WAAS - Identificação e solução de problemas do AppNav

Capítulo: Solução de problemas do AppNav

Este artigo descreve como solucionar problemas de uma implantação do AppNav.

Co

Art
En
trá
So
Oti
Tro
Tro
Tro
Tro
Tro
Tro
Tro
Tro
So
Tro
Tro
Tro
So
So
So
So
Tro

Contents

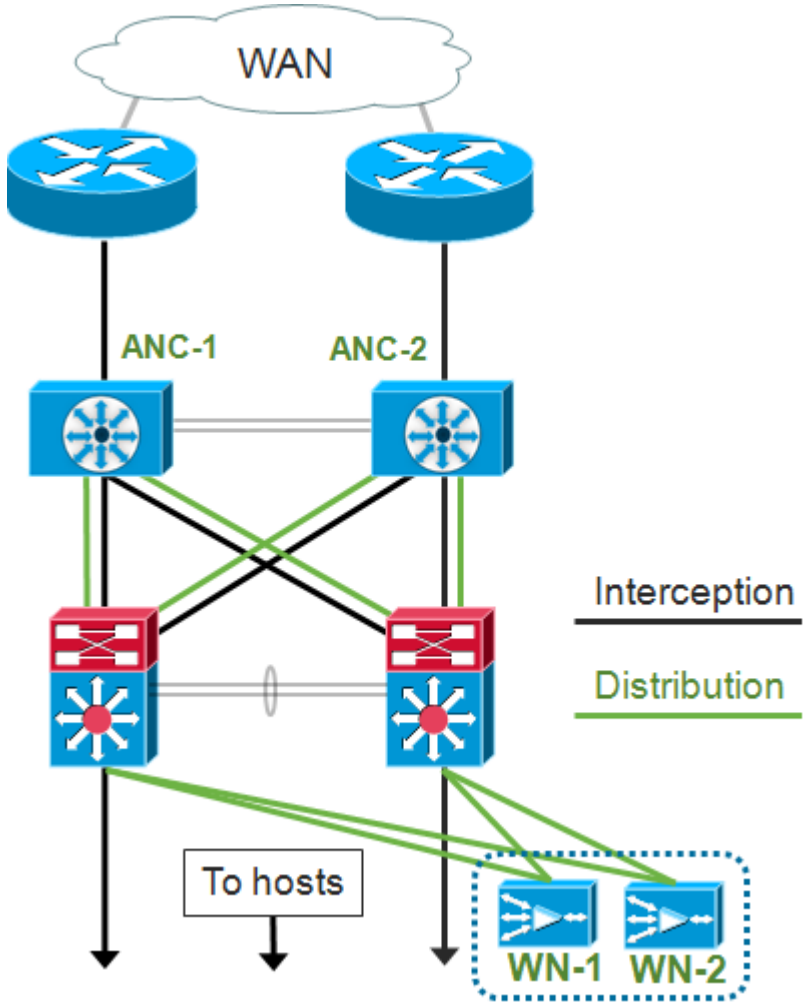
Solução de problemas do AppNav

O Cisco WAAS AppNav simplifica a integração de rede da otimização de WAN e reduz bastante a dependência do switch ou roteador de interceptação usando os controladores AppNav (ANCs) para distribuir o tráfego entre os nós WAAS (WNs) para otimização usando um mecanismo de classe e política avançado. Você pode usar os nós WAAS (WNs) para otimizar o tráfego com base em sites e/ou aplicativos. Este artigo descreve como solucionar problemas do AppNav.

NOTE: O recurso AppNav foi apresentado no WAAS versão 5.0.1. Esta seção não se aplica a versões anteriores do WAAS.

Interceptação no caminho (em linha)

No modo em linha, os ANCs são posicionados no caminho do tráfego de rede, onde interceptam pacotes e os distribuem aos WANs.



A configuração de interface para uma implantação em linha atribui as funções de interceptação e distribuição a interfaces separadas no Módulo de Interface do Controlador Cisco AppNav. Uma interface de grupo de bridge é necessária para interceptação e consiste em duas ou mais interfaces físicas ou de canal de porta ou uma de cada uma. A interface do grupo de bridge não apresenta falha no cabeamento; ou seja, ele falha e o tráfego não é ligado mecanicamente após uma falha ou perda de energia do dispositivo. O AppNav usa clustering para fornecer alta

disponibilidade se o AppNav Controller Interface Module, o caminho do link ou a conectividade com o AppNav Controller Interface Module forem perdidos ou se houver uma falha de energia.

Note: As interfaces de bridge não bloqueiam os pacotes da unidade de dados do protocolo de bridge (BPDU) e, no caso de interfaces redundantes que criam loops, uma das interfaces é bloqueada pelo Spanning Tree Protocol.

A solução de problemas de interceptação em linha consiste nas seguintes etapas:

- Verifique a colocação em linha correta do ANC, verificando o projeto da rede. Se necessário, use ferramentas básicas como ping e traceroute, ou ferramentas ou aplicativos da Camada 7 para confirmar se o caminho do tráfego de rede está conforme o esperado. Verifique o cabeamento físico do ANC.
- Verifique se o ANC está definido para o modo de interceptação em linha.
- Verifique se a interface do grupo de pontes está configurada corretamente.

As duas últimas etapas podem ser executadas no Central Manager ou na linha de comando, embora o Central Manager seja o método preferido e seja descrito primeiro.

No Central Manager, escolha **Devices >** *AppNavController* e escolha **Configure > Interception > Interception Configuration**. Verifique se Interception Method (Método de interceptação) está definido como Inline (Em linha).

Na mesma janela, verifique se uma interface de bridge está configurada. Se uma interface de bridge for necessária, clique em **Create Bridge** para criá-la. Você pode atribuir até duas interfaces membro ao grupo de bridge. Você pode usar a Calculadora de VLAN para definir as entradas de VLAN com base em operações de inclusão ou exclusão. Observe que a interface da bridge não recebe um endereço IP.

Use o painel Alarme ou o comando exec **show alarm** para verificar se algum alarme relacionado à bridge está ativado no dispositivo. Um alarme bridge_down indica que uma ou mais interfaces membro na bridge estão inoperantes.

Na CLI, siga estas etapas para configurar a operação em linha:

1. Defina o método de interceptação como inline:

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

2. Crie a interface bridge-group:

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

3. (Opcional) Especifique a lista de VLANs a interceptar, se necessário:

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

4. Adicione duas interfaces lógicas/físicas à interface do grupo de pontes:

```
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
```

Você pode usar o comando exec **show bridge** para verificar o status operacional da interface bridge e ver as estatísticas da bridge.

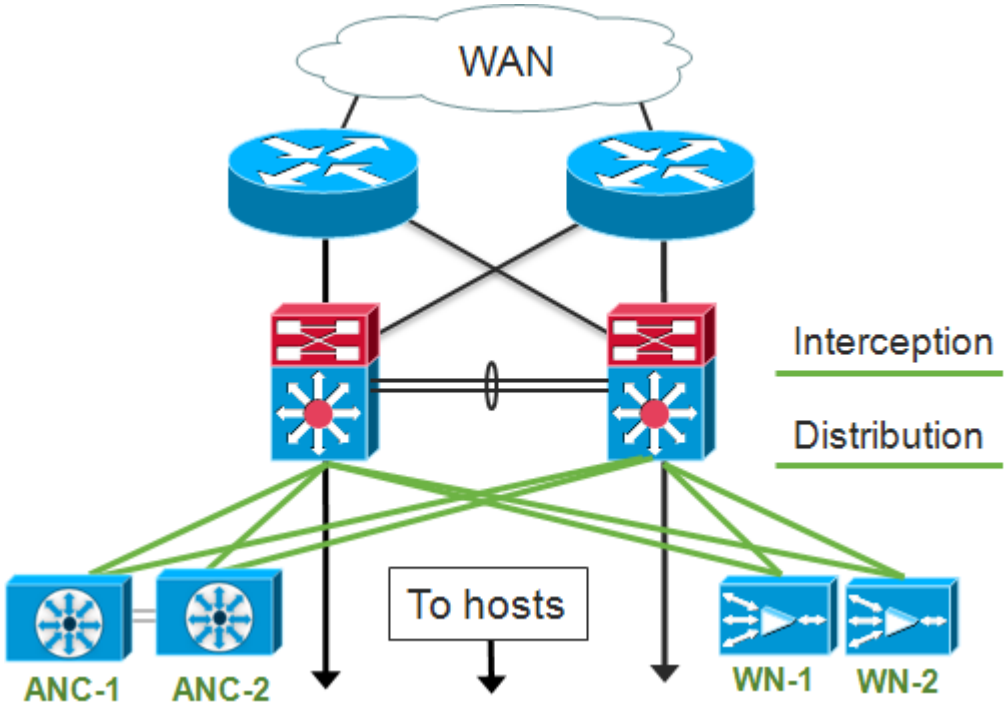
```
wave# show bridge 1
lsp: Link State Propagation
flow sync: AppNav Controller is in the process of flow sync
Member Interfaces:
 GigabitEthernet 1/0
 GigabitEthernet 1/1
Link state propagation: Enabled
VLAN interception:
 intercept vlan-id all                                                    <<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

No exemplo acima, a interface Gig 1/0 está inativa e a interface Gig 1/1 também está inativa devido à propagação do estado do link (LSP). Você também pode ver Down (sincronização de fluxo), o que significa que o ANC está unindo um cluster e sincronizando informações de fluxo com outros ANCs no cluster. Mantém o caminho de interceptação (interface de bridge) fechado por cerca de dois minutos até que todos os ANCs sejam sincronizados para que os fluxos existentes possam ser distribuídos corretamente.

A parte inferior da saída mostra estatísticas de tráfego para as interfaces de membro.

Interceptação fora do caminho (WCCP)

No modo WCCP, os roteadores WCCP são posicionados no caminho do tráfego de rede onde interceptam pacotes e os redirecionam para ANCs, que estão localizados fora do caminho. Como o AppNav lida com o processamento de interceptação, a distribuição inteligente de fluxo e a consideração de carga entre os aceleradores WAAS, a configuração do WCCP nos roteadores é significativamente simplificada.



Na configuração da interface para uma implantação fora do caminho, as funções de interceptação e distribuição podem compartilhar as mesmas interfaces no Cisco AppNav Controller Interface Module, mas isso não é necessário.

A solução de problemas de interceptação fora do caminho consiste nas seguintes etapas:

- Verifique o posicionamento correto dos roteadores WCCP para garantir que eles estejam no caminho do tráfego que vai de e para os hosts otimizados. Você pode usar os comandos **show run** ou **show wccp** para verificar se esses são os mesmos roteadores configurados para WCCP. Se necessário, use ferramentas básicas como ping e traceroute, ou ferramentas ou aplicativos da Camada 7 para confirmar se todo o tráfego que precisa de otimização passa pelos roteadores WCCP.
- Verifique a configuração do WCCP nos WAAS ANCs, usando o Central Manager (preferencial) ou o CLI.
- Verifique a configuração do WCCP nos roteadores de redirecionamento, usando a CLI do roteador.

Para verificar a configuração do WCCP nos ANCs, no Central Manager, escolha **Devices >** *AppNavController* e escolha **Configure > Interception > Interception Configuration**.

- Verifique se o Método de interceptação está definido como WCCP.
- Verifique se a caixa de seleção Ativar serviço WCCP está marcada.
- Verifique se a caixa de seleção Usar gateway padrão como roteador WCCP está marcada ou se os endereços IP do roteador WCCP estão listados no campo Roteador WCCP.
- Verifique se as outras configurações, como a máscara de balanceamento de carga e o método de redirecionamento, estão configuradas corretamente para sua implantação.

Verifique se há alarmes relacionados ao WCCP nos ANCs que fazem parte do farm do WCCP do roteador. No Central Manager, clique no painel Alarmes na parte inferior da tela ou use o comando **show alarm** em cada dispositivo para exibir alarmes. Corrija quaisquer condições de alarme, alterando a configuração no ANC ou roteador, conforme necessário.

Na CLI, siga estas etapas para configurar a operação do WCCP:

1. Defina o método de interceptação como wccp.

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

2. Configure a lista de roteadores WCCP, que contém os endereços IP dos roteadores que participam do farm do WCCP.

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

3. Configure a ID do serviço WCCP. Uma única ID de serviço é preferencial para o AppNav, embora duas IDs de serviço sejam suportadas.

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

4. Associe a lista de roteadores configurada ao serviço WCCP.

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

5. Configure o método de atribuição do WCCP (somente o método de máscara é suportado em um ANC). Se você não especificar as opções dst-ip-mask ou src-ip-mask, a máscara IP de origem padrão será definida como f e a máscara IP de destino será definida como 0.

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

6. Configure o método de redirecionamento WCCP (os métodos de saída e retorno são definidos automaticamente para corresponder ao método de redirecionamento e não são configuráveis para um ANC). Você pode escolher L2 (o padrão) ou GRE. L2 exige que o ANC tenha uma conexão de Camada 2 com o roteador e que o roteador também esteja configurado para o redirecionamento de Camada 2.

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

7. Ative o serviço WCCP.

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

Verifique a interceptação WCCP em cada ANC usando o comando **show running-config**. Os dois exemplos abaixo mostram a saída de configuração atual para redirecionamento L2 e redirecionamento GRE.

Show running-config wccp (para redirecionamento L2):

```
wave# sh run wccp
wccp router-list 1 10.10.10.21 10.10.10.22
wccp tcp-promiscuous service-pair 61
  router-list-num 1
```

```
  enable                                        <<< L2 redirect is default so is not shown in
running config
  exit
```

Show running-config wccp (para GRE):

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

Verifique o status do WCCP em cada ANC usando o comando **show wccp status**.

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

Verifique os roteadores que responderam às mensagens de manutenção de atividade no farm do WCCP usando o comando **show wccp routers**.

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

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

Verifique a visualização de cada ANCs dos outros ANCs no farm do WCCP e dos roteadores alcançáveis por cada um deles usando o comando **show wccp clients**.

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

       IP address = 10.10.10.32   Lead WAE = YES  Weight = 0    <<< YES indicates ANC is serving
as the lead
```

```
       Routers seeing this Wide Area Engine(2)
               192.168.1.1                                    <<< List of routers seeing this
ANC
               192.168.1.2
```

Verifique se os pacotes estão sendo recebidos por cada ANC dos roteadores no farm usando o comando **show statistics wccp**. As estatísticas do tráfego recebido de, passado e enviado a cada roteador são mostradas. As estatísticas cumulativas de todos os roteadores do farm são mostradas na parte inferior. Um comando similar é **show wccp statistics**. Observe que "OE" se refere aos dispositivos ANC aqui.

```
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
```

Configurando e verificando a interceptação WCCP no roteador

Para configurar a interceptação WCCP em cada roteador no farm do WCCP, siga estas etapas.

1. Configure o serviço WCCP no roteador usando o comando do roteador **ip wccp**.

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

2. Configure a interceptação WCCP nas interfaces LAN e WAN do roteador. Você pode configurar a mesma ID de serviço em ambas as interfaces se estiver usando uma única ID de serviço nos ANCs.

```
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. (Opcional) Configure uma interface de túnel se estiver usando saída GRE genérica (somente se você escolher GRE para o método de redirecionamento do WCCP ANC).

```
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
```

Verifique a configuração do WCCP em cada roteador no farm usando o comando **show wccp**.

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

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

       Value SrcAddr    DstAddr    SrcPort DstPort
       ----- -------    -------    ------- -------
       0000: 0x00000000 0x00000000 0x0000  0x0000      <<< Mask assignments
       0001: 0x00000001 0x00000000 0x0000  0x0000
       0002: 0x00000002 0x00000000 0x0000  0x0000
       0003: 0x00000003 0x00000000 0x0000  0x0000
       0004: 0x00000004 0x00000000 0x0000  0x0000
       0005: 0x00000005 0x00000000 0x0000  0x0000
       0006: 0x00000006 0x00000000 0x0000  0x0000
       0007: 0x00000007 0x00000000 0x0000  0x0000
```

```
0008: 0x00000008 0x00000000 0x0000  0x0000
0009: 0x00000009 0x00000000 0x0000  0x0000
0010: 0x0000000A 0x00000000 0x0000  0x0000
0011: 0x0000000B 0x00000000 0x0000  0x0000
0012: 0x0000000C 0x00000000 0x0000  0x0000
0013: 0x0000000D 0x00000000 0x0000  0x0000
0014: 0x0000000E 0x00000000 0x0000  0x0000
0015: 0x0000000F 0x00000000 0x0000  0x0000
```

Additional Information

Para obter informações adicionais, consulte estes documentos:

- Integração de rede WCCP com Cisco Catalyst 6500: Recomendações de melhores práticas para implantações bem-sucedidas
- Redirecionamento do protocolo de comunicação de cache de web dos serviços de aplicativos de longa distância da Cisco: Suporte à plataforma de roteador Cisco
- Configurando recursos avançados do WCCP em roteadores, a partir do *Guia de Configuração do Cisco Wide Area Application Services*
- Configurando o WCCP em WAEs, no *Guia de Configuração do Cisco Wide Area Application Services*

Solução de problemas de conectividade de rede

Ao solucionar problemas de WAAS, pode ser útil determinar como a rede está se comportando com o WAAS desabilitado. Isso é útil quando o tráfego não só não está sendo otimizado, como também não consegue sobreviver. Nesses casos, pode ser que o problema não esteja relacionado ao WAAS. Mesmo nos casos em que o tráfego está passando, essa técnica pode ajudar a determinar quais dispositivos WAAS exigem solução de problemas.

Antes de testar a conectividade da camada 3, verifique se o AppNav Controller Interface Module está conectado às portas corretas do switch. Se o switch conectado suportar e tiver o Cisco Discovery Protocol (CDP) ativado, execute o comando **show cdp neighbors detail** para verificar a conectividade adequada ao switch de rede.

Desabilitar WAAS pode não ser aplicável em todos os casos. Se algum tráfego estiver sendo otimizado e algum não estiver, pode ser inaceitável desativar o WAAS, interrompendo assim o tráfego que está sendo otimizado com sucesso. Nesse caso, a ACL de interceptação ou a política do AppNav podem ser usadas para passar pelo tipo específico de tráfego que está tendo problemas. Para obter detalhes, consulte a seção Passando por tráfego específico.

Para desabilitar o WAAS, diferentes etapas são executadas no modo em linha do que no modo fora do caminho:

- O modo em linha exige colocar a ponte de interceptação no estado de passagem. Para obter detalhes, consulte a seção Desativando um ANC em linha.
- O modo Off-Path requer a desativação do protocolo WCCP. Para obter detalhes, consulte a seção Desativando um ANC fora do caminho.

Em ambientes AppNav, apenas os ANCs precisam ser desativados. Os WANs não precisam ser desativados, pois não participam da interceptação.

Depois que o WAAS for desabilitado, verifique a conectividade de rede usando métodos padrão.

- Verifique a conectividade da Camada 3 usando ferramentas como ping e traceroute.
- Verificar o comportamento do aplicativo para determinar a conectividade da camada superior
- Se a rede estiver enfrentando os mesmos problemas de conectividade que estava com o WAAS ativado, o problema provavelmente não está relacionado ao WAAS.
- Se a rede estiver funcionando bem com o WAAS desabilitado, mas tiver problemas de conexão com o WAAS habilitado, provavelmente há um ou mais dispositivos WAAS que exigem atenção. A próxima etapa é isolar o problema para dispositivos WAAS específicos.
- Se a rede tem conectividade com e sem WAAS habilitado, mas não há otimização, provavelmente há um ou mais dispositivos WAAS que exigem atenção. A próxima etapa é isolar o problema para dispositivos WAAS específicos.

Para verificar o comportamento da rede com WAAS habilitado, siga estas etapas:

1. Reative a funcionalidade WAAS nos ANCs WAAS e, se aplicável, nos roteadores WCCP.

2. Se você tiver determinado que há um problema relacionado ao WAAS, habilite cada cluster do AppNav e/ou ANC individualmente para isolá-lo como uma causa potencial do problema observado.

3. À medida que cada ANC é ativado, execute os mesmos testes básicos de conectividade de rede que nas etapas anteriores e observe se esse ANC específico parece estar funcionando corretamente. Não se preocupe com os NMP individuais nesta fase. O objetivo neste estágio é determinar quais clusters e quais ANCs específicos estão experimentando o comportamento desejado ou indesejado.

4. À medida que cada ANC é ativado e testado, desative-o novamente para que o próximo possa ser ativado. A habilitação e o teste de cada ANC, por sua vez, permitem determinar quais requerem mais solução de problemas.

Essa técnica de identificação e solução de problemas é mais aplicável em situações em que a configuração do WAAS parece não só não ser otimizada, mas também estar causando problemas com a conectividade de rede normal.

Passando por tráfego específico

Você pode passar pelo tráfego específico usando uma ACL de interceptação ou configurando a política do AppNav para passar.

- Crie uma ACL que negue a passagem do tráfego específico e permita todo o resto. Neste exemplo, queremos passar pelo tráfego HTTP (a porta 80 mais antiga). Defina a lista de acesso de interceptação ANC para a ACL definida. As conexões destinadas à porta 80 são passadas. Você pode usar o comando **show statistics pass-through type appnav** para verificar se a passagem está acontecendo verificando se os contadores de ACL de interceptação PT estão aumentando.

```
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
```

- Configure a política ANC para passar pelo tráfego correspondente a classes específicas.

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

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

Desabilitando um ANC em linha

Há várias maneiras de desativar um ANC em linha colocando-o no estado de passagem:

- Defina a lista de VLANs da ponte de interceptação como nenhuma. No Central Manager, escolha um dispositivo ANC e escolha **Configurar > Interceptação > Configuração de interceptação**. Selecione a interface da ponte e clique no ícone **Editar** barra de tarefas. Defina o campo VLANs como o valor "none".
- Desative o contexto de serviço que contém o ANC. No Central Manager, escolha um cluster, clique na guia AppNav Controllers, selecione um ANC e clique no ícone da barra de tarefas **Desativar**.
- Aplique uma ACL de interceptação com critérios "deny ALL" (negar TODAS). Esse método é preferido. (Os dois primeiros métodos interrompem as conexões otimizadas existentes.) Defina uma ACL com os critérios deny ALL (negar TODAS). No Central Manager, escolha um dispositivo ANC, escolha **Configure > Interception > Interception Access List** e escolha a lista de acesso deny ALL na lista suspensa AppNav Controller Interception Access List.

Para desativar a interceptação com uma ACL da CLI, use os seguintes comandos:

```
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
```

Colocando um ANC em estado de passagem:

- Desativa a interceptação do WAAS, não as interfaces.
- Desativa toda a otimização do WAAS.
- Faz com que todo o tráfego passe sem ser afetado.

Desabilitando um ANC fora do caminho

Para desabilitar um ANC que esteja sendo executado no modo fora do caminho, desabilite o protocolo WCCP para o ANC. Você pode fazer essa ação no ANC ou no roteador de redirecionamento ou em ambos. No ANC, você pode desabilitar ou excluir os serviços do WCCP ou pode remover o método de interceptação ou alterá-lo do WCCP para outro método.

Para desabilitar a interceptação WCCP, no Central Manager, escolha um dispositivo ANC e

escolha **Configurar > Interceptação > Configuração de interceptação**. Desmarque a caixa de seleção Ativar serviço WCCP ou clique no ícone da barra de tarefas Remover configurações para remover completamente as configurações de interceptação WCCP (elas serão perdidas).

Para desabilitar a interceptação WCCP da CLI, use os seguintes comandos:

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

Em alguns casos, pode haver vários ANCs recebendo tráfego redirecionado do mesmo roteador. Por conveniência, você pode optar por desabilitar o WCCP no roteador, em vez dos ANCs. A vantagem é que você pode remover vários ANCs de um farm de WCCP em uma única etapa. A desvantagem é que você não pode fazer isso no WAAS Central Manager.

Para desativar o WCCP no roteador, use a seguinte sintaxe:

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

Para reativar o WCCP no roteador, use a seguinte sintaxe:

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

Em cada roteador WCCP, verifique se os ANCs escolhidos para desabilitar não estão sendo exibidos como clientes WCCP. A saída a seguir é exibida quando os serviços WCCP foram excluídos no roteador.

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

Solução de problemas do Cluster do AppNav

Para solucionar problemas de um Cluster do AppNav, você pode usar as seguintes ferramentas:

- Alarmes do AppNav
- Monitoramento do Central Manager
- Comandos CLI do AppNav para monitorar o status do cluster e do dispositivo
- Comandos CLI do AppNav para monitorar estatísticas de distribuição do fluxo
- Rastreamento de conexão
- Registro de depuração do AppNav

Alarmes do AppNav

O Cluster Membership Manager (CMM) eleva os seguintes alarmes devido a condições de erro:

- Cluster degradado (crítico) — visibilidade parcial entre ANCs. A ANC passará por novas conexões.
- Falha na convergência (Crítica)—O ANC não conseguiu convergir em uma visualização estável de ANCs e WANs. A ANC passará por novas conexões.

- Falha na junção ANC (Crítica)—A ANC não conseguiu aderir a um cluster existente devido à possível degradação do cluster com a ANC.
- ANC Mixed Farm (Secundário)—As ANCs no cluster estão executando versões diferentes, mas compatíveis, do protocolo de cluster.
- ANC inalcançável (principal)—Um ANC configurado está inalcançável.
- WN Inalcançável (Major)—Um WAN configurado está inalcançável. Esta WAN não é usada para redirecionamento de tráfego.
- WN excluído (principal)—Um WAN configurado pode ser alcançado, mas excluído porque um ou mais ANCs não podem vê-lo. Esta WAN não é usada para redirecionamento de tráfego (novas conexões).

Você pode ver alarmes no painel Alarmes do Central Manager ou usando o comando EXEC **show alarms** em um dispositivo.

Note: O CMM é um componente interno do AppNav que gerencia o agrupamento de ANCs e WANs em um cluster do AppNav associado a um contexto de serviço.

Monitoramento do Central Manager

Você pode usar o Central Manager para verificar, monitorar e solucionar problemas de clusters do AppNav. O Central Manager tem uma visão global de todos os dispositivos WAAS registrados em sua rede e pode ajudá-lo a localizar rapidamente a maioria dos problemas do AppNav.

No menu Central Manager, escolha **AppNav Clusters >** *nome do cluster*. A janela inicial do cluster exibe a topologia do cluster (incluindo roteadores WCCP e gateway), o status geral do cluster, o status do dispositivo, o status do grupo de dispositivos e o status do link.

Primeiro, verifique se o status geral do cluster está operacional.

Observe que os ícones ANC e WN mostrados neste diagrama têm o mesmo nome de dispositivo porque residem no mesmo dispositivo. Em um ANC que também otimiza o tráfego como um WAN, essas duas funções são mostradas como ícones separados no diagrama de topologia.

Um indicador de aviso de triângulo laranja é mostrado em qualquer dispositivo para o qual o Central Manager pode não ter informações atuais porque o dispositivo não respondeu nos últimos 30 segundos (o dispositivo pode estar off-line ou inacessível).

Você pode obter uma visualização detalhada do status de 360 graus de qualquer dispositivo ANC ou WAN passando o cursor sobre o ícone do dispositivo. A primeira guia exibe alarmes no dispositivo. Você deve resolver todos os alarmes que estão inibindo a operação adequada do cluster.

Clique na guia Interceptação para verificar o método de interceptação do dispositivo em cada ANC.

Se a interceptação estiver inativa, o status será exibido da seguinte forma:

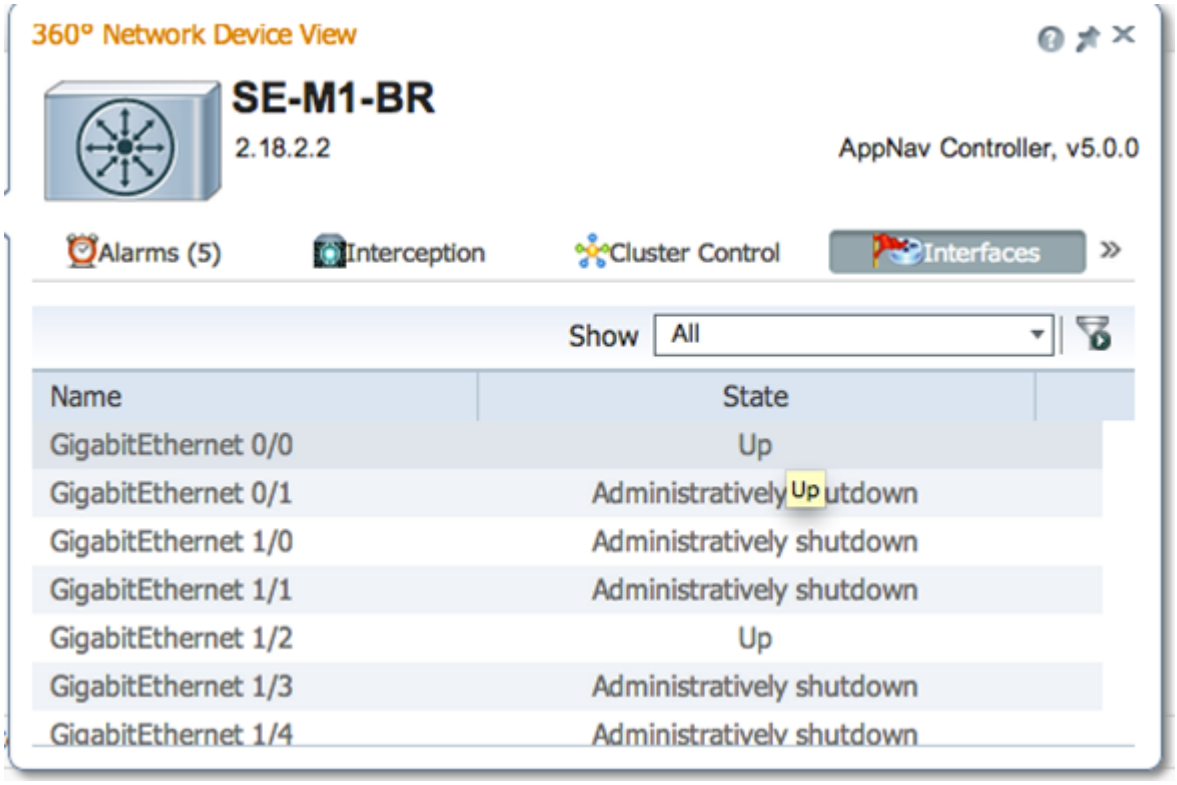
Clique na guia Controle de cluster para ver o endereço IP e o status de cada dispositivo no cluster que este ANC pode ver. Cada ANC no cluster deve ter a mesma lista de dispositivos. Caso contrário, indica um problema de configuração ou de rede.

Se todos os ANCs não puderem se ver, o cluster não estará operacional e todo o tráfego será transmitido devido à incapacidade do cluster de sincronizar fluxos.

Se todos os ANCs estiverem conectados, mas tiverem visualizações diferentes dos WANs, o cluster estará em um estado degradado. O tráfego ainda é distribuído, mas apenas para os WANs que são vistos por todos os ANCs.

Quaisquer WANs não vistas por todos os ANCs são excluídas.

Clique na guia Interfaces (Interfaces) para verificar o estado das interfaces físicas e lógicas no ANC.



Examine a visualização de 360 graus em cada WAN no cluster e verifique o status verde de todos os aceleradores na guia Otimização. Um status amarelo para um acelerador significa que o acelerador está em execução, mas não pode atender a novas conexões, por exemplo, porque ele está sobrecarregado ou porque sua licença foi removida. Um status vermelho indica que o acelerador não está em execução. Se algum acelerador for amarelo ou vermelho, você deverá identificar e solucionar separadamente os problemas desses aceleradores. Se a licença Enterprise estiver ausente, a descrição lerá Licença do sistema foi revogada. Instale a licença da empresa na página **Admin > Histórico > Gerenciamento de licenças**.

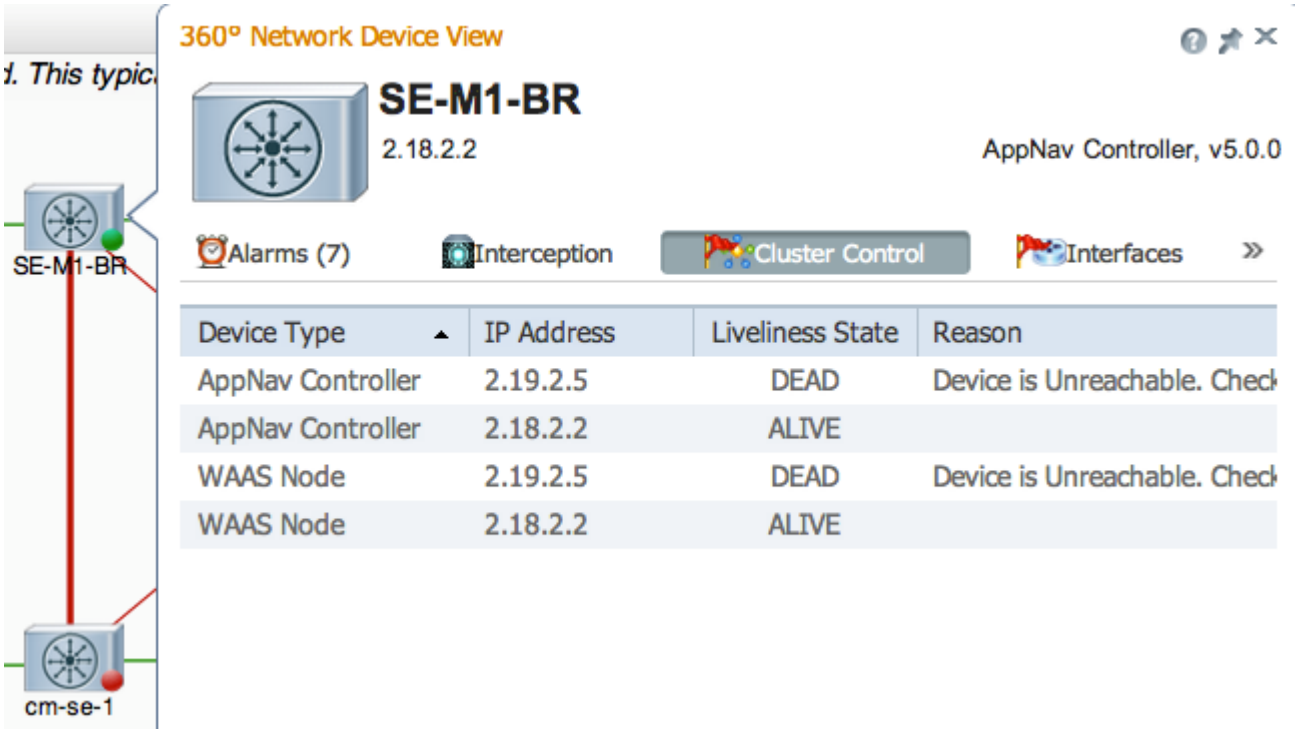
Um cluster dividido resulta de problemas de conectividade entre ANCs no cluster. Se o Central Manager puder se comunicar com todos os ANCs, ele poderá detectar um cluster dividido; no entanto, se não puder se comunicar com alguns ANCs, ele não poderá detectar a divisão. O

alarme "Management status is off-line" será acionado se o Central Manager perder a conectividade com qualquer dispositivo e o dispositivo for exibido como off-line no Central Manager.

Émelhor separar as interfaces de gerenciamento das interfaces de dados para manter a conectividade de gerenciamento mesmo que um enlace de dados esteja inoperante.

Em um cluster dividido, cada subcluster de ANCs distribui de forma independente fluxos para os WNGs que ele pode ver, mas como os fluxos entre os subclusters não são coordenados, ele pode causar conexões de redefinição e o desempenho geral do cluster é degradado.

Verifique a guia Cluster Control de cada ANC para ver se um ou mais ANCs estão inacessíveis. O alarme "Service controller is unreachable" é acionado se dois ANCs que uma vez poderiam se comunicar entre si perderem a conectividade entre si, mas essa situação não é a única causa de um cluster dividido, portanto, é melhor verificar a guia Cluster Control de cada ANC.



Se um ANC tiver uma luz de status cinza, ele pode estar desativado. Verifique se todos os ANCs estão ativados clicando na guia AppNav Controllers abaixo do diagrama de topologia. Se um ANC não estiver ativado, o status Habilitado é Não. Você pode clicar no ícone da barra de tarefas **Habilitar** para habilitar um ANC.

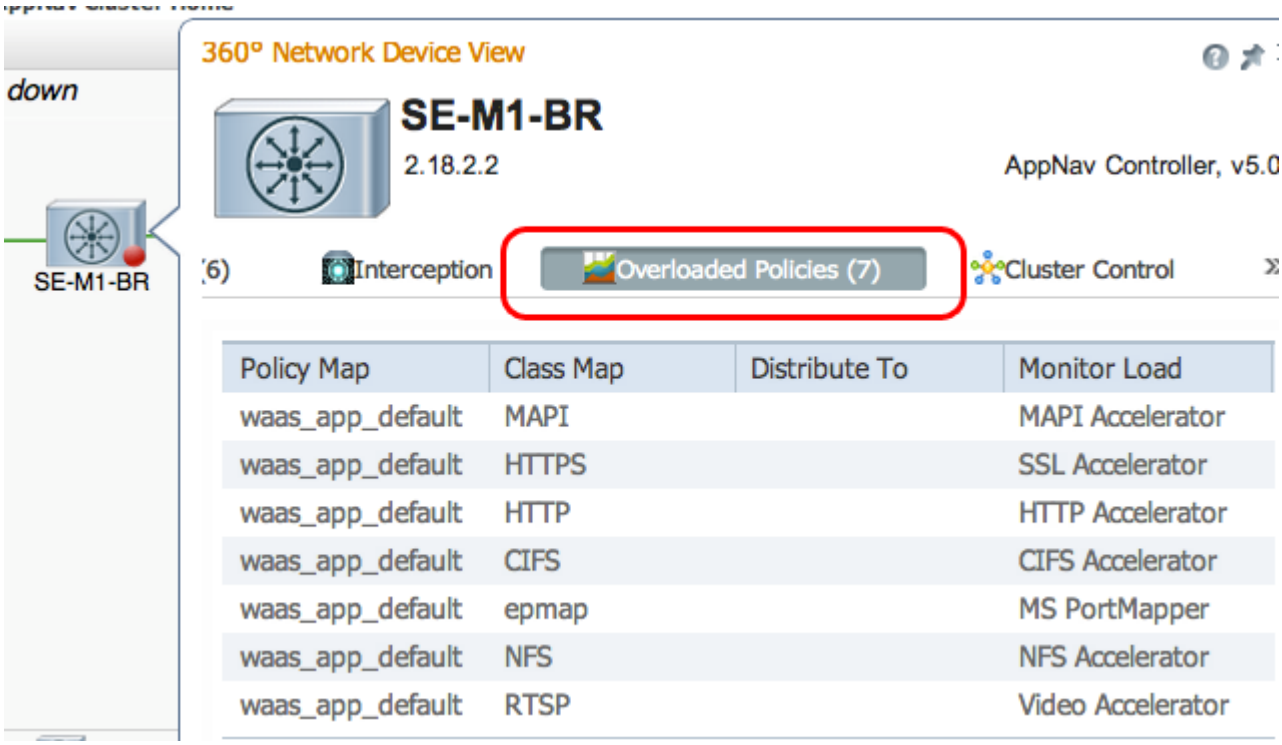
Verifique a política do AppNav em cada ANC que tenha qualquer sinal diferente de uma luz de status verde. Se você passar o cursor sobre a luz de status em um dispositivo, uma dica de ferramenta informará o status ou o problema, se for detectado.

Para verificar as políticas definidas, no menu Central Manager, escolha **Configure > AppNav Policies** e clique no botão **Manage**.

Geralmente, deve haver uma única política atribuída a todos os ANCs no cluster. A política padrão é denominada appnav_default. Selecione o botão de opção ao lado de uma diretiva e clique no ícone **Editar** barra de tarefas. O painel Política do AppNav mostra os ANCs aos quais a política selecionada é aplicada. Se todos os ANCs não forem mostrados com uma marca de seleção, clique na caixa de seleção ao lado de cada ANC desmarcado para atribuir a diretiva a ele. Clique em **OK** para salvar as alterações.

Depois de verificar as atribuições de política, você pode verificar as regras de política na página Políticas do AppNav que permanece exibida. Selecione qualquer regra de política e clique no ícone **Editar** barra de tarefas para alterar sua definição.

Um ANC pode ter uma luz de status amarela ou vermelha se uma ou mais políticas estiverem sobrecarregadas. Verifique a guia Políticas sobrecarregadas da exibição de dispositivo de 360 graus para ver uma lista de políticas monitoradas sobrecarregadas.



Se um ANC estiver se unindo ao cluster, ele será exibido com uma luz de status amarela e status de junção.

A guia Intercepção da exibição do dispositivo de 360 graus mostra que o caminho de interceptação está inoperante devido ao estado de junção. A interceptação é mantida pressionada até que o ANC sincronizou suas tabelas de fluxo com os outros ANCs e esteja pronto para aceitar tráfego. Esse processo geralmente leva no máximo dois minutos.

Se você remover um ANC de um cluster, ele ainda será exibido por alguns minutos no diagrama de topologia e como ativo na guia Controle de cluster, até que todos os ANCs concordem com a nova topologia de cluster. Não recebe nenhum fluxo novo neste estado.

Comandos CLI do AppNav para monitorar o status do cluster e do dispositivo

Vários comandos CLI são úteis para a solução de problemas em um ANC:

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

Use estes comandos em uma WAN:

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

Você pode usar o comando **show service-insertion service-context** em um ANC para ver o status do contexto de serviço e a visualização estável dos dispositivos no cluster:

```
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
```

Se o campo Device Interception State (Estado de interceptação do dispositivo) acima mostrar Shutdown, isso significa que o CMM desligou a interceptação devido a este ANC não estar pronto para receber fluxos de tráfego. Por exemplo, o ANC ainda pode estar no processo de união e o cluster ainda não sincronizou fluxos.

Os campos de Exibição Estável (acima) listam os endereços IP dos ANCs e WANs vistos por este dispositivo ANC em sua última visualização convergida do cluster. Esta é a exibição usada para operações de distribuição. Os campos Exibição atual listam os dispositivos anunciados por este ANC em suas mensagens de pulsação.

Você pode usar o **comando show service-insertion appnav-controller-group** em um ANC para ver o status de cada ANC no grupo ANC:

```
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
```

Para obter uma lista de possíveis status de ANC e status de associação, consulte o comando **show service-insertion** na *Referência de Comandos do Cisco Wide Area Application Services*.

Você pode usar o **comando show service-insertion service-node** em um ANC para ver o status de um WAN específico no cluster:

```
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
```

Você pode usar o **comando show service-insertion service-node-group** em um ANC para ver o status de um WNG específico no cluster:

```
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
```

O primeiro WAN no exemplo acima tem um status Excluído, o que significa que o WAN é visível para o ANC, mas é excluído do cluster porque um ou mais ANCs não podem vê-lo.

A tabela SNG Availability per AO mostra se cada AO é capaz de atender a novas conexões. Está disponível um AO se pelo menos um WNG tiver um estatuto de NÃ VERDE para o AO.

Você pode usar o comando show service-insertion service-node em um WN para ver o status do WAN:

```
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
```

O estado monitorado de um acelerador é o estado real, mas o estado relatado pode ser diferente porque é o menor estado do sistema ou o estado do acelerador.

Para obter mais informações sobre a otimização de solução de problemas em uma WAN, consulte os artigos Otimização de solução de problemas e Troubleshooting de Aceleração de Aplicativos.

Comandos CLI do AppNav para monitorar estatísticas de distribuição do fluxo

Vários comandos CLI são úteis para solucionar problemas de políticas e distribuição de fluxo em um ANC:

- **show policy-map type appnav** *policymap-name* — Mostra as regras de política e as contagens de ocorrências para cada classe no mapa de políticas.
- **show class-map type appnav** *class-name* — Mostra os critérios de correspondência e as contagens de acertos para cada condição de correspondência no mapa de classes.
- **show policy-sub-class type appnav** *level1-class-name level2-class-name* — Mostra os critérios de correspondência e as contagens de acertos para cada condição de

correspondência em um mapa de classes em um mapa aninhado de políticas do AppNav.

- **show statistics class-map type appnav** *class-name* — Mostra as estatísticas de interceptação e distribuição de tráfego para um mapa de classe.
- **show statistics policy-sub-class type appnav** *level1-class-name level2-class-name* — Mostra as estatísticas de interceptação e distribuição de tráfego para um mapa de classes em um mapa aninhado de políticas do AppNav.
- **show statistics pass-through type appnav** — Mostra as estatísticas de tráfego do AppNav para cada motivo de passagem.
- **show appnav-controller flow-distribution** — Mostra como um fluxo hipotético específico seria classificado e distribuído por um ANC, com base na política definida e nas condições de carga dinâmica. Esse comando pode ser útil para verificar como um determinado fluxo será tratado em um ANC e a que classe ele pertence.

Use estes comandos em uma WAN para solucionar problemas de distribuição de fluxo:

- **show statistics service-insertion service-node** *ip-address* — Mostra estatísticas de aceleradores e tráfego distribuídos para o WN.
- **show statistics service-insertion service-node-group name** *group-name* — Mostra estatísticas para aceleradores e tráfego distribuído para o WNG.

Você pode usar o **comando show statistics class-map type appnav** *class-name* em um ANC para solucionar problemas de distribuição de fluxo, por exemplo, para determinar por que o tráfego pode estar lento para uma classe específica. Esse pode ser um mapa de classe de aplicativo, como HTTP, ou, se todo o tráfego para uma filial parecer lento, pode ser um mapa de classe de afinidade de filial. Aqui está um exemplo para a classe HTTP:

```
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
  ...
```

Os motivos de passagem de WAN na seção Indicated by SN incrementam somente se o descarregamento de passagem estiver configurado em um WAN. Caso contrário, o ANC não sabe que o WAN está passando por uma conexão e não a conta.

Se as conexões: Interceptado pelo contador ANC não está aumentando, há um problema de interceptação. Você pode usar o utilitário WAAS TcpTraceroute para solucionar problemas de posicionamento do ANC na rede, localizar caminhos assimétricos e determinar a política aplicada a uma conexão. Para obter detalhes, consulte a seção Rastreamento de conexão.

Comandos CLI do AppNav para conexões de depuração

Para depurar uma conexão individual ou um conjunto de conexões em um ANC, você pode usar o comando **show statistics appnav-controller connection** para exibir a lista de conexões ativas.

```
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
```

Você pode filtrar a lista especificando as opções de endereço IP e/ou porta do cliente ou servidor e pode mostrar estatísticas detalhadas sobre conexões especificando a palavra-chave **detalhada**.

```
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
...
```

Você pode especificar a opção de resumo para exibir o número de conexões distribuídas e de passagem ativas.

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

Rastreamento de conexão

Para ajudar na solução de problemas de fluxos do AppNav, você pode usar a ferramenta Rastreamento de conexão no Gerenciador central. Esta ferramenta mostra as seguintes informações para uma conexão específica:

- Se a conexão foi passada ou distribuída para um WNG
- Motivo da passagem, se aplicável
- O WNG e o WN para os quais a conexão foi distribuída
- Acelerador monitorado para a conexão
- Mapa de classe aplicado

Para usar a ferramenta Rastreamento de conexão, siga estas etapas:

1. No menu Central Manager, escolha **AppNav Clusters >** *nome do cluster* e escolha **Monitor > Ferramentas > Rastreamento de conexão**.

2. Escolha o ANC, o dispositivo WAAS correspondente e especifique os critérios de correspondência de conexão.

3. Clique em **Rastrear** para exibir conexões correspondentes.

O Traceroute TCP do WAAS é outra ferramenta não específica do AppNav que pode ajudá-lo a solucionar problemas de rede e conexão, incluindo caminhos assimétricos. Você pode usá-la para encontrar uma lista de nós WAAS entre o cliente e o servidor e as políticas de otimização configuradas e aplicadas para uma conexão. No Central Manager, você pode escolher qualquer

dispositivo na rede WAAS do qual executar o traceroute. Para usar a ferramenta Traceroute TCP do WAAS Central Manager, siga estas etapas:

1. No menu do WAAS Central Manager, escolha **Monitor > Troubleshoot > WAAS Tcptraceroute**. Como alternativa, você pode escolher um dispositivo primeiro e, em seguida, escolher este item de menu para executar o traceroute a partir desse dispositivo.

2. Na lista suspensa WAAS Node, escolha um dispositivo WAAS do qual executar o traceroute. (Este item não é exibido se você estiver no contexto do dispositivo.)

3. Nos campos IP de destino e Porta de destino, insira o endereço IP e a porta de destino para os quais deseja executar o traceroute

4. Clique em **Executar TCPTraceroute** para exibir os resultados.

Os nós WAAS no caminho rastreado são exibidos na tabela abaixo dos campos. Você também pode executar esse utilitário a partir da CLI com o comando **waas-tcptrace**.

Registro de depuração do AppNav

O seguinte arquivo de log está disponível para solução de problemas com o gerenciador de cluster do AppNav:

- Depurar arquivos de log: /local1/errorlog/cmm-errorlog.current (e cmm-errorlog.*)

Para configurar e ativar o registro de depuração do gerenciador de cluster do AppNav, use os seguintes comandos.

NOTE: O registro de depuração exige muito da CPU e pode gerar uma grande quantidade de saída. Use-o de forma inteligente e moderna em um ambiente de produção.

Você pode ativar o registro detalhado no disco:

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

As opções para depuração do gerenciador de cluster (na versão 5.0.1 e posterior) são as seguintes:

```
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
```

Você pode ativar o registro de depuração para o gerenciador de cluster e, em seguida, exibir o final do registro de erros de depuração da seguinte maneira:

```
WAE# debug cmm all
```

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

Você também pode ativar o registro de depuração para o gerenciador de distribuição de fluxo (FDM) ou o agente de distribuição de fluxo (FDA) com estes comandos:

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

O FDM determina onde distribuir fluxos com base na política e nas condições de carga dinâmicas dos WANs. O FDA coleta informações de carga WAN. Os seguintes arquivos de log estão disponíveis para a solução de problemas de FDM e FDA:

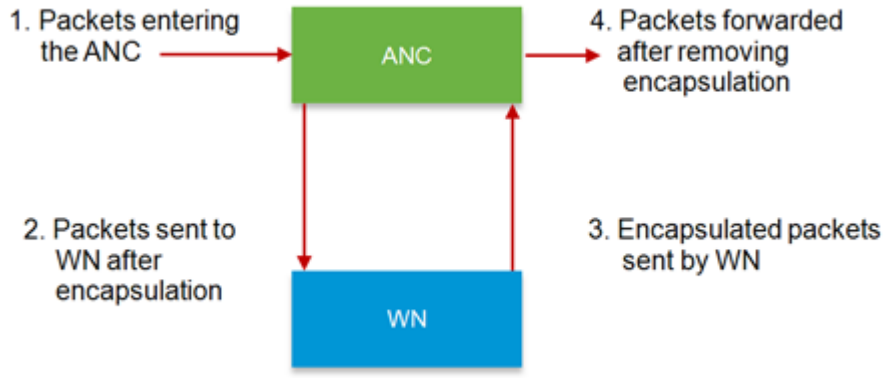
- Depurar arquivos de log: /local1/errorlog/fdm-errorlog.current (e fdm-errorlog.*)
- Depurar arquivos de log: /local1/errorlog/fda-errorlog.current (e fda-errorlog.*)

Captura de pacote do AppNav

Um novo **comando packet-capture** é introduzido para permitir a captura de pacotes de dados em interfaces no Cisco AppNav Controller Interface Module. Esse comando também pode capturar pacotes em outras interfaces e decodificar arquivos de captura de pacotes. O comando **packet-capture** é preferido aos comandos preteridos **tcpdump** e **tethereal**, que não podem capturar pacotes no Cisco AppNav Controller Interface Module. Consulte a *Referência de Comandos do Cisco Wide Area Application Services* para obter detalhes sobre a sintaxe de comandos.

Note: A captura de pacotes ou a captura de depuração podem estar ativas, mas não ambas simultaneamente.

Os pacotes de dados enviados entre ANCs e WANs são encapsulados, como mostrado no diagrama a seguir.



Se você capturar pacotes nos pontos 1 ou 4 do diagrama, eles não serão encapsulados. Se você capturar pacotes nos pontos 2 ou 3, eles serão encapsulados.

Aqui está um exemplo de saída para uma captura de pacote encapsulado:

```
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)
```

Aqui está um exemplo de saída para uma captura de pacote não encapsulada:

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

Diretrizes de captura de pacotes:

- Uma ACL de captura de pacote é sempre aplicada ao pacote IP interno para pacotes encapsulados WCCP-GRE e SIA.
- A captura de pacotes é feita em todas as interfaces ANC se a interface ANC para a captura de pacotes não for fornecida.

Aqui está um exemplo de saída para uma captura de pacote em uma interface WAN:

```
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 ...
```

Aqui está um exemplo de decodificação de um arquivo de captura de pacote:

```
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
```

Você pode especificar uma porta src-ip/dst-ip/src-port/dst para filtrar os pacotes:

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

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