

WAAS - App voor probleemoplossing

Hoofdstuk: App voor probleemoplossing

Dit artikel beschrijft hoe u een AppNav-toepassing kunt oplossen.

Inh

[Ho](#)
[De](#)
[Vo](#)
[Op](#)
[To](#)
[Pro](#)
[Pro](#)
[Pro](#)
[Pro](#)
[Pro](#)
[Pro](#)
[Pro](#)
[Pro](#)
[Pro](#)
[Pro](#)
[Pro](#)
[Pro](#)
[Pro](#)
[Pro](#)
[NA](#)

Inhoud

- [1 AppNav-probleemoplossing](#)
 - [1.1 Onderschepping in pad \(inline\)](#)
 - [1.2 WCCP-onderschepping \(Off Path\)](#)
 - [1.2.1 De WCCP-interceptie op de router configureren en controleren](#)
 - [1.2.2 Aanvullende informatie](#)
 - [1.3 Probleemoplossing voor netwerkconnectiviteit](#)
 - [1.3.1 Doorgifte door specifiek verkeer](#)
 - [1.3.2 Een inline ANC uitschakelen](#)
 - [1.3.3 Een ANC buiten het pad uitschakelen](#)
 - [1.4 AppNav-clusterprobleemoplossing](#)
 - [1.4.1 AppNav-alarmen](#)
 - [1.4.2 Central Manager-bewaking](#)
 - [1.4.3 AppNav CLI-opdrachten voor bewaking van cluster en apparaatstatus](#)
 - [1.4.4 AppNav CLI-opdrachten voor de bewaking van stroomdistributiestatistieken](#)
 - [1.4.5 AppNav CLI-opdrachten voor het afluisteren van verbindingen](#)
 - [1.4.6 Connection-tracering](#)

- [1.4.7 Vastlegging AppNav Debug](#)
- [1.5 AppNav-pakketvastlegging](#)

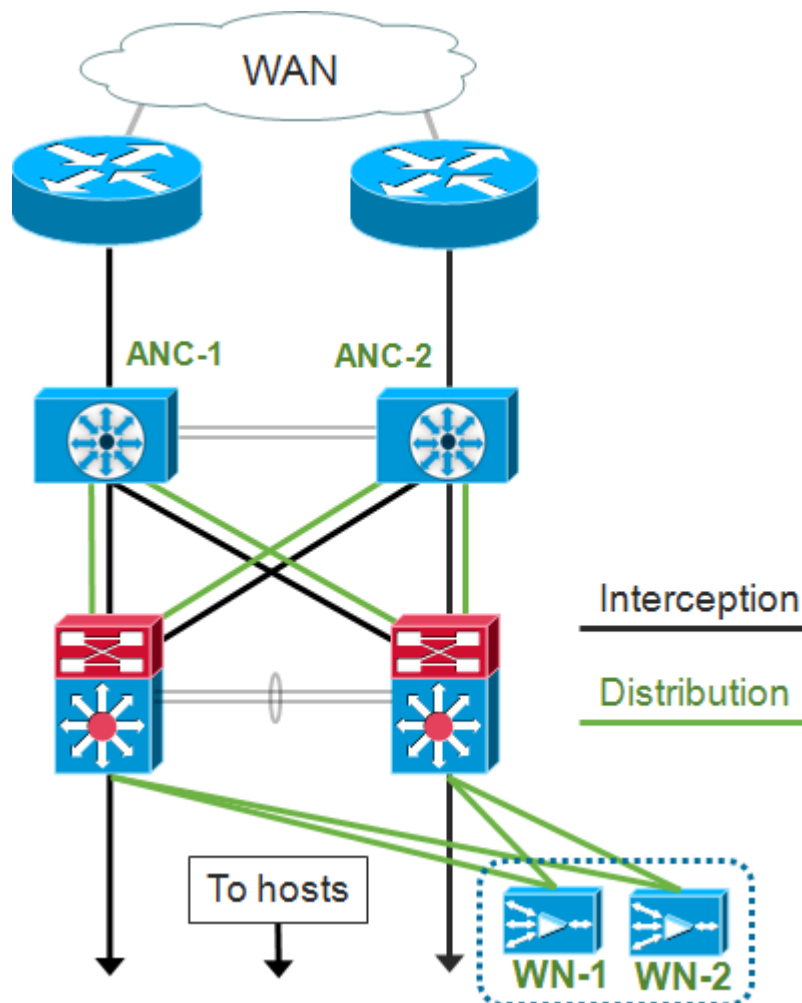
AppNav-probleemoplossing

Cisco WAAS AppNav vereenvoudigt de netwerkintegratie van WAN-optimalisatie en vermindert zeer de afhankelijkheid van de intercepterende switch of router door gebruik te maken van AppNav Controllers (ANC's) om verkeer tussen WAAS-knooppunten (WN's) te distribueren voor optimalisatie met behulp van een krachtig klasse en beleidsmechanisme. U kunt WAAS-knooppunten (WN's) gebruiken om het verkeer te optimaliseren op basis van locaties en/of toepassingen. Dit artikel beschrijft hoe u AppNav problemen kunt oplossen.

OPMERKING: De functie AppNav is toegevoegd in WAAS versie 5.0.1. Deze sectie is niet van toepassing op eerdere WAAS-versies.

Onderschepping in pad (inline)

In de inline modus worden de ANC's in het pad van het netwerkverkeer geplaatst waar ze pakketten onderscheppen en verdelen onder WN's.



De interfaceconfiguratie voor een inline implementatie wijst de interceptie- en distributiefuncties toe om interfaces te scheiden op de Cisco AppNav Controller interfacemodule. Een bridge-group interface is vereist voor interceptie en bestaat uit twee of meer fysieke of poort-kanaalinterfaces of één van elk. De brug-groepsinterface heeft geen bedradingsvermogen; dat wil zeggen dat het niet open is en het verkeer niet mechanisch wordt overbrugd na een storing of een verlies van kracht van de machine. AppNav gebruikt clustering om hoge beschikbaarheid te bieden als de AppNav

Controller interfacemodule, het link pad of de connectiviteit naar de AppNav Controller interfacemodule verloren is of er een stroomuitval is.

Opmerking: Bridge interfaces blokkeren geen BPDU-pakketten (bridge Protocol Data Unit), en in het geval van redundante interfaces, waarmee loops worden gemaakt, wordt een van de interfaces geblokkeerd door het Spanning Tree Protocol.

Problemen oplossen bij inline interceptie bestaat uit deze stappen:

- Controleer de juiste inline plaatsing van de ANC door het netwerkontwerp te controleren. Indien nodig, gebruik basisgereedschappen zoals pingelen en traceroute, of Layer 7 gereedschappen of toepassingen om te bevestigen dat het netwerkverkeerspad zoals verwacht is. Controleer de fysieke bekabeling van de ANC.
- Controleer dat ANC is ingesteld op inline interceptiemodus.
- Controleer dat de bridge-group interface correct is geconfigureerd.

De laatste twee stappen kunnen worden uitgevoerd in Central Manager of op de opdrachtregel, hoewel de Central Manager de voorkeursmethode is en eerst wordt beschreven.

Kies in Central Manager **Apparaten** > *AppNavController* en kies vervolgens **Configureren** > **Interceptie** > **Interceptie-configuratie**. Controleer of de interceptiemethode op Inline is ingesteld.

Controleer in hetzelfde venster of een bridge-interface is ingesteld. Als er een bridge interface nodig is, klikt u op **Bridge maken** om het te maken. U kunt maximaal twee leden interfaces toewijzen aan de bruggroep. U kunt de VLAN calculator gebruiken om de VLAN-items te definiëren op basis van bewerkingen opnemen of uitsluiten. Merk op dat de bridge interface geen IP-adres heeft toegewezen.

Gebruik het Alarmpaneel of de opdracht **Show Alarm** exec om te controleren of er op het apparaat al dan niet een brug gerelateerde alarmen ontstaan. Een bridge_down alarm geeft aan dat één of meer lid interfaces in de brug zijn omlaag.

Van CLI, volg deze stappen om online handeling te configureren:

1. Stel de interceptiemethode in op inline:

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

2. Maak de bridge-groepsinterface:

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

3. (Optioneel) Specificeer indien nodig de lijst met VLAN's die moet worden onderschept:

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

4. Voeg twee logische/fysieke interfaces toe aan de bridge-groepsinterface:

```
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

```

U kunt de opdracht **Show bridge** exec gebruiken om de operationele status van de brug interface te verifiëren en statistieken voor de brug te zien.

```

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

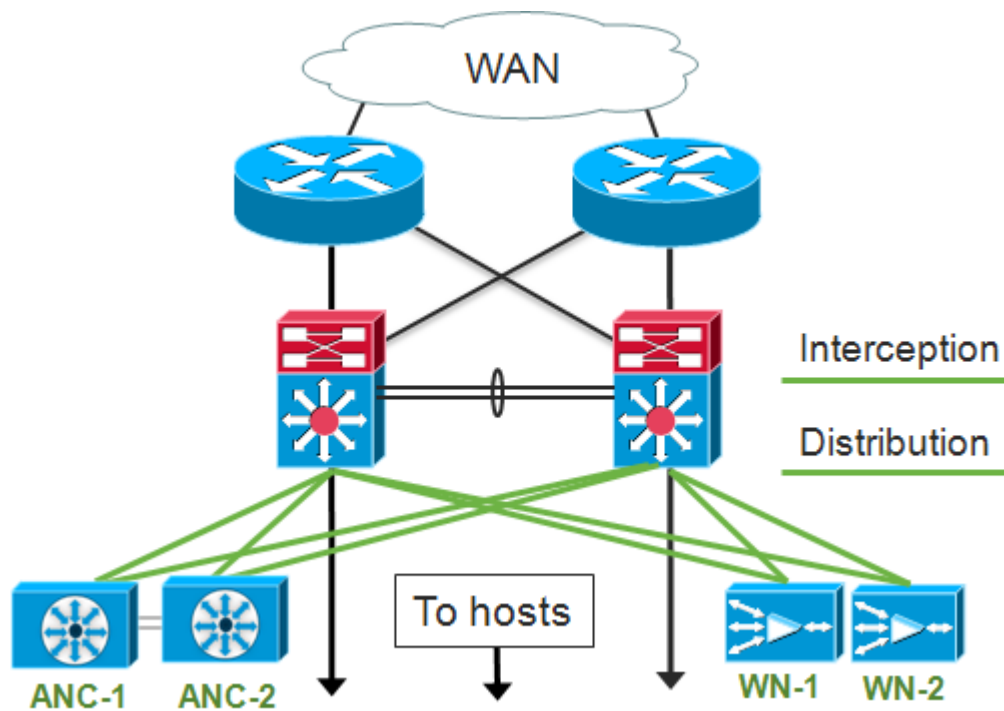
```

In het bovenstaande voorbeeld is de Gig 1/0-interface minder en is de Gig 1/1-interface ook plat vanwege link State propagation (LSP). U kunt ook Down (flow sync) zien, wat betekent dat de ANC zich bij een cluster aansluit en stroominformatie met andere ANCs in het cluster synchroniseert. Het houdt het afluisterpad (bridge interface) ongeveer twee minuten stil totdat alle ANC's gesynchroniseerd zijn, zodat de bestaande stromen correct verdeeld kunnen worden.

Het onderste deel van de output toont verkeersstatistieken voor de lidstaten interfaces.

WCCP-onderschepping (Off Path)

In WCCP-modus worden WCCP-routers in het pad van netwerkverkeer geplaatst waar ze pakketten onderscheppen en doorsturen naar ANC's die zich buiten het pad bevinden. Aangezien AppNav de interceptie-verwerking, de intelligente stroomdistributie en de lading-overweging tussen WAAS-versnellers verwerkt, wordt de WCCP-configuratie op de routers aanzienlijk vereenvoudigd.



In de interfaceconfiguratie voor een off-path implementatie kunnen de interceptie- en distributiefuncties dezelfde interfaces delen op de Cisco AppNav Controller interfacemodule, maar deze is niet vereist.

Problemen oplossen bij afluisteren bestaat uit deze stappen:

- Controleer de juiste plaatsing van de WCCP-routers om te verzekeren dat ze in het pad van verkeer naar en van de geoptimaliseerde hosts zijn. U kunt de opdrachten **Show run** gebruiken of **WCCP (WCCP) laten** zien om te controleren of dit dezelfde routers zijn die voor WCCP zijn ingesteld. Gebruik indien nodig basisgereedschappen zoals ping en traceroute of Layer 7-gereedschappen of toepassingen om te bevestigen dat al het verkeer dat optimalisatie nodig heeft, door de WCCP-routers loopt.
- Controleer de WCCP-configuratie op de WAAS-ANC's met behulp van ofwel de Central Manager (bij voorkeur) of de CLI.
- Controleer de WCCP-configuratie op de routers voor omleiding met behulp van de router CLI.

Om de configuratie van de WCCP op de ANC's te controleren, kiest u in de Central Manager **Apparaten > AppNavController**, en kiest u **Configureren > Interceptie > Interceptie Configuratie**

- Controleer of de interceptiemethode is ingesteld op WCCP.
- Controleer of het vakje Enable WCCP-service is ingeschakeld.
- Controleer dat het vakje Use Default Gateway as WCCP Router Control is ingeschakeld of dat de IP-adressen van de WCCP-router in het veld WCCP-router zijn opgenomen.
- Controleer dat de andere instellingen zoals het taakverdelingsmasker en de omleidingsmethode goed voor uw implementatie zijn ingesteld.

Controleer op alle WCCP-gerelateerde alarmen op de ANC's die deel uitmaken van het WCCP-routerbedrijf. Klik in Central Manager op het Alarmpaneel onder op het scherm of gebruik de opdracht Alarm op elk apparaat om alarmen weer te geven. Corrigeer alle alarmcondities door de configuratie op de ANC of router te wijzigen, zoals nodig.

Volg deze stappen vanuit de CLI om de WCCP-handeling te configureren:

1. Stel de interceptiemethode in op WCCP.

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

2. Het configureren van de WCCP-routerlijst, die de IP-adressen bevat van de routers die deelnemen aan de WCCP-boerderij.

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

3. Het configureren van de WCCP-service-ID. Eén service-ID wordt bij voorkeur voor AppNav gebruikt, hoewel twee service-ID's worden ondersteund.

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

4. Associeer de geconfigureerde routerlijst met de WCCP-service.

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

5. Het configureren van de WCCP-toewijzingsmethode (alleen de maskermethode wordt op een ANC ondersteund). Als u niet het dst-ip-masker of de src-ip-masker opties specificeert, wordt het IP-masker van de standaardbron op f ingesteld en wordt het IP-masker van de bestemming op 0 ingesteld.

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

6. Het configureren van de WCCP-omleidingsmethode (de egress- en retourmethoden worden automatisch ingesteld om de methode-omleiding aan te passen en zijn niet configureerbaar voor een ANC). U kunt L2 (de standaard) of GRE kiezen. L2 vereist dat ANC een Layer 2 verbinding met de router heeft en de router ook voor Layer 2 omleiding wordt geconfigureerd.

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

7. Schakel de WCCP-service in.

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

Controleer de interceptie van WCCP op elke ANC door het **tonen in werking stellen -in werking stellen** -configuratie opdracht te gebruiken. De twee onderstaande voorbeelden tonen de in werking gestelde configuratie uitvoer voor L2 omleiden en GRE omleiden.

Toon in werking stellen-configuratie wcp (voor L2 redirect):

```
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

WCCP (in werking stellen) weergeven (voor 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

Controleer de WCCP-status op elke ANC door de opdracht **WCCP-status weergeven** te gebruiken.

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

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

Controleer de routers die hebben gereageerd om berichten in leven te houden in de WCCP-boerderij door de opdracht **WCCP-routers** te gebruiken.

```
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
-NONE-
```

<<< List of routers seen by this ANC
<<< List of routers not seen by this ANC
<<< List of routers notified of but not configured in router list

Controleer de visie van elke ANCs op de andere ANCs in de WCCP-boerderij en de routers die door elk van hen bereikbaar zijn door de opdracht **van de show klanten te** gebruiken.

```
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
farm
Routers seeing this Wide Area Engine(2)
192.168.1.1
ANC
192.168.1.2
IP address = 10.10.10.32  Lead WAE = YES  Weight = 0
```

<<< Number of ANCs in the farm
<<< Entry for each ANC in the farm
<<< List of routers seeing this
<<< 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

Controleer dat de pakketten door elke ANC van de routers in het landbouwbedrijf worden ontvangen door de opdracht van de **show statistics wcp** te gebruiken. Statistieken voor verkeer dat van wordt ontvangen, doorgegeven en naar elke router wordt verstuurd, worden weergegeven. Cumulatieve statistieken voor alle routers in het bedrijf worden onderaan weergegeven. Een soortgelijk commando is **gebaseerd op wcp statistieken**. Merk op dat "OE" verwijst naar de ANC-apparaten hier.

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
```

De WCCP-interceptie op de router configureren en controleren

Om WCCP-interceptie op elke router in het WCCP-bedrijf te configureren volgt u deze stappen.

1. Het configureren van de WCCP-service op de router door de **IP**-routeropdracht te gebruiken.

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

2. Het configureren van WCCP-interceptie op de router LAN- en WAN-interfaces. U kunt dezelfde service-ID op beide interfaces configureren als u één service-ID op de ANC's gebruikt.


```
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. (Optioneel) Configureer een tunnelinterface als u generieke GRE-spanning gebruikt (alleen als u GRE voor de ANC WCCP-omleidingsmethode hebt gekozen).

```
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
```

Controleer de WCCP-configuratie op elke router in het landbouwbedrijf door de WCCP-opdracht **tonen** te gebruiken.

```
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
```

Aanvullende informatie

Zie voor meer informatie deze documenten:

- [WCCP-netwerkintegratie met Cisco Catalyst 6500: Aanbevelingen voor beste praktijken voor succesvolle implementaties](#)
- [Cisco Wide Area Application Services Web Cache Communication Protocol-omleiding: Ondersteuning van Cisco-routerplatform](#)
- [Geavanceerde WCCP-functies op routers configureren vanuit de Cisco Wide Area Application Services Configuration-gids](#)
- [WCCP op WAE's configureren vanuit de Cisco Wide Area Application Services Configuration-gids](#)

Probleemoplossing voor netwerkconnectiviteit

Bij het oplossen van problemen met WAAS is het misschien handig om te bepalen hoe het netwerk zich gedraagt met WAAS uitgeschakeld. Dit is behulpzaam wanneer het verkeer niet alleen niet optimaal is, maar er helemaal niet in slaagt te slagen. In deze gevallen kan blijken dat het probleem niet te maken heeft met WAAS. Zelfs in gevallen waar verkeer doorkomt, kan deze techniek helpen bepalen welke WAAS-apparaten een oplossing vereisen.

Voordat u Layer 3-connectiviteit gaat testen, dient u te controleren of de AppNav-controller interfacemodule is aangesloten op de juiste switch-poorten. Als de aangesloten switch ondersteuning biedt en Cisco Discovery Protocol (CDP) ingeschakeld heeft, **laat** de opdracht **Cdp-buurt****details** zien om de juiste connectiviteit in de switch van het netwerk te controleren.

WAAS uitschakelen is mogelijk niet in alle gevallen van toepassing. Als al het verkeer wordt geoptimaliseerd en sommige niet, kan het onacceptabel zijn om WAAS uit te schakelen, waardoor het verkeer wordt verstoord dat met succes wordt geoptimaliseerd. In zo'n geval kan het interceptie ACL of het AppNav beleid worden gebruikt om door het specifieke type verkeer te gaan dat problemen ondervindt. Zie voor meer informatie het gedeelte [dat door specifiek verkeer gaat](#).

Om WAAS uit te schakelen worden er verschillende stappen uitgevoerd voor inline modus dan voor off-path modus:

- Voor inline mode moet de interceptiebrug in de doorvoerstaat geplaatst worden. Zie voor meer informatie de sectie [Een inline ANC uitschakelen](#).
- Voor de off-path-modus moet u het WCCP-protocol uitschakelen. Zie voor meer informatie het gedeelte [Een ANC uit het pad uitschakelen](#).

In AppNav-omgevingen hoeven alleen de ANC's te worden uitgeschakeld. Ze hoeven niet te worden uitgeschakeld, omdat ze niet deelnemen aan interceptie.

Nadat WAAS is uitgeschakeld, controleert u de netwerkconnectiviteit met behulp van standaardmethoden.

- Controleer Layer 3 connectiviteit met gereedschap zoals pingelen en traceroute.
- Toepassingsgedrag controleren om de bovenste lagen connectiviteit te bepalen
- Als het netwerk de zelfde connectiviteitsproblemen ervaart die het met WAAS toegelaten was, is het probleem waarschijnlijk niet-WAAS gerelateerd.
- Als het netwerk prima werkt met WAAS uitgeschakeld, maar aansluitingsproblemen met WAAS ingeschakeld heeft, dan zijn er waarschijnlijk een of meer WAAS-apparaten die aandacht vereisen. De volgende stap is het probleem te isoleren van specifieke WAAS-apparaten.
- Als het netwerk connectiviteit heeft met en zonder WAAS toegelaten, maar er is geen optimalisatie, dan zijn er waarschijnlijk één of meerdere WAAS apparaten die aandacht vereisen. De volgende stap is het probleem te isoleren van specifieke WAAS-apparaten.

Om netwerkgedrag te controleren met WAAS ingeschakeld, volgt u deze stappen:

1. De WAAS-functionaliteit op de WAAS-ANC's en, indien van toepassing, de WCCP-routers kan worden hersteld.
2. Als u heeft vastgesteld dat er een WAAS-gerelateerd probleem is, stelt u elke AppNav-cluster en/of ANC afzonderlijk in om het te isoleren als mogelijke oorzaak van het waargenomen probleem.
3. Aangezien elke ANC is ingeschakeld, voert u dezelfde basistests voor de netwerkconnectiviteit uit als in eerdere stappen en merkt u op of deze specifieke ANC correct lijkt te werken. In dit stadium zijn geen individuele WN's van toepassing. Het doel in deze fase is om te bepalen welke clusters, en welke specifieke ANC's, gewenst of ongewenst gedrag ervaren.
4. Als elke ANC is ingeschakeld en getest, schakelt u deze opnieuw uit zodat de volgende ANC ingeschakeld kan worden. Het in staat stellen en het testen van elke ANC staat u om te bepalen welke van de ANC's verdere problemen vereisen.

Deze techniek voor het oplossen van problemen is het meest van toepassing in situaties waar de WAAS-configuratie niet alleen niet lijkt te optimaliseren, maar ook problemen veroorzaakt met de normale netwerkconnectiviteit.

Doorgifte door specifiek verkeer

U kunt door specifiek verkeer passeren door een interceptie ACL te gebruiken of door het beleid AppNav te configureren voor doorgifte.

- Maak een ACL die het specifieke verkeer ontkent om door te gaan en laat al het andere toe. In dit voorbeeld willen we doorgeven door HTTP-verkeer (testpoort 80). Stel de ANC-toeganglijst voor interceptie in op de gedefinieerde ACL. Aansluitingen bestemd voor poort 80 worden doorlopen. U kunt de opdracht **Show statistics pass-through type appnav** gebruiken om te verifiëren dat pass-through plaatsvindt door te controleren dat de PT Intercept ACL tellers stijgend zijn.

```
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
```

- Configureer het beleid ANC om door specifieke klassen van verkeer te bladeren.

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

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

Een inline ANC uitschakelen

Er zijn verschillende manieren om een inline ANC uit te schakelen door deze in doorvoerstaat te plaatsen:

- Stel de lijst VLAN-interceptiebridge in op nul. Kies in Central Manager een ANC-apparaat en kies vervolgens **Configureren > Interceptie > Interceptie Configuratie**. Selecteer de bridge-interface en klik op het pictogram Eigenschappen. Stel het veld VLAN's in op de waarde "geen".
- Schakel de serviceconnector uit die de ANC bevat. Kies in Central Manager een cluster en klik vervolgens op het tabblad AppNav-controllers, selecteer een ANC en klik op het pictogram taakbalk **uitschakelen**.
- Pas een interceptie ACL toe met "ontkennen ALLE" criteria. Deze methode heeft de voorkeur. (De eerste twee methoden verstoren bestaande geoptimaliseerde verbindingen.) Definieer een ACL met ontken ALLE criteria. Kies in Central Manager een ANC-apparaat en kies vervolgens **Configureren > Interceptie > Toegangslijst met interceptie** en kies de vervolgkeuzelijst ALLE toegang in de AppNav Controller interceptie van interceptie ontkennen.

Om interceptie met een ACL uit de CLI uit te schakelen, gebruikt u de volgende opdrachten:

```
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
```

Een ANC in doorvoertoestand plaatsen:

- Schakel WAAS-interceptie uit in plaats van de interfaces.
- schakelt alle WAAS-optimalisatie uit.
- Veroorzaakt al het verkeer onaangetast door te gaan.

Een ANC buiten het pad uitschakelen

Als u een ANC wilt uitschakelen die in de off-path-modus staat, schakelt u het WCCP-protocol voor de ANC uit. U kunt deze actie uitvoeren op de ANC of op de router of beide. Op ANC kunt u de WCCP-services uitschakelen of verwijderen, of u kunt de interceptiemethode verwijderen of deze van WCCP naar een andere methode wijzigen.

Om WCCP-interceptie uit te schakelen kiest u in Central Manager een ANC-apparaat en kiest u **vervolgens Configuration > Interception > Interception Configuration**. Schakel het aankruisvakje voor WCCP-service uit of klik op het pictogram Instellingen verwijderen om de WCCP-interceptie-instellingen volledig te verwijderen (deze worden verloren).

Om WCCP-interceptie vanuit de CLI uit te schakelen, gebruikt u de volgende opdrachten:

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

In sommige gevallen, kunnen er meerdere ANC's zijn die hergericht verkeer van de zelfde router ontvangen. Voor het gemak kunt u ervoor kiezen om WCCP op de router uit te schakelen, in plaats van de ANC's. Het voordeel is dat u meerdere ANC's uit een WCCP-boerderij in één stap kunt verwijderen. Het nadeel is dat je dit niet kunt doen vanuit WAAS Central Manager.

Om WCCP op de router uit te schakelen, gebruikt u de volgende syntaxis:

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

Om WCCP op de router opnieuw in te schakelen, gebruikt u de volgende syntaxis:

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

Controleer bij elke WCCP-router of de ANC's die u hebt geselecteerd om uit te schakelen, niet worden weergegeven als WCCP-clients. De volgende uitvoer wordt weergegeven wanneer de WCCP-services op de router zijn verwijderd.

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

AppNav-clusterprobleemoplossing

U kunt de volgende gereedschappen gebruiken om een AppNav-cluster problemen op te lossen:

- [AppNav-alarmen](#)
- [Central Manager-bewaking](#)
- [AppNav CLI-opdrachten voor bewaking van cluster en apparaatstatus](#)
- [AppNav CLI-opdrachten voor de bewaking van stroomdistributiestatistieken](#)
- [Connection-tracering](#)
- [Vastlegging AppNav Debug](#)

AppNav-alarmen

De Cluster Membership Manager (CMM) roept de volgende alarmen op als gevolg van foutomstandigheden:

- Verlaagd cluster (kritiek) — gedeeltelijk zicht onder ANC's. ANC zal door nieuwe verbindingen gaan.
- Convergentie is mislukt (Kritisch) - ANC is er niet in geslaagd om samen te vallen op een stabiele weergave van ANC's en WN's. ANC zal door nieuwe verbindingen gaan.
- ANC Join mislukt (Kritisch)—ANC is er niet in geslaagd zich aan te sluiten bij een bestaand cluster door mogelijke degradatie van het cluster met de ANC erin.
- ANC Mixed Farm (Minor)—ANC's in het cluster zijn verschillende maar compatibele versies van het clusterprotocol actief.
- ANC onbereikbaar (groot) - een geconfigureerde ANC is onbereikbaar.
- WN onbereikbaar (groot) - een ingesteld WN is onbereikbaar. Dit WAN wordt niet gebruikt voor verkeersomleiding.
- WN Uitgesloten (Major) - Een ingesteld WN is bereikbaar maar uitgesloten omdat een of meer andere ANC's het niet kunnen zien. Dit WAN wordt niet gebruikt voor omleiding van verkeer (nieuwe verbindingen).

U kunt alarmen zien in het paneel Centrale Manager of door het bevel van de **show EXEC** op een apparaat te gebruiken.

Opmerking: CMM is een interne AppNav-component die de groepering van ANC's en WN's in een AppNav-cluster beheert die gekoppeld is aan een servicecontext.

Central Manager-bewaking

U kunt de clusters van de Centrale Manager gebruiken om te verifiëren, controleren en problemen oplossen in AppNav. Central Manager heeft een globaal beeld van alle geregistreerde WAAS-apparaten in uw netwerk en kan u snel helpen de meeste AppNav-problemen te vinden.

Kies in het menu Central Manager de **naam AppNav-clusters > clusternaam**. Het venster van het clusterstartpunt toont de clustertopologie (met inbegrip van WCCP en gatewayrouters), de algemene clusterstatus, de status van het apparaat, de status van de apparaatgroep en de verbindingstatus.

Controleer eerst of de algemene clusterstatus operationeel is.

Merk op dat de ANC en de WN pictogrammen in dit diagram dezelfde apparaatnaam hebben omdat ze op hetzelfde apparaat voorkomen. Op een ANC die ook verkeer als WAN optimaliseert, worden deze twee functies als afzonderlijke pictogrammen in het topologiediagram weergegeven.

Een oranje driehoekswaarschuwingsindicator wordt getoond op elk apparaat waarvoor de Centrale Manager wellicht geen actuele informatie heeft omdat het apparaat niet binnen de laatste

30 seconden heeft gereageerd (het apparaat zou offline of onbereikbaar kunnen zijn).

U kunt een gedetailleerde statusweergave van 360 graden van elk ANC- of WAN-apparaat verkrijgen door de cursor over het pictogram van het apparaat te laten zweven. Het eerste tabblad geeft alarmen op het apparaat weer. U dient alle alarmen op te lossen die de juiste clusterwerking remmen.

Klik op het tabblad Interceptie om de methode voor apparaatinterceptie bij elke ANC te controleren.

Als de interceptie wordt afgebroken, wordt de status als volgt weergegeven:

Klik op het tabblad Cluster Control om het IP-adres en de status van elk apparaat in het cluster te zien dat deze ANC kan zien. Elke ANC in het cluster moet dezelfde lijst van apparaten hebben. Als dit niet het geval is, duidt dit op een probleem met de configuratie of het netwerk.

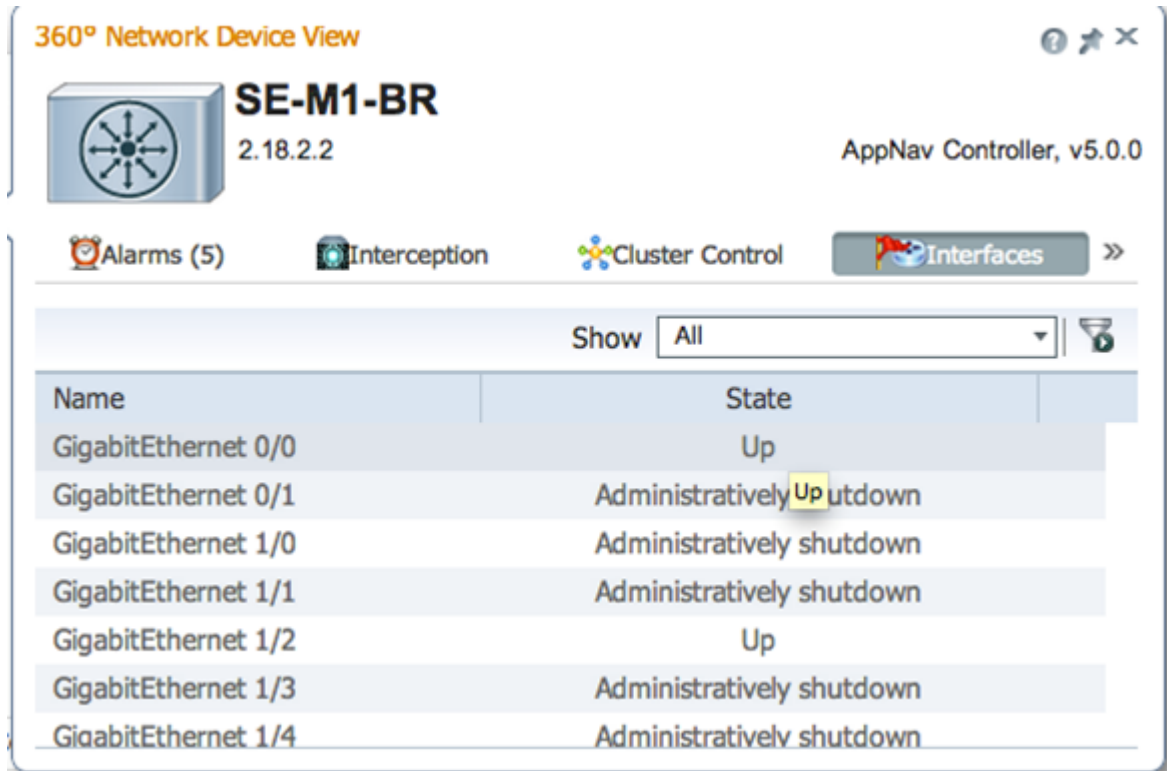
Als alle ANC's elkaar niet kunnen zien, is de cluster niet operationeel en wordt al het verkeer doorgeleid door het onvermogen van de cluster om stromen te synchroniseren.

Als alle ANC's aangesloten zijn maar verschillende opvattingen van de WN's hebben, is het

cluster in gedegradeerde staat. Het verkeer is nog verdeeld, maar alleen aan de WN's die door alle ANC's worden gezien.

Alle WN's die niet door alle ANC's worden gezien, worden uitgesloten.

Klik op het tabblad Interfaces om de status van de fysieke en logische interfaces in de ANC te controleren.



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 shutdown
GigabitEthernet 1/0	Administratively shutdown
GigabitEthernet 1/1	Administratively shutdown
GigabitEthernet 1/2	Up
GigabitEthernet 1/3	Administratively shutdown
GigabitEthernet 1/4	Administratively shutdown

Kijk naar de 360 graden weergave op elk WN in het cluster en controleer de groene status van alle versnellers in het tabblad Optimization. Een gele status voor een versneller betekent dat de versneller actief is maar geen nieuwe verbindingen kan onderhouden, bijvoorbeeld omdat de versneller overbelast is of omdat de licentie is verwijderd. Een rode status geeft aan dat de versneller niet actief is. Als een versneller geel of rood is, moet u deze versnellers afzonderlijk oplossen. Als de Enterprise-licentie ontbreekt, wordt de systeemicentie ingetrokken. Installeer de Enterprise-licentie in **Admin > History > Licentiebeheer**.

Een gesplitste cluster resultaat van connectiviteitsproblemen tussen ANC's in de cluster. Als de Central Manager met alle ANC's kan communiceren, kan het een gesplitste cluster detecteren, maar als deze niet met sommige ANC's kan communiceren, kan dit de gesplitste bestanden niet detecteren. Het "Beheersstatus is offline" alarm wordt verhoogd als de Centrale Manager connectiviteit met om het even welk apparaat verliest en het apparaat als offline in de Centrale Manager wordt getoond.

Het is best om de beheerinterfaces van de gegevensinterfaces te scheiden om beheerconnectiviteit te handhaven zelfs als een gegevenslink is neergeslagen.

In een gesplitste cluster verdeelt elke subcluster van ANC's onafhankelijk stromen naar de WNG's die zij kan zien, maar aangezien stromen tussen de subclusters niet gecoördineerd zijn, kan zij terugstelverbindingen veroorzaken en de algehele clusterprestaties afnemen.

Controleer het tabblad Cluster Control van elke ANC om te zien of een of meer ANC's onbereikbaar zijn. Het "Service Controller is onbereikbaar"-alarm wordt verhoogd als twee ANC's die ooit met elkaar konden communiceren, onderlinge connectiviteit verliezen, maar deze situatie is niet de enige oorzaak van een gesplitste cluster zodat het best het tabblad Cluster Control van elke ANC te controleren is.

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	

Als een ANC een grijs statuslicht heeft, wordt het uitgeschakeld. Controleer of alle ANC's zijn ingeschakeld door op het tabblad AppNav-controllers onder het topologiediagram te klikken. Als een ANC niet is ingeschakeld, is de Aan/Uit-status Nee. U kunt op het pictogram Taakbalk inschakelen klikken om een ANC in te schakelen.

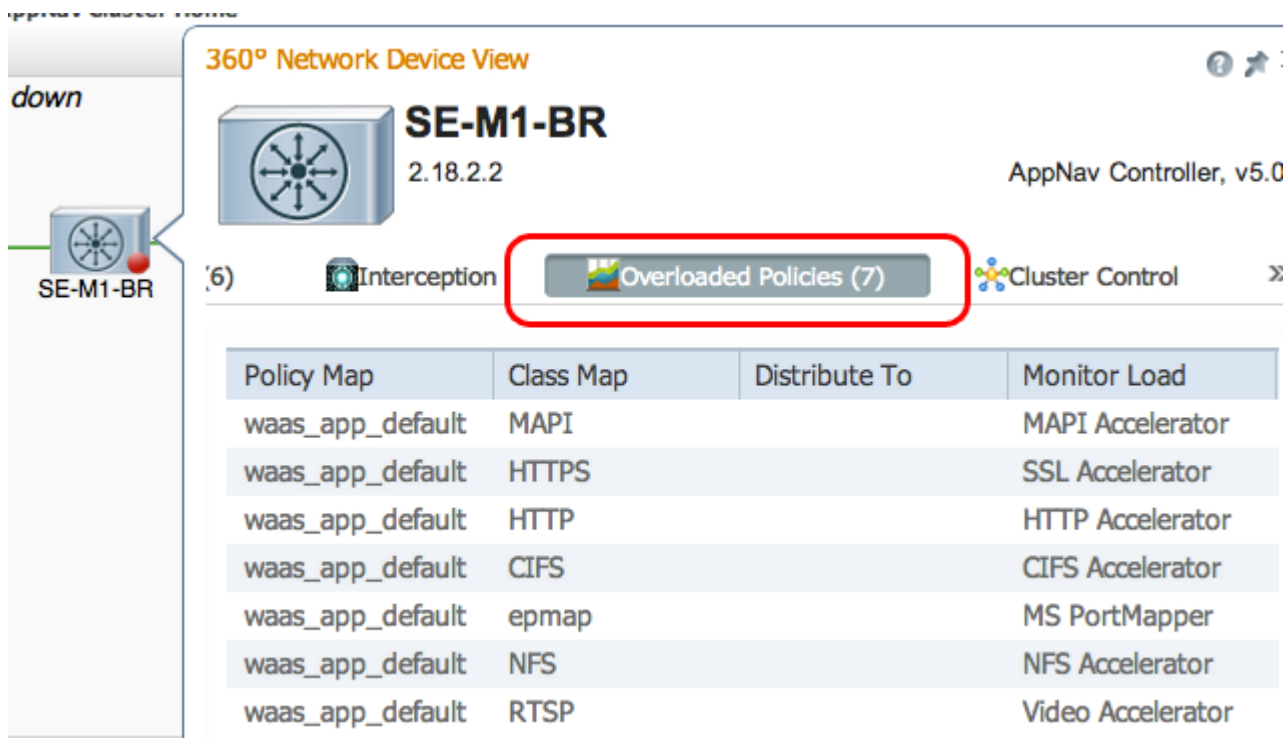
Controleer het AppNav-beleid op elke ANC die iets anders heeft dan een groen statuslicht. Als u de cursor over het statuslicht op een apparaat zweeft, dan vertelt een gereedschapstip u de status of het probleem als er een is gedetecteerd.

Om het gedefinieerde beleid te controleren kiest u in het menu Central Manager **beleid instellen > AppNav beleid** en vervolgens klikt u op de knop **Manager**.

In het algemeen moet één enkel beleid worden toegewezen aan alle ANC's in het cluster. Het standaard beleid heet appnav_default. Selecteer de radioknop naast een beleid en klik op het pictogram van de taakbalk **bewerken**. Het venster AppNav-beleid toont de ANC's waarop het geselecteerde beleid van toepassing is. Als alle ANC's niet met een selectieteken worden weergegeven, klikt u op het selectieteken naast elke ongecontroleerde ANC om het beleid aan deze ANC toe te wijzen. Klik op **OK** om de wijzigingen op te slaan.

Na het controleren van de beleidstaken, kunt u de beleidsregels in de pagina AppNav Beleid verifiëren dat wordt weergegeven. Selecteer een willekeurige beleidsregel en klik op het pictogram Taakbalk bewerken om de definitie ervan te wijzigen.

Een ANC zou een geel of rood statuslicht kunnen hebben als een of meer beleid worden overbelast. Controleer het tabblad Overload beleid van het apparaat met 360 graden om een lijst te zien van gemonitord beleid dat overbelast is.



360° Network Device View

down

SE-M1-BR

SE-M1-BR

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

Als een ANC zich bij het cluster voegt, wordt het getoond met een geel statuslicht en toetredende status.

Het tabblad Interceptie van de apparaatweergave van 360 graden toont aan dat het afluisterpad is afgenomen vanwege de toetredende staat. Interceptie wordt afgebroken totdat de ANC zijn stroomtabellen met de andere ANC's heeft gesynchroniseerd en klaar is om verkeer te accepteren. Dit proces duurt doorgaans niet langer dan twee minuten.

Als u een ANC uit een cluster verwijdert, wordt het nog een paar minuten in het topologiediagram en als levend in het tabblad Cluster Control weergegeven, tot alle ANCs het eens zijn over de nieuwe clustertopologie. Zij ontvangt geen nieuwe stromen in deze staat.

AppNav CLI-opdrachten voor bewaking van cluster en apparaatstatus

Verschillende CLI-opdrachten zijn handig om een oplossing te vinden in een ANC:

- draaiing service-invoeging tonen
- service-invoeging-context tonen
- IT-invoeging van dienst tonen
- Service-invoeging tonen van serviceknoopgroep
- voor het aanbrengen van de dienst bestemde controller *IP-adres*
- Service-insertie-serviceknooppunt tonen [*ip-adres*]
- Service-invoeging tonen van serviceknoopgroep *groepsnaam*

Gebruik deze opdrachten in een WAN:

- draaiing service-invoeging tonen
- serviceknooppunt voor installatie tonen

U kunt de opdracht **service-invoegservice-context** op een ANC gebruiken om de status van de serviceconversiecontext en de stabiele weergave van de apparaten in het cluster te zien:

```
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
```

Als het veld Apparaat Interception State (hoger) de shutdown toont, betekent dit dat de CMM de interceptie heeft afgesloten omdat deze ANC niet klaar is om verkeersstromen te ontvangen. Zo zou de ANC nog steeds deel kunnen uitmaken van het toetredingsproces en heeft het cluster nog geen gesynchroniseerde stromen.

De velden van de Stable View (hierboven) maken een lijst van de IP adressen van de ANC's en van WAN's die door dit ANC-apparaat in zijn laatste geconvergeerde weergave van het cluster worden gezien. Dit is de weergave die wordt gebruikt voor distributieactiviteiten. De velden Huidige weergave bevatten een lijst van de apparaten die door deze ANC worden geadverteerd in de hartslag berichten.

U kunt de opdracht voor de **show service-insertie van een controller-group** op een ANC gebruiken om de status van elke ANC in de ANC-groep te zien:

```
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
```

Voor een lijst van mogelijke ANC status en de toetredende status, zie de opdracht van de **show service-invoeging** in de *Cisco Wide Area Application Services Opdrachtshandleiding*.

U kunt de opdracht **service-invoegservice-knooppunt** op een ANC gebruiken om de status van een bepaald WN in het cluster te zien:

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
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
```

<<< WN is visible

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
```

U kunt de opdracht van de **show service-invoegservice-knooppunt-groep** op een ANC gebruiken om de status van een bepaalde WNG in het cluster te zien:

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

Het eerste WN in het bovenstaande voorbeeld heeft een status van exclusief, wat betekent dat het WN zichtbaar is voor de ANC, maar van het cluster is uitgesloten omdat een of meer andere ANC's het niet kunnen zien.

De beschikbaarheid van SNG per AO-tabel toont als elke AO nieuwe verbindingen kan onderhouden. Er is een AO beschikbaar indien ten minste één WN in het WNG een GROENE status heeft voor de AO.

U kunt de opdracht **service-invoegservice-knooppunt** in een WN gebruiken om de status van het WAN te zien:

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
```

De gecontroleerde toestand van een versneller is de werkelijke toestand, maar de gerapporteerde toestand kan verschillen omdat die de laagste is van de systeemtoestand of de accelerator.

Zie de artikelen [Problemen oplossen](#) en [Problemen oplossen bij optimalisatie van de toepassing](#).

AppNav CLI-opdrachten voor de bewaking van stroomdistributiestatistieken

Verschillende CLI-opdrachten zijn nuttig voor het oplossen van problemen en voor de stroomdistributie op een ANC:

- **Toon het beleid-kaart type appnav *beleidskaart-naam*** — toont de beleidsregels en slaat tellingen op voor elke klasse in de beleidskaart.
- **Toon class-map type appnav *class-name*** — Toont de matchcriteria en hit tellingen voor elke matrixconditie in de class map.
- **Toon beleid-subklasse type appnav *level1-class-name level2-class-name*** — toont de matchcriteria en hit tellingen voor elke matrixconditie in een class map in een geneste AppNav-beleidskaart.
- **Toon statistieken class-map type appnav *class-name*** — Toont traffic interception and distribution statistics voor een class map.
- **Statistieken beleid-subklasse type appnav *level1-class-name level2-class-name*** — toont verkeersinterceptie- en distributiestatistieken voor een class map in een geneste AppNav-beleidskaart.
- **Statistieken doorgeven-type app** — Toont AppNav-verkeersstatistieken voor elke doorvoerreden.
- **toont de stroomverdeling van de controller** — toont hoe een specifieke hypothetische stroom door een ANC zou worden geclassificeerd en verdeeld op basis van het vastgestelde beleid en de dynamische belastingsomstandigheden. Deze opdracht kan handig zijn om te controleren hoe een bepaalde stroom op een ANC verwerkt zal worden en op welke klasse de opdracht behoort.

Gebruik deze opdrachten in een WN om de stroomdistributie van de oplossing te verbeteren:

- **Statistische dienst-invoeging service-knooppunt *ip-adres*** — Geeft statistieken weer voor versnellers en verkeer gedistribueerd naar de WAN.
- **Toon statistieken service-invoeging service-knooppunt-groepsnaam *groepsnaam*** — Toont statistieken voor versnellers en verkeer dat naar WNG wordt gedistribueerd.

U kunt de opdracht **class-map** van de **show statistics class-map type *class-name*** op een ANC

gebruiken om de stroomdistributie van de problemen op te lossen, bijvoorbeeld om te bepalen waarom verkeer voor een bepaalde klasse langzaam zou kunnen zijn. Dit kan een applicatie class-kaart zijn zoals HTTP of, als al het verkeer naar een tak langzaam lijkt, kan het een tak-affiniteitclass-kaart zijn. Hier is een voorbeeld voor de 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
  ...

```

De WAN-doorvoerredenen in de modus aangegeven door de toename van de SN-sectie alleen als de doorloop-offload op een WAN is ingesteld. Anders weet de ANC niet dat het WAN door een verbinding stroomt en telt het niet.

Als de verbindingen: Interceptie door een ANC-teller neemt niet toe, er is een onderscheppingsprobleem. U kunt de WAAS TCPTraceroute-hulpprogramma gebruiken om de plaatsing van ANC in het netwerk problemen op te lossen, asymmetrische paden te vinden en het beleid te bepalen dat op een verbinding wordt toegepast. Zie voor meer informatie de sectie

[Connection Tracing.](#)

AppNav CLI-opdrachten voor het afluisteren van verbindingen

Om een individuele verbinding of een reeks verbindingen op een ANC te zuiveren, kunt u de opdracht van de **de verbinding van de** showstatistiek **gebruiken** om de actieve verbindinglijst te tonen.

```
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
```

U kunt de lijst filteren door het client- of server-IP-adres en/of poortopties op te geven en u kunt gedetailleerde statistieken over verbindingen tonen door het **detail** sleutelwoord te specificeren.

```
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
...
```

U kunt de summiere optie specificeren om het aantal actieve gedistribueerde en doorvoerverbindingen weer te geven.

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

Connection-tracering

Als u wilt helpen bij het oplossen van problemen in de stromen van AppNav, kunt u het gereedschap Koppelspoor in de Centrale Manager gebruiken. Dit gereedschap bevat de volgende informatie voor een bepaalde verbinding:

- Als de aansluiting is doorgegeven of gedistribueerd naar een WNG
- Doorloopreden, indien van toepassing
- Het WNG en de WAN waarnaar de verbinding werd verdeeld
- Accelerator bewaakt voor aansluiting
- Klasse-kaart toegepast

U kunt het gereedschap Koppingspaneel gebruiken door de volgende stappen te volgen:

1. Kies in het menu Central Manager de optie **AppNav-clusters** > *clusternaam* en kies vervolgens **monitor** > **Gereedschappen** > **Koppingspaneel**.
2. Kies de ANC, het peer WAAS-apparaat en specificeer de verbindingscriteria.
3. Klik op **Overtrekken** om de gekoppelde verbindingen weer te geven.

WAAS TCP Traceroute is een ander gereedschap dat niet specifiek is voor AppNav dat u kan helpen netwerk- en verbindingskwesties, met inbegrip van asymmetrische paden, oplossen. U kunt het gebruiken om een lijst van WAAS knopen tussen de client en de server te vinden, en het geconfigureerde en toegepaste optimaliseringsbeleid voor een verbinding. Van de Centrale Manager, kunt u om het even welk apparaat in uw netwerk van WAAS kiezen waarvan om het Tracoute te lopen. Om het gereedschap WAAS Central Manager TCP Traceroute te gebruiken, volgt u deze stappen:

1. Kies in het menu WAAS Central Manager de optie **Monitor** > **Probleemoplossing** > **WAAS Tcptraceroute**. In plaats hiervan kunt u eerst een apparaat kiezen en vervolgens dit menu-item kiezen om de traceroute van dat apparaat uit te voeren.
2. Selecteer in de vervolgkeuzelijst WAAS Node een WAAS-apparaat waarmee u het traceroute kunt uitvoeren. (Dit item is niet weergegeven als u zich in de apparaatcontext bevindt.)
3. In de velden Bestemming IP en Bestemming van de poort geeft u het IP-adres en de poort van de bestemming in waarop u de traceroute wilt uitvoeren
4. Klik op **TCPtraceroute uitvoeren** om de resultaten weer te geven.

WAAS-knooppunten in het overtrek-pad worden in de tabel onder de velden weergegeven. U kunt deze voorziening ook vanuit de CLI uitvoeren met de opdracht **waas-tcptrace**.

Vastlegging AppNav Debug

Het volgende logbestand is beschikbaar voor problemen met AppNav-clustermanager bij probleemoplossing:

- Debug logbestanden: /local1/errorlog/cmm-errorlog.current (en cmm-orlog.*)

Gebruik de volgende opdrachten om de houtkap van de AppNav-clustermanager in te stellen en in te schakelen.

OPMERKING: Debug logging is CPU-intensief en kan een grote hoeveelheid output genereren. Gebruik het voorzichtig en spaarzaam in een productieomgeving.

U kunt gedetailleerd loggen op de schijf inschakelen:

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

De opties voor het fouilleren van clustermanager (op 5.0.1 en later) zijn als volgt:

```
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
```

U kunt debug-loggen voor de clusterbeheerder inschakelen en vervolgens het einde van het debug-logbestand als volgt weergeven:

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

U kunt ook debug logging mogelijk maken voor de flow distribution Manager (FDM) of het flow distribution Agent (FDA) met deze opdrachten:

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

De FDM bepaalt waar de stromen worden verdeeld op basis van het beleid en de dynamische belastingsomstandigheden van de WAN's. De FDA verzamelt gegevens over de belasting in het EIGEN LAND. De volgende logbestanden zijn beschikbaar voor problemen met FDM en FDA:

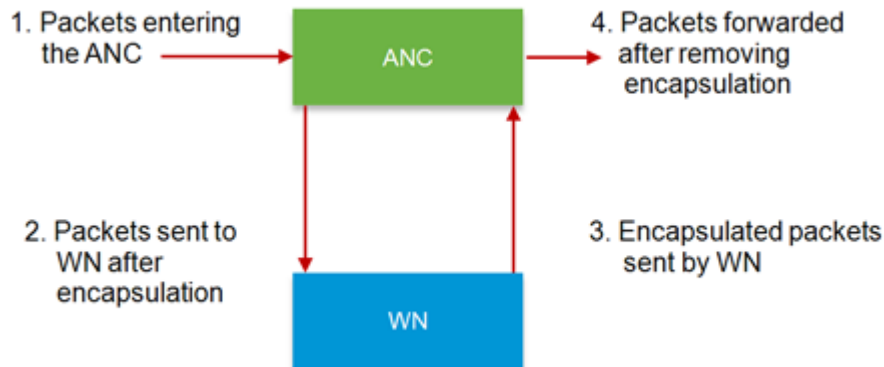
- Debug logbestanden: /local1/errorlog/fdm-errorlog.current (en fdm-errorlog.*)
- Debug logbestanden: /local1/errorlog/fda-errorlog.current (en fda-errorlog.*)

AppNav-pakketvastlegging

Er wordt een nieuwe opdracht voor **pakketvastlegging** geïntroduceerd om het opnemen van gegevenspakketten op interfaces op de Cisco AppNav Controller interfacemodule mogelijk te maken. Deze opdracht kan ook pakketten op andere interfaces opnemen en pakketvastlegging bestanden decoderen. De opdracht **pakketvastlegging** heeft de voorkeur boven de opdrachten **tcpdf** en **traal**, die geen pakketten kunnen opnemen in de Cisco AppNav Controller interfacemodule. Zie de *Cisco Wide Area Application Services Opdracht* voor meer informatie over opdrachtstaxis.

Opmerking: Ofwel pakketvastlegging of debug-opname kan actief zijn, maar niet allebei tegelijkertijd.

Gegevenspakketten die tussen ANC's en WN's worden verzonden, worden ingekapseld, zoals in het volgende schema wordt weergegeven.



Als u pakketten opneemt op punten 1 of 4 in het schema, zijn deze niet ingekapseld. Als u pakketten opneemt op punt 2 of 3, worden deze ingekapseld.

Hier is een voorbeelduitvoer voor een ingekapselde pakketvastlegging:

```
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)
```

Hier is een voorbeelduitvoer voor een niet-gekapselde pakketvastlegging:

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

richtlijnen voor pakketvastlegging:

- Een ACL-pakketvastlegging wordt altijd op inwendig IP-pakket toegepast voor WCCP-GRE en SIA ingekapselde pakketten.
- De pakketvastlegging gebeurt op alle ANC-interfaces als de ANC-interface voor de pakketvastlegging niet is geleverd.

Hier is een voorbeelduitvoer voor een pakketvastlegging op een WAN-interface:


```
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 is een voorbeeld van het decoderen van een pakketvastlegging bestand:

```
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
```

U kunt een src-ip/dst-ip/src-poort/dst-poort instellen voor het filteren van de pakketten:

ANC# pakketvastlegging decode bron-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
```