WAAS - AppNav 문제 해결

장:AppNav 문제 해결

이 문서에서는 AppNav 배포 문제를 해결하는 방법에 대해 설명합니다.

목차

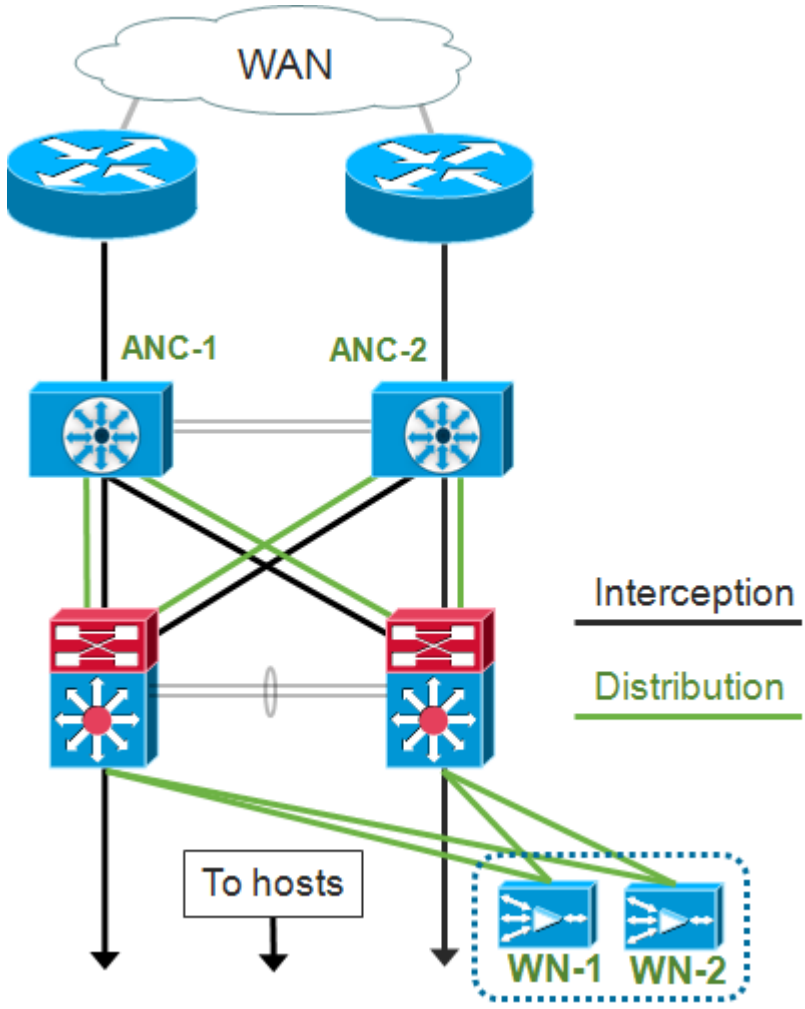
AppNav 문제 해결

Cisco WAAS AppNav는 강력한 클래스 및 정책 메커니즘을 사용하여 최적화를 위해 AppNav Controller(ANC)를 사용하여 WAAS Nodes(WN) 간에 트래픽을 분산함으로써 WAN 최적화의 네트워크 통합을 간소화하고 가로채기 스위치 또는 라우터에 대한 의존도를 크게 줄입니다.WAAS 노드(WN)를 사용하여 사이트 및/또는 애플리케이션을 기반으로 트래픽을 최적화할 수 있습니다.이 문서에서는 AppNav 문제 해결 방법에 대해 설명합니다.

참고: AppNav 기능은 WAAS 버전 5.0.1에 도입되었습니다. 이 섹션은 이전 WAAS 버전에는 적용되지 않습니다.

In-Path(인라인) 가로채기

인라인 모드에서는 ANC가 패킷을 가로채서 WN에 배포하는 네트워크 트래픽 경로에 배치됩니다.



인라인 구축의 인터페이스 컨피그레이션은 Cisco AppNav Controller Interface Module의 개별 인터페이스에 가로채기와 배포 역할을 할당합니다.인터셉션에 브리지 그룹 인터페이스가 필요하며 둘 이상의 물리적 또는 포트 채널 인터페이스 또는 각 인터페이스 중 하나로 구성됩니다.브리지 그룹 인터페이스는 유선 기능에 실패하지 않습니다.즉, 디바이스 장애 또는 전력 손실 후에도 트래픽이 기계적으로 브리지되지 않고 열린 상태로 작동하지 않습니다.AppNav는 클러스터링을 사용하여 AppNav Controller Interface Module, 링크 경로 또는 AppNav Controller Interface Module에 대한 연결이 끊어졌거나 전원 장애가 발생한 경우 고가용성을 제공합니다.

참고:브리지 인터페이스는 BPDU(Bridge Protocol Data Unit) 패킷을 차단하지 않으며, 루프를 생성

하는 이중 인터페이스의 경우 인터페이스 중 하나가 스패닝 트리 프로토콜에 의해 차단됩니다.

인라인 가로채기 문제 해결은 다음 단계로 구성됩니다.

- 네트워크 설계를 확인하여 ANC의 올바른 인라인 배치를 확인합니다.필요한 경우 ping, traceroute 또는 Layer 7 툴 또는 애플리케이션과 같은 기본 툴을 사용하여 네트워크 트래픽 경로가 예상대로 작동하는지 확인합니다.ANC의 물리적 케이블을 확인합니다.
- ANC가 인라인 차단 모드로 설정되어 있는지 확인합니다.
- bridge-group 인터페이스가 올바르게 구성되었는지 확인합니다.

Central Manager가 기본 설정이며 먼저 설명되는 경우에도 Central Manager나 명령행에서 마지막 두 단계를 수행할 수 있습니다.

Central Manager에서 **Devices >** AppNavController를 선택한 다음 **Configure > Interception > Interception Configuration을 선택합니다**.차단 방법이 인라인으로 설정되어 있는지 확인합니다.

동일한 창에서 브리지 인터페이스가 구성되었는지 확인합니다.브리지 인터페이스가 필요한 경우 Create **Bridge**를 클릭하여 생성합니다.브리지 그룹에 최대 2개의 멤버 인터페이스를 할당할 수 있습니다.VLAN 계산기를 사용하여 포함 또는 제외 작업을 기반으로 VLAN 항목을 정의할 수 있습니다.브리지 인터페이스에는 IP 주소가 할당되지 않습니다.

Alarm(알람) 패널 또는 **show alarm** exec 명령을 사용하여 디바이스에서 브리지 관련 경보가 발생하는지 확인합니다.bridge_down 경보는 브리지에 있는 하나 이상의 멤버 인터페이스가 다운되었음을 나타냅니다.

CLI에서 다음 단계를 수행하여 인라인 작업을 구성합니다.

1. 차단 방법을 인라인으로 설정합니다.

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

2. 브리지 그룹 인터페이스를 생성합니다.

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

3 .(선택 사항) 필요할 경우 차단할 VLAN 목록을 지정합니다.

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

4. 브리지 그룹 인터페이스에 두 개의 논리적/물리적 인터페이스를 추가합니다.

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

show bridge exec 명령을 사용하여 브리지 인터페이스 작동 상태를 확인하고 브리지에 대한 통계를 볼 수 있습니다.

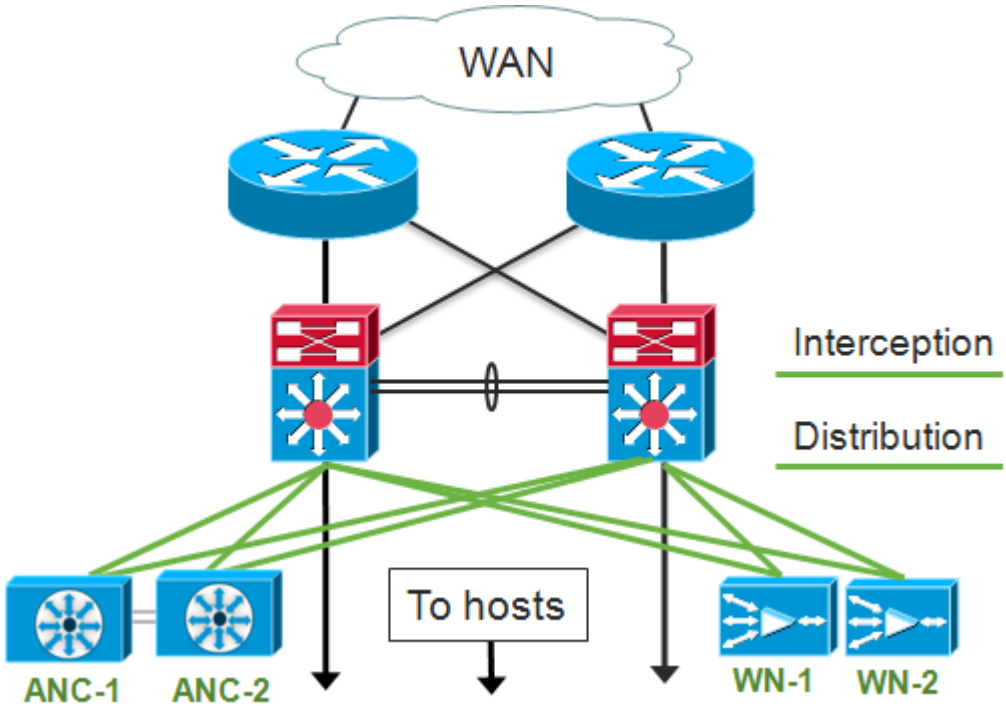
```
wave# show bridge 1
lsp: Link State Propagation
flow sync: AppNav Controller is in the process of flow sync
Member Interfaces:
 GigabitEthernet 1/0
 GigabitEthernet 1/1
Link state propagation: Enabled
VLAN interception:
 intercept vlan-id all                                                    <<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

위의 예에서 Gig 1/0 인터페이스는 다운되었으며 LSP(링크 상태 전파)로 인해 Gig 1/1 인터페이스도 다운되었습니다. 또한 Down(flow sync)이 표시될 수 있습니다. 즉, ANC가 클러스터에 가입하고 클러스터의 다른 ANC와 흐름 정보를 동기화하고 있습니다.또한 기존 플로우를 올바르게 배포할 수 있도록 모든 ANC가 동기화될 때까지 약 2분 동안 인터셉션 경로(브리지 인터페이스)를 종료합니다.

출력의 하단에는 멤버 인터페이스에 대한 트래픽 통계가 표시됩니다.

WCCP(Off-Path) 가로채기

WCCP 모드에서는 WCCP 라우터가 네트워크 트래픽 경로에 배치되며, 네트워크 트래픽은 패킷을 가로채서 경로 외부에 있는 ANC로 리디렉션됩니다.AppNav는 가로채기 처리, 지능형 흐름 분배, WAAS 가속기 간의 로드 고려 사항을 처리하므로 라우터의 WCCP 구성이 대폭 간소화됩니다.



오프 경로 구축을 위한 인터페이스 컨피그레이션에서는 인터셉션 및 디스트리뷰션 역할이 Cisco AppNav Controller Interface Module에서 동일한 인터페이스를 공유할 수 있지만 반드시 공유하지는 않습니다.

경로 외부 가로채기 문제 해결은 다음 단계로 구성됩니다.

- WCCP 라우터가 최적화된 호스트로 드나드는 트래픽 경로에 있는지 확인합니다.**show run** 또는 **show wccp** 명령을 사용하여 WCCP에 대해 구성된 동일한 라우터인지 확인할 수 있습니다.필요한 경우 ping, traceroute 또는 Layer 7 툴 또는 애플리케이션과 같은 기본 툴을 사용하여 최적화가 필요한 모든 트래픽이 WCCP 라우터를 통과하는지 확인합니다.
- 중앙 관리자(기본 설정) 또는 CLI를 사용하여 WAAS ANC에서 WCCP 컨피그레이션을 확인합니다.
- 라우터 CLI를 사용하여 리디렉션 라우터에서 WCCP 컨피그레이션을 확인합니다.

ANC에서 WCCP 컨피그레이션을 확인하려면 Central Manager에서 Devices **> AppNavController**를 선택한 다음 **Configure > Interception > Interception Configuration**을 선택합니다.

- 차단 방법이 WCCP로 설정되어 있는지 확인합니다.
- Enable WCCP Service(WCCP 서비스 활성화) 확인란이 선택되어 있는지 확인합니다.
- Use Default Gateway as WCCP Router(기본 게이트웨이를 WCCP 라우터로 사용) 확인란이 선택되었는지 또는 WCCP 라우터 IP 주소가 WCCP 라우터 필드에 나열되어 있는지 확인합니다.
- 부하 분산 마스크 및 리디렉션 방법과 같은 다른 설정이 배포에 맞게 구성되어 있는지 확인합니다.

라우터 WCCP 팜에 포함된 ANC에서 WCCP 관련 경보를 확인합니다.Central Manager에서 화면 하단의 Alarms(경보) 패널을 클릭하거나 각 디바이스에서 **show alarm** 명령을 사용하여 경보를 표시합니다.필요에 따라 ANC 또는 라우터의 컨피그레이션을 변경하여 경보 조건을 수정합니다.

CLI에서 다음 단계를 수행하여 WCCP 작업을 구성합니다.

1. 차단 방법을 wccp로 설정합니다.

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

2. WCCP 팜에 참여하는 라우터의 IP 주소를 포함하는 WCCP 라우터 목록을 구성합니다.

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

3. WCCP 서비스 ID를 구성합니다.AppNav에 단일 서비스 ID가 선호되지만 두 개의 서비스 ID가 지원됩니다.

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

4. 구성된 라우터 목록을 WCCP 서비스와 연결합니다.

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

5. WCCP 할당 방법을 구성합니다(ANC에서는 마스크 방법만 지원됨). dst-ip-mask 또는 src-ip-mask 옵션을 지정하지 않으면 기본 소스 IP 마스크가 f로 설정되고 대상 IP 마스크가 0으로 설정됩니다.

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

6. WCCP 리디렉션 방법을 구성합니다(이그레스 및 반환 방법이 리디렉션 방법과 일치하도록 자동으로 설정되며 ANC에 대해 구성할 수 없음). L2(기본값) 또는 GRE를 선택할 수 있습니다.L2를 사용하려면 ANC가 라우터와 레이어 2 연결을 가지며 라우터는 레이어 2 리디렉션을 위해 구성되어 있어야 합니다.

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

7. WCCP 서비스를 활성화합니다.

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

show running-config 명령을 사용하여 각 ANC에서 WCCP 가로채기를 확인합니다.아래의 두 예는 L2 리디렉션 및 GRE 리디렉션에 대한 실행 중인 컨피그레이션 출력을 보여줍니다.

running-config wccp 표시(L2 리디렉션의 경우):

```
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
```

running-config wccp 표시(GRE용):

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

show wccp status 명령을 사용하여 각 ANC에서 WCCP 상태를 확인합니다.

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

show wccp routers 명령을 사용하여 WCCP 팜에서 keep-alive 메시지에 응답한 라우터를 확인합니다.

```
wave# show wccp routers
```

```
Router Information for Service Id: 61

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

show wccp clients 명령을 사용하여 WCCP 팜의 다른 ANC에 대한 각 ANC의 보기 및 각 ANC가 연결할 수 있는 라우터를 **확인합니다**.

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

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

show statistics wccp 명령을 사용하여 팜의 라우터에서 각 ANC에서 패킷**을 수신하는지** 확인합니다.각 라우터에서 수신, 통과 및 각 라우터로 전송되는 트래픽에 대한 통계가 표시됩니다.팜의 모든 라우터에 대한 누적 통계는 아래쪽에 표시됩니다.유사한 명령은 show wccp **statistics입니다** ."OE"는 여기에서 ANC 디바이스를 나타냅니다.

```
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
```

라우터에서 WCCP 가로채기 구성 및 확인

WCCP 팜의 각 라우터에서 WCCP 가로채기를 구성하려면 다음 단계를 수행합니다.

1. ip wccp router 명령을 사용하여 라우터에서 WCCP 서비스를 구성합니다.

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

2. 라우터 LAN 및 WAN 인터페이스에서 WCCP 가로채기를 구성합니다.ANC에서 단일 서비스 ID를 사용하는 경우 두 인터페이스에서 동일한 서비스 ID를 구성할 수 있습니다.

```
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 .(선택 사항) 일반 GRE 이그레스(egress)를 사용하는 경우 터널 인터페이스를 구성합니다(ANC WCCP 리디렉션 방법으로 GRE를 선택한 경우에만).

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

show wccp 명령을 사용하여 팜의 각 라우터에서 WCCP 컨피그레이션을 확인합니다.

```
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
```

추가 정보

자세한 내용은 다음 문서를 참조하십시오.

- WCCP Network Integration with Cisco Catalyst 6500:성공적인 구축을 위한 모범 사례 권장 사항
- Cisco Wide Area Application Services Web Cache Communication Protocol 리디렉션:Cisco 라우터 플랫폼 지원
- *Cisco Wide Area Application Services 컨피그레이션 가이드*에서 라우터에서 고급 WCCP 기능 구성
- *Cisco Wide Area Application Services 컨피그레이션 가이드*에서 WAE에서 WCCP 구성

네트워크 연결 문제 해결

WAAS를 트러블슈팅할 때 네트워크가 WAAS를 비활성화하여 작동하는 방식을 확인하는 것이 도움이 될 수 있습니다.이는 트래픽이 최적화되지 않을 뿐만 아니라 전혀 통과되지 않을 때 유용합니다.이러한 경우, 문제가 WAAS와 관련이 없는 것으로 판명될 수 있습니다.트래픽이 통과되는 경우에도 이 기술을 통해 어떤 WAAS 장치에 문제 해결이 필요한지 확인할 수 있습니다.

레이어 3 연결을 테스트하기 전에 AppNav Controller Interface Module이 올바른 스위치 포트에 연결되어 있는지 확인하십시오.연결된 스위치가 CDP(Cisco Discovery Protocol)를 지원하고 활성화한 경우 **show cdp neighbors detail** 명령을 실행하여 네트워크 스위치에 대한 적절한 연결을 확인합니다.

WAAS를 비활성화하는 것은 모든 경우에 적용되지 않을 수 있습니다.일부 트래픽이 최적화되고 있고 일부는 최적화되지 않은 경우 WAAS를 비활성화하는 것은 허용되지 않을 수 있으므로 성공적으로 최적화되고 있는 트래픽을 중단시킬 수 있습니다.이러한 경우 차단 ACL 또는 AppNav 정책을 사용하여 문제가 발생하는 특정 유형의 트래픽을 전달할 수 있습니다.자세한 내용은 특정 트래픽 통과 섹션을 참조하십시오.

WAAS를 비활성화하려면 경로 외 모드가 아닌 인라인 모드에 대해 여러 단계가 수행됩니다.

- 인라인 모드에서는 인터셉션 브리지를 통과 상태로 설정해야 합니다.자세한 내용은 인라인 ANC 비활성화 섹션을 참조하십시오.
- 경로 외 모드에서는 WCCP 프로토콜을 비활성화해야 합니다.자세한 내용은 오프 경로 ANC 비활성화 섹션을 참조하십시오.

AppNav 환경에서는 ANC만 비활성화해야 합니다.WN은 가로채기에 참여하지 않으므로 비활성화할 필요가 없습니다.

WAAS가 비활성화되면 표준 방법을 사용하여 네트워크 연결을 확인합니다.

- ping 및 traceroute와 같은 툴을 사용하여 레이어 3 연결을 확인합니다.
- 애플리케이션 동작을 확인하여 상위 레이어 연결 확인
- 네트워크에서 WAAS가 활성화된 것과 동일한 연결 문제가 발생하는 경우, 이 문제는 WAAS와 관련이 없는 것일 가능성이 높습니다.
- 네트워크가 WAAS를 비활성화한 상태에서 정상적으로 작동하지만 WAAS를 활성화한 연결 문제가 있는 경우 주의가 필요한 하나 이상의 WAAS 장치가 있을 수 있습니다.다음 단계는 특정 WAAS 디바이스로 문제를 격리하는 것입니다.
- 네트워크에 WAAS를 활성화하거나 사용하지 않는 연결이 있지만 최적화가 없으면 주의가 필요한 하나 이상의 WAAS 장치가 있을 수 있습니다.다음 단계는 특정 WAAS 디바이스로 문제를 격리하는 것입니다.

WAAS가 활성화된 네트워크 동작을 확인하려면 다음 단계를 수행하십시오.

1. WAAS ANC에서 WAAS 기능을 다시 활성화하고, 해당되는 경우 WCCP 라우터를 다시 활성화합니다.

2. WAAS 관련 문제가 있다고 판단되면 각 AppNav 클러스터 및/또는 ANC를 개별적으로 활성화하여 관찰된 문제의 잠재적 원인으로 격리합니다.

3. 각 ANC가 활성화되면 이전 단계와 동일한 기본 네트워크 연결 테스트를 수행하고 이 특정 ANC가 올바르게 작동하는 것 같은지 확인합니다.이 단계에서는 개별 WN에 대해 걱정하지 마십시오.이 단계의 목표는 어떤 클러스터와 어떤 특정 ANC에서 원하는 행동 또는 원하지 않는 행동을 경험하는지 확인하는 것입니다.

4. 각 ANC가 사용 및 테스트될 때 다음 ANC를 사용할 수 있도록 다시 비활성화합니다.각 ANC를 차례로 활성화하고 테스트하면 추가 트러블슈팅이 필요한 ANC를 결정할 수 있습니다.

이 트러블슈팅 기술은 WAAS 컨피그레이션이 최적화에 실패했을 뿐만 아니라 정상적인 네트워크 연결에 문제가 발생하는 경우에 가장 적합합니다.

특정 트래픽 통과

차단 ACL을 사용하거나 통과를 위해 AppNav 정책을 구성하여 특정 트래픽을 전달할 수 있습니다.

- 통과될 특정 트래픽을 거부하고 다른 모든 것을 허용하는 ACL을 생성합니다.이 예에서는

HTTP 트래픽(대상 포트 80)을 통과하려고 합니다. ANC 차단 액세스 목록을 정의된 ACL로 설정합니다.포트 80으로 향하는 연결이 통과됩니다.**show statistics pass-through type appnav** 명령을 사용하여 PT 가로채기 ACL 카운터가 증가하는지 확인하여 패스스루가 발생하는지 확인할 수 있습니다.

```
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
```

- 특정 클래스와 일치하는 트래픽을 통과하도록 ANC 정책을 구성합니다.

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

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

인라인 ANC 비활성화

인라인 ANC를 통과 상태로 전환하여 비활성화하는 방법에는 여러 가지가 있습니다.

- 인터셉션 브리지 VLAN 목록을 none으로 설정합니다.Central Manager에서 ANC 디바이스를 선택한 다음 Configure(구성) **> Interception(차단) > Interception Configuration(차단 컨피그레이션)을** 선택합니다.브리지 인터페이스를 선택하고 **Edit** 작업 표시줄 아이콘을 클릭합니다 .VLANs 필드를 "none" 값으로 설정합니다.
- ANC가 포함된 서비스 컨텍스트를 비활성화합니다.중앙 관리자에서 클러스터를 선택한 다음 AppNav Controllers(AppNav 컨트롤러) 탭을 클릭하고 ANC를 선택한 다음 작업 표시줄 **비활성화** 아이콘을 클릭합니다.
- "deny ALL(모두 거부)" 기준을 사용하여 차단 ACL을 적용합니다.이 방법을 사용하는 것이 좋습니다.(처음 두 방법은 기존의 최적화된 연결을 중단시킵니다.) 모든 거부 기준을 사용하여 ACL을 정의합니다.Central Manager에서 ANC 디바이스를 선택한 다음 **Configure > Interception > Interception Access List를** 선택하고 AppNav Controller Interception Access List 드롭다운 목록에서 DENY ALL 액세스 목록을 선택합니다.

CLI에서 ACL로 가로채기를 비활성화하려면 다음 명령을 사용합니다.

```
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
```

ANC를 통과 상태로 전환:

- 인터페이스가 아닌 WAAS 가로채기를 비활성화합니다.
- 모든 WAAS 최적화를 비활성화합니다.
- 모든 트래픽이 영향을 받지 않고 통과하도록 합니다.

경로 외 ANC 비활성화

경로 외 모드에서 실행 중인 ANC를 비활성화하려면 ANC에 대해 WCCP 프로토콜을 비활성화합니다.ANC 또는 리디렉션 라우터 또는 둘 다에서 이 작업을 수행할 수 있습니다.ANC에서 WCCP 서비스를 비활성화 또는 삭제하거나 차단 방법을 제거하거나 WCCP에서 다른 방법으로 변경할 수 있습니다.

WCCP 가로채기를 비활성화하려면 중앙 관리자에서 ANC 디바이스를 선택한 다음 Configure(구성) > Interception(차단) **> Interception Configuration(가로채기 컨피그레이션)을** 선택합니다.WCCP 서비스 활성화 확인란의 선택을 취소하거나 설정 제거 작업 표시줄 아이콘을 클릭하여 WCCP 가로채기 설정을 완전히 제거합니다(WCCP 가로채기가 손실됩니다).

CLI에서 WCCP 가로채기를 비활성화하려면 다음 명령을 사용합니다.

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

경우에 따라 동일한 라우터에서 리디렉션된 트래픽을 수신하는 ANC가 여러 개 있을 수 있습니다.편의를 위해 ANC가 아닌 라우터에서 WCCP를 비활성화하도록 선택할 수 있습니다.한 번에 WCCP 팜에서 여러 ANC를 제거할 수 있다는 장점이 있습니다.단점은 WAAS Central Manager에서 이 작업을 수행할 수 없다는 것입니다.

라우터에서 WCCP를 비활성화하려면 다음 구문을 사용합니다.

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

라우터에서 WCCP를 다시 활성화하려면 다음 구문을 사용합니다.

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

각 WCCP 라우터에서 비활성화하도록 선택한 ANC가 WCCP 클라이언트로 표시되지 않는지 확인합니다.다음 출력은 라우터에서 WCCP 서비스를 삭제하면 표시됩니다.

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

AppNav 클러스터 문제 해결

AppNav 클러스터의 문제를 해결하려면 다음 도구를 사용할 수 있습니다.

- AppNav 경보
- Central Manager 모니터링

- 클러스터 및 디바이스 상태 모니터링을 위한 AppNav CLI 명령
- 플로우 배포 통계 모니터링을 위한 AppNav CLI 명령
- 연결 추적
- AppNav 디버그 로깅

AppNav 경보

CMM(Cluster Membership Manager)은 오류 조건으로 인해 다음 경보를 발생시킵니다.

- Degraded Cluster(Critical)(저하된 클러스터(Critical)) - ANC 간의 부분 가시성ANC는 새 연결을 통과합니다.
- Convergence Failed (Critical)(컨버전스 실패(위험)) - ANC가 ANC 및 WN의 안정적인 보기를 통합하지 못했습니다.ANC는 새 연결을 통과합니다.
- ANC Join Failed (Critical)(ANC 가입 실패(중요)) - ANC가 클러스터에 ANC가 있는 클러스터가 저하될 수 있으므로 기존 클러스터에 가입하지 못했습니다.
- ANC Mixed Farm(Minor)(ANC 혼합 팜(Minor)) - 클러스터의 ANC가 클러스터 프로토콜의 서로 다르지만 호환 가능한 버전을 실행하고 있습니다.
- ANC Unreachable (Major)(ANC Unreachable (Major)(ANC 연결 불가(주요)) - 구성된 ANC에 연결할 수 없습니다.
- WN Unreachable (Major)(WN 연결 불가(주요)) - 구성된 WN에 연결할 수 없습니다.이 WN은 트래픽 리디렉션에 사용되지 않습니다.
- WN Excluded (Major)(WN Excluded (Major)(WN 제외(주요)) - 구성된 WN에 연결할 수 있지만 하나 이상의 다른 ANC에서 해당 WN을 볼 수 없으므로 제외됩니다.이 WN은 트래픽 리디렉션(새 연결)에 사용되지 않습니다.

Central Manager Alarms(중앙 관리자 알람) 패널에서 또는 디바이스에서 **show alarms** EXEC 명령을 사용하여 경보를 볼 수 있습니다.

참고:CMM은 서비스 컨텍스트와 연결된 AppNav 클러스터로 ANC 및 WN의 그룹을 관리하는 내부 AppNav 구성 요소입니다.

Central Manager 모니터링

중앙 관리자를 사용하여 AppNav 클러스터를 확인, 모니터링 및 트러블슈팅할 수 있습니다.Central Manager는 네트워크에 등록된 모든 WAAS 장치를 전체적으로 볼 수 있으며 대부분의 AppNav 문제를 신속하게 찾을 수 있도록 지원합니다.

Central Manager 메뉴에서 AppNav **Clusters(AppNav 클러스터) >** cluster-*name*을 선택합니다.클러스터 홈 창에는 클러스터 토폴로지(WCCP 및 게이트웨이 라우터 포함), 전체 클러스터 상태, 디바이스 상태, 디바이스 그룹 상태 및 링크 상태가 표시됩니다.

먼저 전체 클러스터 상태가 작동 중인지 확인합니다.

이 다이어그램에 표시된 ANC 및 WN 아이콘은 동일한 디바이스에 상주하므로 동일한 디바이스 이름을 갖습니다.트래픽을 WN으로 최적화하는 ANC에서는 이러한 두 기능이 토폴로지 다이어그램에 별도의 아이콘으로 표시됩니다.

지난 30초 내에 디바이스가 응답하지 않아 Central Manager가 현재 정보를 갖지 못할 수 있는 디바이스에 주황색 삼각형 경고 표시기가 표시됩니다(디바이스가 오프라인 상태이거나 연결할 수 없는 상태일 수 있음).

디바이스 아이콘 위에 커서를 올려 놓으면 ANC 또는 WN 디바이스의 자세한 상태 보기를 확인할 수 있습니다.첫 번째 탭은 디바이스의 경보를 표시합니다.올바른 클러스터 작업을 방해하는 모든 경보를 해결해야 합니다.

Interception(차단) 탭을 클릭하여 각 ANC에서 디바이스 차단 방법을 확인합니다.

가로채기가 중지되면 상태는 다음과 같이 나타납니다.

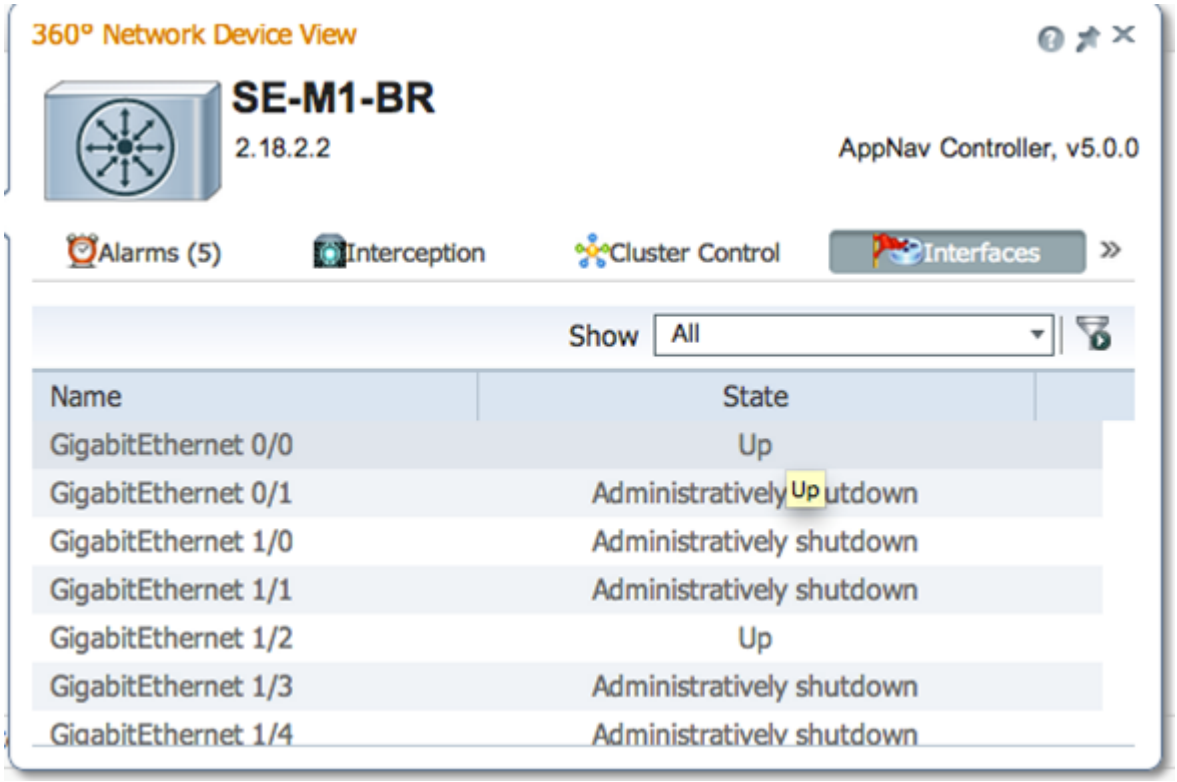
Cluster Control(클러스터 제어) 탭을 클릭하여 이 ANC가 볼 수 있는 클러스터의 각 디바이스의 IP 주소 및 상태를 확인합니다.클러스터의 각 ANC에는 동일한 디바이스 목록이 있어야 합니다.그렇지 않은 경우 컨피그레이션 또는 네트워크 문제를 나타냅니다.

모든 ANC가 서로를 볼 수 없는 경우 클러스터가 작동하지 않으며 클러스터의 플로우 동기화 불가 때문에 모든 트래픽이 통과됩니다.

모든 ANC가 연결되었지만 WN의 보기가 서로 다른 경우, 클러스터는 성능이 저하된 상태입니다.트래픽은 여전히 분산되지만 모든 ANC에서 보이는 WN에만 적용됩니다.

모든 ANC에서 볼 수 없는 WN은 제외됩니다.

Interfaces 탭을 클릭하여 ANC에서 물리적 및 논리적 인터페이스의 상태를 확인합니다.



클러스터의 각 WN에 대한 360도 보기를 살펴보고 Optimization(최적화) 탭에서 모든 가속기의 녹색 상태를 확인합니다.가속기의 노란색 상태는 가속기가 실행 중이지만 과부하되었거나 라이센스가 제거되었기 때문에 새 연결을 서비스할 수 없음을 의미합니다.빨간색 상태는 가속기가 실행되고 있지 않음을 나타냅니다.가속기가 노란색이나 빨간색인 경우 해당 가속기를 별도로 해결해야 합니다.엔터프라이즈 라이센스가 없으면 설명은 System license has been revoked라고 표시됩니다.Admin(관리) > History(기록) **> License Management Device(라이센스 관리** 디바이스) 페이지**에**

Enterprise 라이센스를 설치합니다.

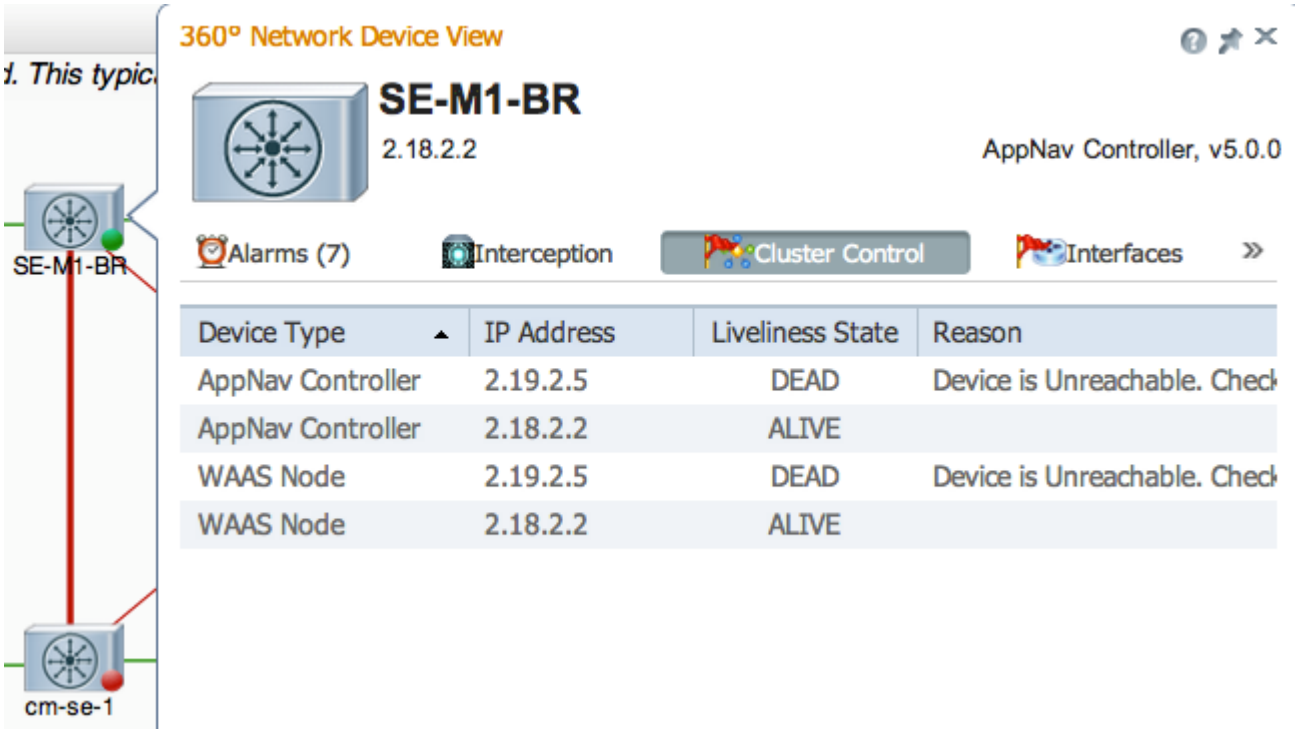
클러스터의 ANC 간 연결 문제로 인해 클러스터 분리가 발생합니다.Central Manager는 모든 ANC와 통신할 수 있는 경우 분할 클러스터를 탐지할 수 있지만 일부 ANC와 통신할 수 없는 경우 분할을 탐지할 수 없습니다.Central Manager가 어떤 디바이스와의 연결이 끊기고 해당 디바이스가 Central Manager에 오프라인으로 표시되는 경우 "Management status is offline(관리 상태가 오프라인)" 경보가 발생합니다.

데이터 링크가 다운된 경우에도 관리 연결을 유지하려면 관리 인터페이스를 데이터 인터페이스와 분리하는 것이 가장 좋습니다.

분할 클러스터에서 ANC의 각 하위 클러스터는 볼 수 있는 플로우를 WNG에 독립적으로 분배하지만, 하위 클러스터 간의 플로우가 조정되지 않으므로 재설정 연결을 생성할 수 있으며 전체 클러스

터 성능이 저하될 수 있습니다.

각 ANC의 Cluster Control(클러스터 제어) 탭에서 하나 이상의 ANC에 연결할 수 없는지 확인합니다.한 번 서로 통신할 수 있는 두 ANC가 두 ANC의 연결이 끊길 경우 "서비스 컨트롤러에 연결할 수 없음" 경보가 발생합니다. 그러나 이 상황은 스플릿 클러스터의 유일한 원인은 아니므로 각 ANC의 클러스터 제어 탭을 확인하는 것이 가장 좋습니다.



ANC에 회색 상태 표시등이 있는 경우 비활성화될 수 있습니다.토폴로지 다이어그램 아래의 AppNav Controller(AppNav 컨트롤러) 탭을 클릭하여 모든 ANC가 활성화되었는지 확인합니다.ANC가 활성화되지 않은 경우 해당 활성화 상태는 아니요로 표시됩니다. 작업 표시줄 사용 아이콘을 클릭하여 ANC를 활성화할 수 있습니다.

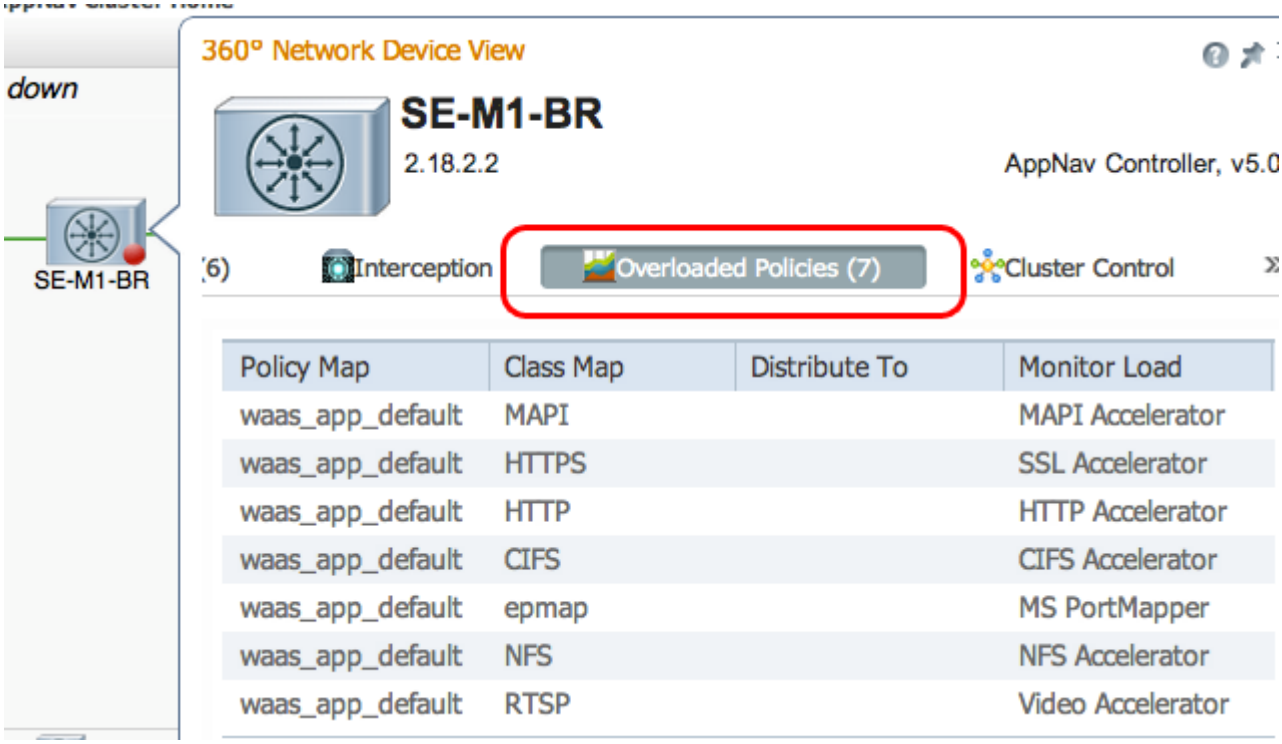
녹색 상태 표시등 이외의 다른 항목이 있는 각 ANC에서 AppNav 정책을 확인합니다.디바이스의 상태 표시등에 커서를 올려 놓으면 툴 팁이 상태 또는 문제가 발견되면 알려줍니다.

정의된 정책을 확인하려면 Central Manager 메뉴에서 Configure(구성) **> AppNav Policies(AppNav 정책)를** 선택한 다음 Manage(**관리**) 버튼을 클릭합니다.

일반적으로 클러스터의 모든 ANC에 단일 정책이 할당되어야 합니다.기본 정책의 이름은 appnav_default입니다.정책 옆의 라디오 버튼을 선택하고 **Edit** 작업 표시줄 아이콘을 클릭합니다 .AppNav Policy(AppNav 정책) 창에는 선택한 정책이 적용되는 ANC가 표시됩니다.모든 ANC에 확인 표시가 표시되지 않으면 각 선택 취소된 ANC 옆의 확인란을 클릭하여 정책을 할당합니다.확인**을** 클릭하여 변경 사항을 저장합니다.

정책 할당을 확인한 후 표시되는 AppNav Policies(AppNav 정책) 페이지에서 정책 규칙을 확인할 수 있습니다.정책 규칙을 선택하고 **Edit** 작업 표시줄 아이콘을 클릭하여 정의를 변경합니다.

하나 이상의 정책이 오버로드되면 ANC에 노란색 또는 빨간색 상태 표시등이 표시될 수 있습니다 .360도 디바이스 보기의 Overloaded Policies(오버로드된 정책) 탭을 확인하여 오버로드된 모니터링된 정책 목록을 확인합니다.



ANC가 클러스터에 참여하는 경우 노란색 상태 표시등과 조인 상태가 표시됩니다.

360도 디바이스 뷰의 Interception(가로채기) 탭은 인터셉션 경로가 조인 상태로 인해 다운되었음을 보여줍니다.ANC가 흐름 테이블을 다른 ANC와 동기화하여 트래픽을 받아들일 준비가 될 때까지 가로채기가 중단됩니다.이 프로세스는 일반적으로 2분을 넘지 않습니다.

클러스터에서 ANC를 제거하면 모든 ANC가 새 클러스터 토폴로지에 동의할 때까지 토폴로지 다이어그램에서 몇 분 동안 그리고 Cluster Control(클러스터 제어) 탭에 활성 상태로 표시됩니다.이 상태에서는 새 플로우가 수신되지 않습니다.

클러스터 및 디바이스 상태 모니터링을 위한 AppNav CLI 명령

여러 CLI 명령은 ANC에서 문제를 해결하는 데 유용합니다.

- **show run service-insertion**
- **서비스 삽입 서비스 컨텍스트 표시**
- **show service-insertion appnav-controller-group**
- **show service-insertion service-node-group all**
- **show service-inserappnav-controller** *ip 주소*
- **show service-insertion service-node** [*ip-address*]
- **show service-insertion service-node-group** *그룹 이름*

WN에서 다음 명령을 사용합니다.

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

ANC에서 **show service-insertion service-context** 명령을 사용하여 클러스터에 있는 디바이스의 서비스 컨텍스트 상태 및 안정적인 보기를 확인할 수 있습니다.

```
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
```

위의 Device Interception State(디바이스 차단 상태) 필드에 Shutdown(종료)이 표시되면 이 ANC가 트래픽 흐름을 수신할 준비가 되지 않아 CMM이 가로채기를 종료했음을 의미합니다.예를 들어, ANC는 여전히 가입 프로세스에 있을 수 있으며 클러스터는 아직 플로우를 동기화하지 않았습니다.

위의 Stable View(안정적 보기) 필드에는 클러스터의 마지막 통합 보기에서 이 ANC 디바이스에서 보이는 ANC 및 WN의 IP 주소가 나열됩니다.배포 작업에 사용되는 보기입니다.Current View(현재 보기) 필드에는 하트비트 메시지에서 이 ANC가 광고한 디바이스가 나열됩니다.

ANC에서 **show service-insertion appnav-controller-group** 명령을 사용하여 ANC 그룹의 각 ANC의 상태를 볼 수 있습니다.

```
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
```

가능한 ANC 상태 및 조인 상태의 목록은 *Cisco Wide Area Application Services 명령 참조*에서 **show service-insertion** 명령을 참조하십시오.

ANC에서 **show service-insertion service-node** 명령을 사용하여 클러스터에 있는 특정 WN의 상태를 확인할 수 있습니다.

```
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
```

ANC에서 **show service-insertion service-node-group** 명령을 사용하여 클러스터의 특정 WNG의 상태를 확인할 수 있습니다.

```
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
```

위의 예에서 첫 번째 WN의 상태는 Excluded(제외됨)입니다. 즉, WN은 ANC에 표시되지만 하나 이상의 다른 ANC가 볼 수 없으므로 클러스터에서 제외됩니다.

AO별 SNG 가용성 테이블에는 각 AO가 새 연결을 서비스할 수 있는지 여부가 표시됩니다.WNG에서 하나 이상의 WN이 AO에 대해 녹색 상태인 경우 AO를 사용할 수 있습니다.

WN에서 **show service-insertion service-node** 명령을 사용하여 WN의 상태를 확인할 수 있습니다.

```
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
```

가속기의 모니터링된 상태는 실제 상태이지만 보고된 상태는 시스템 상태 또는 가속기 상태의 하단이므로 다를 수 있습니다.

WN의 최적화 문제 해결에 대한 자세한 내용은 최적화 문제 해결 및 애플리케이션 가속화 문제 해결 문서를 참조하십시오.

플로우 배포 통계 모니터링을 위한 AppNav CLI 명령

여러 CLI 명령은 ANC에서 정책 및 흐름 분포를 트러블슈팅하는 데 유용합니다.

- **show policy-map type appnav policymap***-name* — 정책 맵의 각 클래스에 대한 정책 규칙 및 히트 수를 표시합니다.
- **show class-map type appnav** *class-name* — 클래스 맵의 각 일치 조건에 대한 일치 기준 및 히트 수를 표시합니다.
- **show policy-sub-class type appnav** *level1-class-name level2-class-name* — 중첩된 AppNav 정책 맵의 클래스 맵에서 각 일치 조건의 일치 기준 및 히트 수를 표시합니다.
- **show statistics class-map type appnav** *class-name* — 클래스 맵에 대한 트래픽 가로채기와 배포 통계를 표시합니다.
- **show statistics policy-sub-class type appnav level***1-class-name* level*2-class-name* — 중첩된 AppNav 정책 맵에서 클래스 맵에 대한 트래픽 가로채기와 배포 통계를 표시합니다.
- **show statistics pass-through type appnav** — 각 pass-through 사유에 대한 AppNav 트래픽 통계를 표시합니다.
- **show appnav-controller flow-distribution** — 정의된 정책 및 동적 로드 조건을 기반으로 특정 가상 흐름을 ANC에서 분류 및 배포하는 방법을 보여 줍니다.이 명령은 특정 플로우가 ANC에서 처리되는 방법과 해당 플로우가 속한 클래스를 확인하는 데 유용합니다.

WN에서 다음 명령을 사용하여 플로우 배포 문제를 해결하십시오.

- **show statistics service-insertion service-node** *ip-address* — WN에 배포된 가속기 및 트래픽에 대한 통계를 표시합니다.
- **show statistics service-insertion service-node-group name** group-*name* — WNG에 배포된 가속기 및 트래픽에 대한 통계를 표시합니다.

ANC에서 **show statistics class-map type appnav** *class-name* 명령을 사용하여 흐름 분산 문제를 해결할 수 있습니다. 예를 들어, 특정 클래스에 대해 트래픽이 느려지는 이유를 확인할 수 있습니다.이는 HTTP와 같은 애플리케이션 클래스 맵일 수도 있고, 브랜치에 대한 모든 트래픽이 느린 것처럼 보일 경우 브랜치 선호도 클래스 맵일 수도 있습니다.다음은 HTTP 클래스의 예입니다.

```
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
  ...
```

SN으로 표시 섹션의 WN 통과 이유는 WN에 통과 오프로드가 구성된 경우에만 증가합니다.그렇지 않으면 ANC는 WN이 연결을 통과하고 있음을 알지 못하고 그 수는 계산하지 않습니다.

연결:ANC 카운터에 의해 가로채기는 증가하지 않으며 가로채기에 문제가 있습니다.WAAS TcpTraceroute 유틸리티를 사용하여 네트워크에서 ANC의 배치 문제를 해결하고, 비대칭 경로를 찾고, 연결에 적용된 정책을 결정할 수 있습니다.자세한 내용은 연결 추적 섹션을 참조하십시오.

연결 디버깅을 위한 AppNav CLI 명령

ANC에서 개별 연결 또는 연결 집합을 디버깅하려면 **show statistics appnav-controller connection** 명령을 사용하여 활성 연결 목록을 표시할 수 있습니다.

```
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
```

클라이언트 또는 서버 IP 주소 및/또는 포트 옵션을 지정하여 목록을 필터링하고 detail 키워드를 지정하여 연결에 대한 자세한 통계를 표시할 수 있습니다.

```
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
...
```

요약 옵션을 지정하여 활성 분산 및 통과 연결 수를 표시할 수 있습니다.

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

연결 추적

AppNav 흐름 문제 해결을 지원하기 위해 중앙 관리자에서 연결 추적 도구를 사용할 수 있습니다.이 도구는 특정 연결에 대한 다음 정보를 표시합니다.

- 연결이 WNG에 전달되거나 배포된 경우
- 통과 이유(해당되는 경우)
- 연결이 배포된 WNG 및 WN

- 연결을 위해 모니터링되는 가속기
- 클래스 맵이 적용됨

연결 추적 도구를 사용하려면 다음 단계를 수행합니다.

1. [중앙 관리자] 메뉴에서 [**AppNav 클러스터] >** *클러스터 이름*을 선택한 다음 [**모니터] > [도구] > [연결 추적]을 선택합니다**.

2. ANC, 피어 WAAS 디바이스를 선택하고 연결 일치 기준을 지정합니다.

3. **추적을** 클릭하여 일치하는 연결을 표시합니다.

WAAS TCP Traceroute는 AppNav와 관련되지 않은 또 다른 툴로서 비대칭 경로를 포함하여 네트워크 및 연결 문제를 해결하는 데 도움이 됩니다.이를 사용하여 클라이언트와 서버 간의 WAAS 노드 목록과 연결을 위해 구성 및 적용된 최적화 정책을 찾을 수 있습니다.Central Manager에서 WAAS 네트워크에서 traceroute를 실행할 디바이스를 선택할 수 있습니다.WAAS Central Manager TCP Traceroute 툴을 사용하려면 다음 단계를 수행합니다.

1. WAAS Central Manager 메뉴에서 **Monitor > Troubleshoot > WAAS Tcptraceroute를** 선택합니다.또는 먼저 디바이스를 선택한 다음 이 메뉴 항목을 선택하여 해당 디바이스에서 traceroute를 실행할 수 있습니다.

2. WAAS Node(WAAS 노드) 드롭다운 목록에서 traceroute를 실행할 WAAS 장치를 선택합니다.(장치 컨텍스트에 있는 경우에는 이 항목이 나타나지 않습니다.)

3. Destination IP and Destination Port 필드에 traceroute를 실행할 대상의 IP 주소 및 포트를 입력합니다.

4. TCPTraceroute **실행을 눌러** 결과를 표시합니다.

추적된 경로의 WAAS 노드는 필드 아래의 테이블에 표시됩니다.CLI에서 waas**-tcptrace** 명령을 사용하여 이 유틸리티를 실행할 수도 있습니다.

AppNav 디버그 로깅

다음 로그 파일을 사용하여 AppNav 클러스터 관리자 문제를 해결할 수 있습니다.

- 디버그 로그 파일:/local1/errorlog/cmm-errorlog.current(및 cmm-errorlog*)

AppNav 클러스터 관리자의 디버그 로깅을 설정하고 활성화하려면 다음 명령을 사용합니다.

참고:디버그 로깅은 CPU를 많이 사용하며 대량의 출력을 생성할 수 있습니다.생산 환경에서 현명하게 그리고 드물게 사용하십시오.

디스크에 대한 자세한 로깅을 활성화할 수 있습니다.

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

클러스터 관리자 디버깅(5.0.1 이상)에 대한 옵션은 다음과 같습니다.

```
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
```

클러스터 관리자에 대한 디버그 로깅을 활성화한 다음 디버그 오류 로그의 끝을 다음과 같이 표시할 수 있습니다.

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

다음 명령을 사용하여 FDM(Flow Distribution Manager) 또는 FDA(Flow Distribution Agent)에 대한 디버그 로깅을 활성화할 수도 있습니다.

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

FDM은 WN의 정책 및 동적 로드 조건을 기반으로 플로우를 분배할 위치를 결정합니다.FDA는 WN 로드 정보를 수집합니다.다음 로그 파일을 사용하여 FDM 및 FDA 문제를 해결할 수 있습니다.

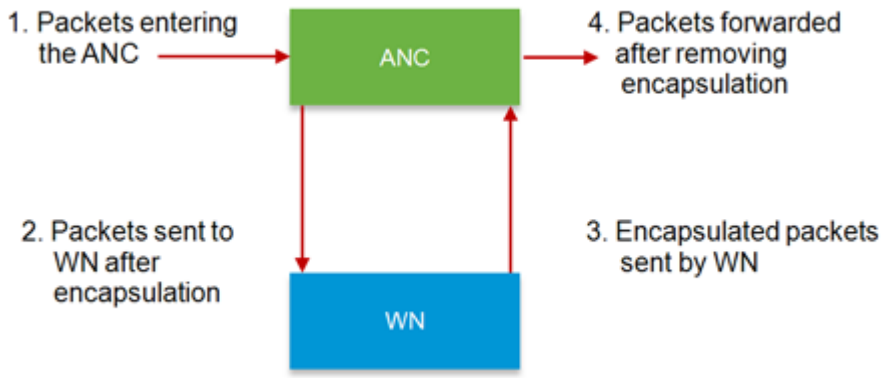
- 디버그 로그 파일:/local1/errorlog/fdm-errorlog.current(및 fdm-errorlog*)
- 디버그 로그 파일:/local1/errorlog/fda-errorlog.current(및 fda-errorlog*)

AppNav 패킷 캡처

Cisco AppNav Controller Interface Module의 인터페이스에서 데이터 패킷을 캡처할 수 있도록 새로운 **packet-capture** 명령이 도입되었습니다.이 명령은 다른 인터페이스에서 패킷을 캡처할 수 있으며 패킷 캡처 파일을 디코딩할 수 있습니다.packet-**capture** 명령은 사용되지 않는 명령 tcpdump 및 **tethereal**보다 선호되며, Cisco AppNav Controller Interface Module에서 패킷을 캡처할 수 없습니다.명령 구문에 대한 자세한 내용은 *Cisco Wide Area Application Services 명령 참조*를 참조하십시오.

참고:패킷 캡처 또는 디버그 캡처는 활성 상태일 수 있지만 둘 다 동시에 활성화할 수는 없습니다.

ANC와 WN 간에 전송되는 데이터 패킷은 다음 다이어그램과 같이 캡슐화됩니다.



다이어그램의 포인트 1 또는 4에서 패킷을 캡처하면 캡슐화되지 않습니다.포인트 2 또는 3에서 패킷을 캡처하면 캡슐화됩니다.

캡슐화된 패킷 캡처에 대한 샘플 출력입니다.

```
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)
```

다음은 캡슐화되지 않은 패킷 캡처의 샘플 출력입니다.

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

패킷 캡처 지침:

- 패킷 캡처 ACL은 WCCP-GRE 및 SIA 캡슐화된 패킷의 내부 IP 패킷에 항상 적용됩니다.
- 패킷 캡처에 대한 ANC 인터페이스가 제공되지 않은 경우 모든 ANC 인터페이스에서 패킷 캡처가 수행됩니다.

다음은 WN 인터페이스의 패킷 캡처에 대한 샘플 출력입니다.

```
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 ...
```

다음은 패킷 캡처 파일을 디코딩하는 예입니다.

```
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
```

패킷을 필터링하기 위해 src-ip/dst-ip/src-port/dst-port를 지정할 수 있습니다.

anc# packet-capture 디코드 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
```