正常，但在啟用WAAS時出現連線問題，則可能有一個或多個WAAS裝置需要注意。下一步是將問題隔離到特定WAAS裝置。
- 如果網路具有啟用WAAS和未啟用WAAS的連線，但沒有最佳化，則可能有一個或多個WAAS裝置需要注意。下一步是將問題隔離到特定WAAS裝置。

要在啟用WAAS的情況下檢查網路行為，請執行以下步驟：

1.在WAAS ANC和WCCP路由器 ( 如果適用 ) 上重新啟用WAAS功能。

2.如果您已確定存在與WAAS相關的問題，請分別啟用每個AppNav群集和/或ANC，以將其隔離為已發現問題的潛在原因。

3.啟用每個ANC後，執行與前面步驟相同的基本網路連線測試，並注意此特定ANC是否正常運行。在這個階段，不要關心單個WN。此階段的目標是確定哪些群集和哪些特定ANC正在經歷期望或不期望的行為。

4.在啟用和測試每個ANC後，再次將其禁用，以便可以啟用下一個ANC。啟用和測試每個ANC可讓您確定哪些需要進一步的故障排除。

此故障排除技術最適用於WAAS配置似乎不僅未能最佳化，而且還導致正常網路連線問題的情況。

## 通過特定流量

您可以通過攔截ACL或配置AppNav策略來通過特定流量。

- 建立一個ACL，拒絕特定流量通過，但允許所有其他流量。在本例中，我們希望通過HTTP流量 ( 目標埠80 )。將ANC偵聽訪問清單設定為定義的ACL。目的地為連線埠80的連線會通過。您可以使用**show statistics pass-through type appnav**命令通過檢查PT Intercept ACL計數器是否遞增來驗證是否正在進行傳遞。

```
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
```

- 配置ANC策略以通過匹配特定類的流量。

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

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

## 禁用內聯ANC

通過將內聯ANC置於傳遞狀態來禁用內聯ANC的方法有多種：

- 將攔截網橋VLAN清單設定為無。在Central Manager中，選擇一個ANC裝置，然後選擇 **Configure > Interception > Interception Configuration**。選擇網橋介面並按一下Edit工作列圖示。將VLAN欄位設定為值「none」。
- 禁用包含ANC的服務上下文。在Central Manager中，選擇一個群集，然後按一下AppNav

Controllers頁籤，選擇一個ANC，然後按一下**Disable**工作列圖示。

- 套用具有「deny ALL」標準的攔截ACL。此方法為首選。（前兩種方法會中斷現有的最佳化連線。）使用deny ALL標準定義ACL。在Central Manager中，選擇一個ANC裝置，然後選擇**Configure > Interception > Interception Access List**，然後在AppNav Controller Interception Access List下拉選單中選擇deny ALL訪問清單。

要通過ACL從CLI禁用攔截，請使用以下命令：

```
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
```

將ANC置於傳遞狀態：

- 禁用WAAS攔截，而不是介面。
- 禁用所有WAAS最佳化。
- 使所有流量不受影響地通過。

## 禁用非路徑ANC

要禁用以脫離路徑模式運行的ANC，請為ANC禁用WCCP協定。您可以在ANC上執行此操作，也可以在重定向路由器上執行此操作，或者同時在ANC和/或ANC上執行此操作。在ANC上，您可以禁用或刪除WCCP服務，或者可以刪除偵聽方法或將其從WCCP更改為其他方法。

要禁用WCCP攔截，請在中央管理器中選擇一個ANC裝置，然後選擇**配置>攔截>攔截配置**。取消選中Enable WCCP Service覈取方塊或按一下Remove Settings工作列圖示完全刪除WCCP攔截設定（它們將丟失）。

要從CLI禁用WCCP攔截，請使用以下命令：

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

在某些情況下，可能有多個ANC接收來自同一路由器的重定向流量。為方便起見，您可以選擇在路由器而不是ANC上禁用WCCP。其優點是可以在單個步驟中從WCCP場中刪除多個ANC。缺點是無法從WAAS中央管理器執行此操作。

要在路由器上禁用WCCP，請使用以下語法：

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

要在路由器上重新啟用WCCP，請使用以下語法：

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

在每台WCCP路由器上，驗證您選擇禁用的ANC未顯示為WCCP客戶端。在路由器上刪除WCCP服務時，將顯示以下輸出。

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

## AppNav群集故障排除

要對AppNav群集進行故障排除，可以使用以下工具：

- [AppNav警報](#)
- [Central Manager監控](#)
- [用於監控集群和裝置狀態的AppNav CLI命令](#)
- [用於監控流分佈統計資訊的AppNav CLI命令](#)
- [連線跟蹤](#)
- [AppNav調試日誌記錄](#)

## AppNav警報

由於錯誤情況，群整合員管理器(CMM)引發以下警報：

- 降級群集 ( 嚴重 ) — ANC之間的部分可見性。ANC將通過新連線。
- 收斂失敗 ( 嚴重 ) — ANC未能收斂於ANC和WN的穩定檢視。ANC將通過新連線。
- ANC Join Failed(Critical)(ANC加入失敗 ( 嚴重 ) ) — 由於包含ANC的群集可能會降級，ANC無法加入現有群集。
- ANC Mixed Farm ( 次要 ) — 群集中的ANC正在運行不同但相容版本的群集協定。
- ANC無法連線 ( 主要 ) — 無法連線已設定的ANC。
- WN無法連線 ( 主要 ) — 無法連線已設定的WN。此WN不用於流量重定向。
- WN Excluded(Major) — 可訪問已配置的WN，但由於一個或多個其他ANC看不到它而將其排除。此WN不用於流量重定向 ( 新連線 )。

您可以在Central Manager的「警報」面板中或在裝置上使用**show alarms EXEC**命令來檢視警報。

**附註：** CMM是內部AppNav元件，用於管理ANC和WN到與服務上下文關聯的AppNav群集的分組。

## Central Manager監控

您可以使用中央管理器驗證、監控和排除AppNav群集故障。Central Manager擁有網路中所有已註冊WAAS裝置的全域性檢視，可以幫助您快速找到大多數AppNav問題。

從Central Manager選單中，選擇**AppNav Clusters > cluster-name**。集群主視窗顯示集群拓撲 ( 包括WCCP和網關路由器 )、總體集群狀態、裝置狀態、裝置組狀態和鏈路狀態。

首先，驗證整個群集狀態是否正常。

請注意，此圖中所示的ANC和WN圖示具有相同的裝置名稱，因為它們位於同一裝置上。在同樣將流量作為WN進行最佳化的ANC上，這兩個功能在拓撲圖中以單獨的圖示顯示。

橙色三角形警告指示符顯示在任何裝置上，由於裝置在過去30秒內未響應（裝置可能離線或無法訪問），Central Manager可能沒有當前資訊。

通過將游標懸停在裝置圖示上，可以獲得任何ANC或WN裝置的詳細360度狀態檢視。第一個頁籤顯示裝置上的警報。您應解決阻止正確群集操作的任何警報。

點選Interception頁籤以驗證每個ANC上的裝置偵聽方法。

如果攔截已關閉，則狀態顯示如下：

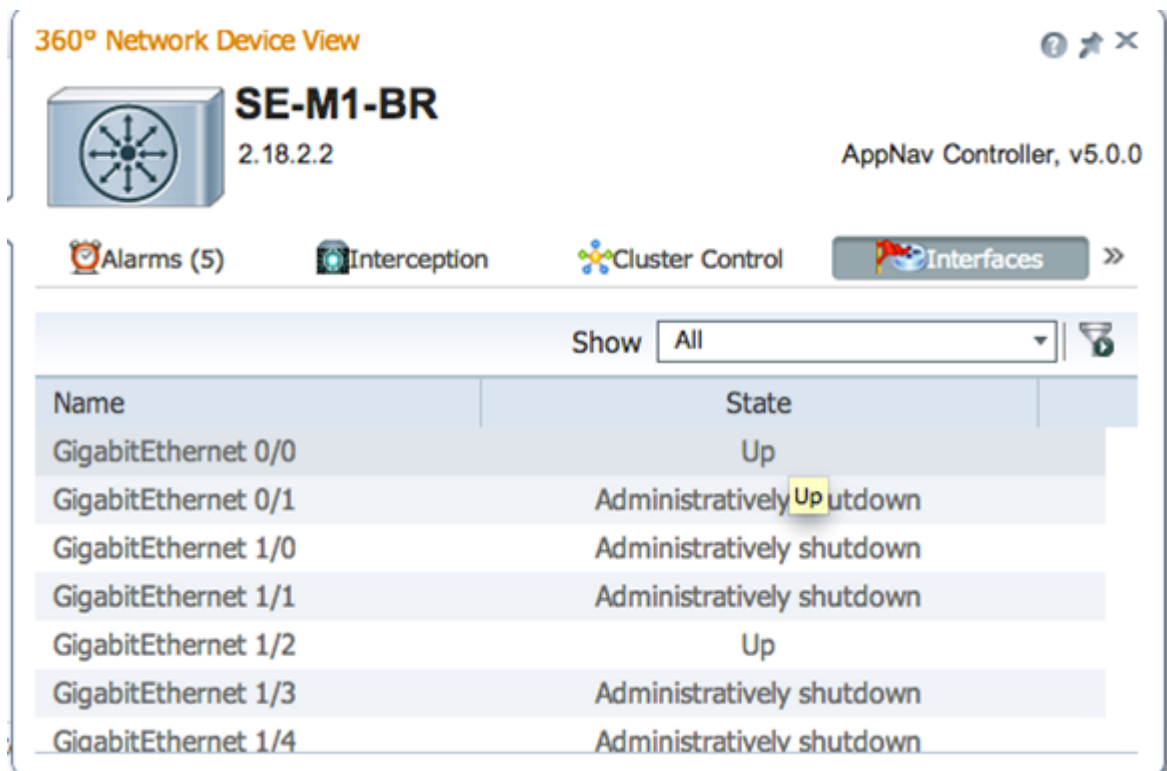
按一下Cluster Control頁籤，檢視此ANC可以看到的群集中每台裝置的IP地址和狀態。集群中的每個ANC應具有相同的裝置清單。如果不是，則表示配置或網路問題。

如果所有ANC無法看到彼此，則集群無法運行，並且由於集群無法同步流，所有流量都會通過。

如果所有ANC都連線但具有不同的WN檢視，則群集處於降級狀態。流量仍會分佈，但僅分佈到所有ANC看到的WN。

所有ANC都看不到任何WN。

點選Interfaces頁籤，檢驗ANC上物理和邏輯介面的狀態。



360° Network Device View

SE-M1-BR  
2.18.2.2  
AppNav Controller, v5.0.0

Alarms (5) Interception Cluster Control Interfaces >>

Show All

Name	State
GigabitEthernet 0/0	Up
GigabitEthernet 0/1	Administratively Up outdown
GigabitEthernet 1/0	Administratively shutdown
GigabitEthernet 1/1	Administratively shutdown
GigabitEthernet 1/2	Up
GigabitEthernet 1/3	Administratively shutdown
GigabitEthernet 1/4	Administratively shutdown

檢視集群中每個WN的360度檢視，並在「最佳化」頁籤中驗證所有加速器的綠色狀態。加速器的黃色狀態表示加速器正在運行但無法服務新連線，例如因為它已過載或它的許可證已移除。紅色狀態表示加速器未運行。如果任何加速器為黃色或紅色，您必須單獨對這些加速器進行故障排除。如果缺少Enterprise許可證，則說明為System license has been revoked。在Admin > History > License Management device頁面安裝企業許可證。

拆分群集是由群集中ANC之間的連線問題導致的。如果Central Manager可以與所有ANC通訊，它可以檢測到拆分群集；但是，如果它不能與某些ANC通訊，則無法檢測到拆分。如果Central Manager失去與任何裝置的連線，並且裝置在Central Manager中顯示為離線，則會觸發「管理狀態為離線」警報。

即使資料鏈路斷開，最好將管理介面與資料介面分離，以保持管理連線。

在拆分群集中，ANC的每個子群集將流獨立分配到它可以看到的WNG，但是由於子群集之間的流不協調，這會導致重置連線並且整個群集效能降低。

檢查每個ANC的Cluster Control頁籤以檢視是否可以訪問一個或多個ANC。如果兩個ANC之間曾經可以相互通訊，但失去彼此之間的連線，但這種情況並不是拆分群集的唯一原因，因此最好檢查每個ANC的Cluster Control頁籤，則會發出「服務控制器無法訪問」警報。

360° Network Device View

SE-M1-BR  
2.18.2.2

AppNav Controller, v5.0.0

Alarms (7) Interception Cluster Control Interfaces >>

Device Type	IP Address	Liveliness State	Reason
AppNav Controller	2.19.2.5	DEAD	Device is Unreachable. Check
AppNav Controller	2.18.2.2	ALIVE	
WAAS Node	2.19.2.5	DEAD	Device is Unreachable. Check
WAAS Node	2.18.2.2	ALIVE	

如果ANC的狀態為灰色，則它可能被禁用。按一下拓撲圖下方的AppNav Controllers頁籤，檢查是否啟用所有ANC。如果ANC未啟用，其「已啟用」狀態是「否」。您可以按一下**啟用**工作列圖示來啟用ANC。

檢查每個ANC上除綠色狀態指示燈以外的AppNav策略。如果將游標懸停在裝置上的狀態指示燈上，工具提示會告訴您狀態或問題（如果檢測到狀態）。

要檢查定義的策略，請從Central Manager選單中選擇**Configure > AppNav Policies**，然後按一下**Manage**按鈕。



通常，應該為群集中的所有ANC分配一個策略。預設策略名為appnav\_default。選擇策略旁的單選按鈕，然後按一下**Edit**工作列圖示。AppNav Policy窗格顯示所選策略應用到的ANC。如果所有ANC均未顯示為複選標籤，請按一下每個未選中ANC旁邊的覈取方塊以將策略分配給它。按一下「**OK**」以儲存變更內容。

驗證策略分配後，您可以在AppNav Policies頁面中驗證策略規則，該頁面將一直顯示。選擇任何策略規則，然後按一下**編輯**工作列圖示以更改其定義。

如果一個或多個策略過載，ANC的狀態燈可能為黃色或紅色。檢查360度裝置檢視的Overloaded Policies ( 過載策略 ) 頁籤，檢視過載的監控策略清單。

360° Network Device View

SE-M1-BR  
2.18.2.2  
AppNav Controller, v5.0

(6) Interception **Overloaded Policies (7)** Cluster Control

Policy Map	Class Map	Distribute To	Monitor Load
waas_app_default	MAPI		MAPI Accelerator
waas_app_default	HTTPS		SSL Accelerator
waas_app_default	HTTP		HTTP Accelerator
waas_app_default	CIFS		CIFS Accelerator
waas_app_default	epmap		MS PortMapper
waas_app_default	NFS		NFS Accelerator
waas_app_default	RTSP		Video Accelerator

如果ANC正在加入群集，則其顯示為黃色狀態燈和正在加入狀態。

360度裝置檢視的Interception頁籤顯示偵聽路徑因加入狀態而關閉。攔截被暫停，直到ANC已將其流表與其他ANC同步並準備好接受流量。此過程通常不超過兩分鐘。

如果從群集中刪除ANC，它仍會在拓撲圖中顯示幾分鐘，並在集群控制頁籤中顯示為活動狀態，直到所有ANC都同意新的集群拓撲。在此狀態下不會收到任何新流。

### 用於監控集群和裝置狀態的AppNav CLI命令

以下幾個CLI命令對ANC上的故障排除很有用：

- **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***

在WN上使用以下命令：

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

您可以在ANC上使用show service-insertion service-context命令檢視集群中裝置的服務情景狀態和穩定檢視：

```

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

```

如果Device Interception State ( 上面的 ) 欄位顯示Shutdown，則表示CMM已關閉攔截，因為此ANC未準備好接收流量。例如，ANC可能仍在連線過程中，並且群集尚未同步流。

「穩定檢視」欄位 ( 上面 ) 列出了此ANC裝置在集群的最後一個融合檢視中看到的ANC和WN的IP地址。這是用於分發操作的檢視。「當前檢視」欄位列出了此ANC在其心跳消息中通告的裝置。

您可以在ANC上使用show service-insertion appnav-controller-group命令檢視ANC組中每個ANC的狀態：

```

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

```

有關可能的ANC狀態和加入狀態的清單，請參閱思科廣域應用服務命令參考中的show service-insertion命令。

您可以在ANC上使用show service-insertion service-node命令檢視集群中特定WN的狀態：

```

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

您可以在ANC上使用**show service-insertion service-node-group**命令檢視集群中特定WNG的狀態：

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  
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

<<< WN status

A0 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  
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

<<< WN status

A0 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  
WNG

<<< AO status for entire

```
-----
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
```

上例中的第一個WN的狀態為「已排除」，這意味著ANC可以看到WN，但由於一個或多個其他ANC看不到該WN，因此它被排除在群集之外。

「每個AO的SNG可用性」表顯示每個AO是否能夠為新連線提供服務。如果WNG中至少有一個WN的AO狀態為綠色，則AO可用。

您可以在WN上使用**show service-insertion service-node**命令檢視WN的狀態：

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
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
```

<<< WN is responding to

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
```

```

-----
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

```

加速器的監視狀態是其實際狀態，但報告的狀態可能不同，因為它是系統狀態或加速器狀態的較低者。

有關在WN上進行最佳化故障排除的詳細資訊，請參閱[最佳化故障排除和應用加速故障排除](#)文章。

### 用於監控流分佈統計資訊的AppNav CLI命令

以下幾個CLI命令可用於對ANC上的策略和流量分佈進行故障排除：

- **show policy-map type appnav *polycymap-name*** — 顯示策略對映中每個類的策略規則和命中計數。
- **show class-map type appnav *class-name*** — 顯示類對映中每個匹配條件的匹配條件和命中計數。
- **show policy-sub-class type appnav *level1-class-name level2-class-name*** — 在巢狀AppNav策略對映的類對映中顯示每個匹配條件的匹配條件和命中計數。
- **show statistics class-map type appnav *class-name*** — 顯示類對映的流量攔截和分佈統計資訊。
- **show statistics policy-sub-class type appnav *level1-class-name level2-class-name*** — 顯示巢狀AppNav策略對映中類對映的流量攔截和分佈統計資訊。
- **show statistics pass-through type appnav** — 顯示每個直通原因的AppNav流量統計資訊。
- **show appnav-controller flow-distribution** — 顯示如何根據定義的策略和動態負載條件對ANC分類並分配特定假設流。此命令對於驗證如何在ANC上處理特定流及其屬於哪個類非常有用。

在WN上使用以下命令對流量分配進行故障排除：



- **show statistics service-insertion service-node *ip-address*** — 顯示分發到WN的加速器和流量的統計資訊。
- **show statistics service-insertion service-node-group name *group-name*** — 顯示分發到WNG的加速器和流量的統計資訊。

可以在ANC上使用**show statistics class-map type appnav *class-name***命令對流量分佈進行故障排除，例如確定特定類的流量可能緩慢的原因。這可能是應用程式類對映（如HTTP），或者，如果到分支的所有流量看起來都很慢，可能是分支關聯類對映。以下是HTTP類的示例：

```

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
  ...

```

僅當在WN上配置了傳遞解除安裝時，「由SN指示」部分中的WN傳遞原因才會增加。否則，ANC不知道WN正在通過某個連線，因此不會計算它。

如果連線：被ANC計數器攔截的次數沒有增加，存在攔截問題。您可以使用WAAS

TcpTraceroute實用程式來排查ANC在網路中的位置、查詢非對稱路徑並確定應用於連線的策略。有關詳細資訊，請參見[連線跟蹤](#)部分。

## 用於調試連線的AppNav CLI命令

要調試ANC上的單個連線或一組連線，可以使用**show statistics appnav-controller connection**命令顯示活動連線清單。

```
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
```

您可以通過指定客戶端或伺服器IP地址和/或埠選項來過濾清單，還可以通過指定**detail**關鍵字來顯示有關連線的詳細統計資訊。

```
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
...
```

您可以指定摘要選項以顯示活動的分散式和傳遞連線的數量。

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

## 連線跟蹤

為了幫助排除AppNav流故障，您可以使用中央管理器中的連線跟蹤工具。此工具顯示特定連線的以下資訊：

- 如果連線通過或分發到WNG
- 傳遞原因 ( 如果適用 )
- 將連線分發到的WNG和WN
- 針對連線監控加速器
- 類對映已應用

要使用連線跟蹤工具，請執行以下步驟：

- 1.從Central Manager選單中選擇**AppNav Clusters** > *cluster-name*，然後選擇**Monitor** > **Tools** > **Connection Trace**。
- 2.選擇ANC ( 對等WAAS裝置 )，並指定連線匹配條件。
- 3.按一下**跟蹤**以顯示匹配的連線。

WAAS TCP Traceroute是另一個並非專用於AppNav的工具，可幫助您解決網路和連線問題，包括非對稱路徑。您可以使用它來查詢客戶端和伺服器之間的WAAS節點清單，以及用於連線的已配置和應用的最佳化策略。在Central Manager中，您可以選擇運行traceroute的WAAS網路中的任何裝置。要使用WAAS Central Manager TCP Traceroute工具，請執行以下步驟：

- 1.從WAAS Central Manager選單中，選擇**Monitor** > **Troubleshoot** > **WAAS Tcptraceroute**。或者，您可以先選擇一個裝置，然後選擇此選單項以從該裝置運行traceroute。
- 2.從WAAS Node下拉選單中，選擇要從中運行traceroute的WAAS裝置。( 如果您在裝置上下文中，則不會顯示此專案。 )
- 3.在「目標IP」和「目標埠」欄位中，輸入要運行traceroute的目標的IP地址和埠
- 4.按一下**運行TCPTraceroute**以顯示結果。

跟蹤路徑中的WAAS節點顯示在欄位下面的表中。您也可以使用**waas-tcptrace**命令從CLI運行此實用程式。

## AppNav調試日誌記錄

以下日誌檔案可用於對AppNav群集管理器問題進行故障排除：

- 調試日誌檔案：/local1/errorlog/cmm-errorlog.current ( 和cmm-errorlog.\* )

要設定並啟用AppNav群集管理器的調試日誌記錄，請使用以下命令。

**附註：**調試日誌記錄是CPU密集型，可以生成大量輸出。在生產環境中慎重而謹慎地使用它。

您可以對磁碟啟用詳細日誌記錄：

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

集群管理器調試 ( 在5.0.1及更高版本上 ) 的選項如下 :

```
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
```

您可以為集群管理器啟用調試日誌記錄，然後按如下方式顯示調試錯誤日誌的結束：

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

還可以使用以下命令為流分配管理器(FDM)或流分配代理(FDA)啟用調試日誌記錄：

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

FDM根據WN的策略和動態負載條件確定分配流的位置。FDA收集WN負載資訊。以下日誌檔案可用於排除FDM和FDA問題：

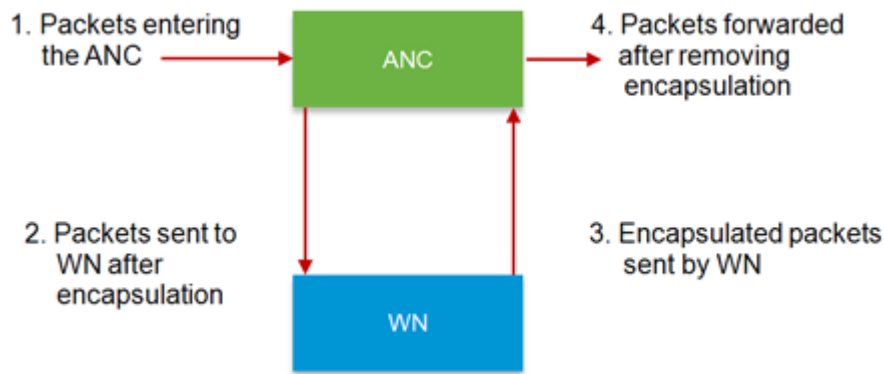
- 調試日誌檔案：/local1/errorlog/fdm-errorlog.current ( 和fdm-errorlog.\* )
- 調試日誌檔案：/local1/errorlog/fda-errorlog.current ( 和fda-errorlog.\* )

## AppNav封包擷取

引入了新的**packet-capture**命令，以允許在Cisco AppNav控制器介面模組的介面上捕獲資料包。此命令還可以捕獲其他介面上的資料包，還可以解碼資料包捕獲檔案。**packet-capture**命令優先於已棄用的**tcpdump**和**tethereal**命令，後者無法在Cisco AppNav控制器介面模組上捕獲資料包。有關命令語法的詳細資訊，請參閱**思科廣域應用服務命令參考**。

**附註：**資料包捕獲或調試捕獲都可以處於活動狀態，但不能同時處於活動狀態。

在ANC和WN之間傳送的資料包將被封裝，如下圖所示。



如果在圖中的點1或4捕獲資料包，則這些資料包將被解封。如果在點2或3捕獲資料包，則將其封裝。

以下是封裝封包擷取的輸出範例：

```
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)
```

以下是未封裝封包擷取的輸出範例：

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

資料包捕獲准則：

- 封包擷取ACL一律套用到WCCP-GRE和SIA封裝封包的內部IP封包。
- 如果沒有提供資料包捕獲的ANC介面，則所有ANC介面上都將完成資料包捕獲。

以下是WN介面上資料包捕獲的輸出示例：

```
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 ...
```

以下是解碼資料包捕獲檔案的示例：

```
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
```

您可以指定src-ip/dst-ip/src-port/dst-port以過濾資料包：

```
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
```