# WAAS - Resolución de problemas de AppNav

## Capítulo: Resolución de problemas de AppNav

En este artículo se describe cómo resolver problemas de una implementación de AppNav.

## Contenido

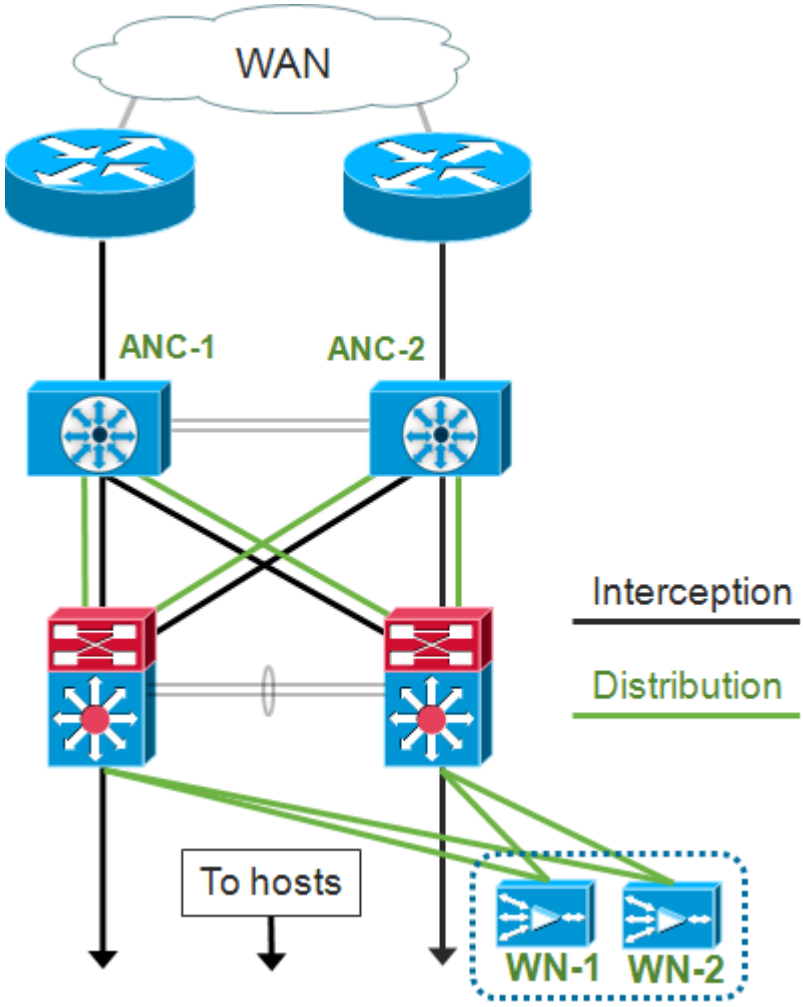
# Solución de problemas de AppNav

Cisco WAAS AppNav simplifica la integración de la red de la optimización de WAN y reduce en gran medida la dependencia del switch o router de interceptación mediante los controladores de AppNav (ANC) para distribuir el tráfico entre los nodos WAAS (WN) con el fin de optimizar mediante un potente mecanismo de políticas y clases. Puede utilizar nodos WAAS (WN) para optimizar el tráfico en función de sitios o aplicaciones. En este artículo se describe cómo resolver problemas de AppNav.

**NOTE:** La función AppNav se introdujo en WAAS versión 5.0.1. Esta sección no se aplica a las versiones anteriores de WAAS.

## Interceptación en ruta (en línea)

En el modo en línea, los ANC se colocan en el trayecto del tráfico de red donde interceptan paquetes y los distribuyen a los WN.




La configuración de la interfaz para una implementación en línea asigna las funciones de intercepción y distribución a interfaces independientes en el módulo de interfaz del controlador Cisco AppNav. Se requiere una interfaz de grupo de puente para la intercepción y consta de dos

o más interfaces físicas o de canal de puerto o una de cada una. La interfaz de grupo de bridges no falla en la capacidad de cableado; es decir, falla al abrir y el tráfico no se puentea mecánicamente después de una falla en el dispositivo o una pérdida de energía. AppNav utiliza la agrupación en clúster para proporcionar alta disponibilidad si el AppNav Controller Interface Module, la trayectoria de link o la conectividad con el AppNav Controller Interface Module se pierde o se produce una falla de alimentación.

**Nota:** Las interfaces de puente no bloquean los paquetes de unidad de datos de protocolo de puente (BPDU) y, en el caso de interfaces redundantes que crean bucles, el protocolo de árbol de extensión bloquea una de las interfaces.

La resolución de problemas de interceptación en línea consta de los siguientes pasos:

- Verifique la ubicación en línea correcta del ANC al verificar el diseño de la red. Si es necesario, utilice herramientas básicas como ping y traceroute, o herramientas o aplicaciones de capa 7 para confirmar que la ruta de tráfico de red es la esperada. Verifique el cableado físico del ANC.
- Verifique que el ANC esté configurado en modo de intercepción en línea.
- Verifique que la interfaz de grupo de bridges esté configurada correctamente.

Los dos últimos pasos se pueden realizar en Central Manager o en la línea de comandos, aunque Central Manager es el método preferido y se describe primero.

En el Administrador central, elija **Devices >** *AppNavController* **y luego elija Configure > Interception > Interception Configuration**. Verifique que el método de intercepción esté establecido en Línea.

En la misma ventana, verifique que se haya configurado una interfaz de puente. Si se necesita una interfaz de puente, haga clic en **Crear puente** para crearlo. Puede asignar hasta dos interfaces miembro al grupo de bridges. Puede utilizar la calculadora VLAN para definir las entradas de VLAN basadas en operaciones de inclusión o exclusión. Tenga en cuenta que a la interfaz de bridge no se le asigna una dirección IP.

Utilice el panel Alarma o el comando **show alarm** exec para verificar si se han producido alarmas relacionadas con el puente en el dispositivo. Una alarma bridge_down indica que una o más interfaces miembro en el bridge están inactivas.

En la CLI, siga estos pasos para configurar el funcionamiento en línea:

1. Establezca el método de intercepción en línea:

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

2. Cree la interfaz de grupo de bridges:

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

3. (Opcional) Especifique la lista de VLAN a interceptar, si es necesario:

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

4. Agregue dos interfaces lógicas/físicas a la interfaz de grupo de bridges:

```
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
```

Puede utilizar el comando **show bridge** exec para verificar el estado operativo de la interfaz de bridge y ver las estadísticas para el bridge.

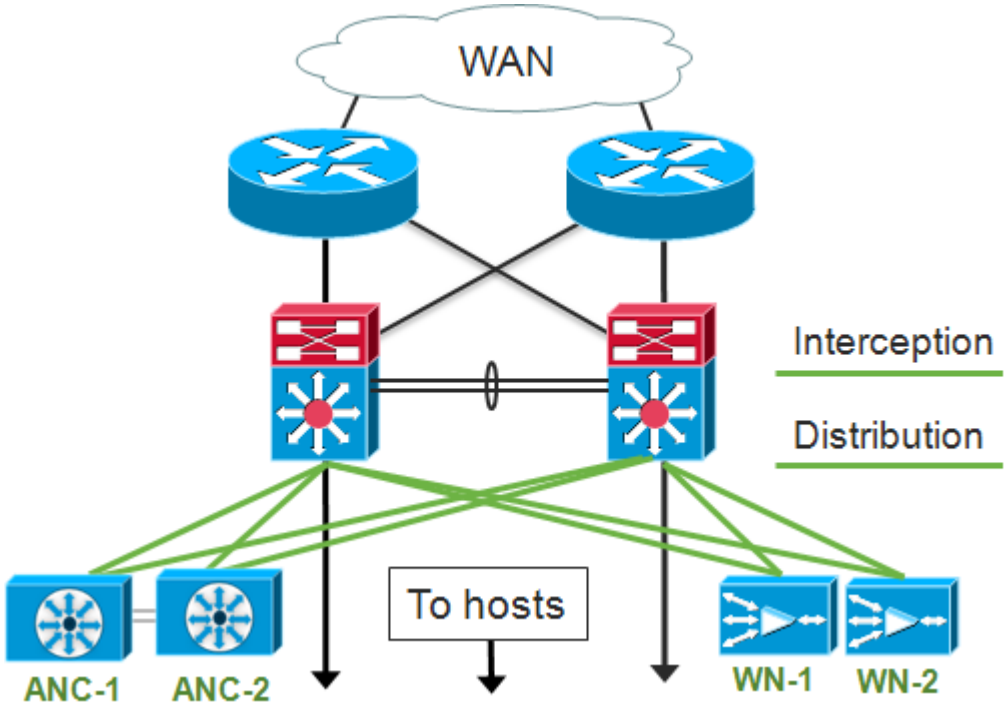
```
wave# show bridge 1
lsp: Link State Propagation
flow sync: AppNav Controller is in the process of flow sync
Member Interfaces:
 GigabitEthernet 1/0
 GigabitEthernet 1/1
Link state propagation: Enabled
VLAN interception:
 intercept vlan-id all                                                    <<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

En el ejemplo anterior, la interfaz Gig 1/0 está inactiva y la interfaz Gig 1/1 también está inactiva debido a la propagación del estado de link (LSP). También puede ver Down(flow sync), lo que significa que el ANC se une a un clúster y sincroniza la información de flujo con otros ANC en el clúster. Mantiene la ruta de intercepción (interfaz de puente) cerrada durante unos dos minutos hasta que todos los ANC estén sincronizados para que los flujos existentes puedan distribuirse correctamente.

La parte inferior del resultado muestra las estadísticas de tráfico para las interfaces miembro.

## Interceptación fuera de ruta (WCCP)

En el modo WCCP, los routers WCCP se colocan en la trayectoria del tráfico de red donde interceptan los paquetes y los redirigen a ANC, que se encuentran fuera de la ruta. Dado que AppNav gestiona el procesamiento de intercepción, la distribución de flujo inteligente y la consideración de carga entre los aceleradores WAAS, la configuración WCCP en los routers se simplifica significativamente.




En la configuración de la interfaz para una implementación fuera de ruta, las funciones de intercepción y distribución pueden compartir las mismas interfaces en el módulo de interfaz del controlador Cisco AppNav, pero no es necesario.

La resolución de problemas de interceptación fuera de ruta consta de los siguientes pasos:

- Verifique la ubicación correcta de los routers WCCP para asegurarse de que estén en la trayectoria del tráfico que va hacia y desde los hosts optimizados. Puede utilizar los comandos **show run** o **show wccp** para verificar que sean los mismos routers configurados para WCCP. Si es necesario, utilice herramientas básicas como ping y traceroute, o herramientas o aplicaciones de capa 7 para confirmar que todo el tráfico que necesita optimización pasa a través de los routers WCCP.
- Verifique la configuración WCCP en los ANC WAAS, utilizando el Administrador central (preferido) o la CLI.
- Verifique la configuración de WCCP en los routers de redireccionamiento, usando la CLI del router.

Para verificar la configuración WCCP en los ANC, en el Administrador Central, elija **Devices >** *AppNavController* **y luego elija Configure > Interception > Interception Configuration.**

- Verifique que el método de intercepción esté configurado en WCCP.
- Verifique que la casilla de verificación Enable WCCP Service esté marcada.
- Verifique que la casilla de verificación Use Default Gateway as WCCP Router esté marcada o que las direcciones IP del router WCCP estén enumeradas en el campo WCCP Router.
- Verifique que los otros ajustes como la máscara de balanceo de carga y el método de redirección estén configurados correctamente para su implementación.

Verifique cualquier alarma relacionada con WCCP en los ANC que forman parte de la granja WCCP del router. En el Administrador central, haga clic en el panel Alarmas en la parte inferior de la pantalla o utilice el comando **show alarm** en cada dispositivo para ver alarmas. Corrija cualquier condición de alarma cambiando la configuración en el ANC o router, según sea necesario.

En la CLI, siga estos pasos para configurar la operación WCCP:

1. Establezca el método de intercepción en wccp.

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

2. Configure la lista de routers WCCP, que contiene las direcciones IP de los routers que participan en la granja WCCP.

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

3. Configure el ID de servicio WCCP. Se prefiere una única ID de servicio para AppNav, aunque se admiten dos ID de servicio.

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

4. Asocie la lista de routers configurada con el servicio WCCP.

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

5. Configure el método de asignación WCCP (sólo se admite el método mask en un ANC). Si no especifica las opciones dst-ip-mask o src-ip-mask, la máscara IP de origen predeterminada se establece en f y la máscara IP de destino se establece en 0.

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

6. Configure el método de redirección WCCP (los métodos de salida y retorno se configuran automáticamente para que coincidan con el método de redirección y no se pueden configurar para un ANC). Puede elegir L2 (el valor predeterminado) o GRE. L2 requiere que el ANC tenga una conexión de Capa 2 con el router y que el router también esté configurado para la redirección de Capa 2.

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

7. Habilite el servicio WCCP.

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

Verifique la intercepción WCCP en cada ANC usando el comando **show running-config**. Los dos ejemplos siguientes muestran el resultado de configuración en ejecución para la redirección L2 y la redirección GRE.

### Show running-config wccp (para 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                                        <<< 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 el estado de WCCP en cada ANC usando el 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 los routers que han respondido a los mensajes de mantenimiento en el bloque WCCP usando el 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 la vista de cada ANC de los otros ANC en el bloque WCCP y los routers a los que cada uno de ellos puede acceder mediante el 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 que los paquetes estén siendo recibidos por cada ANC de los routers en la granja usando el comando **show statistics wccp**. Se muestran las estadísticas del tráfico recibido, pasado y enviado a cada router. Las estadísticas acumulativas para todos los routers de la granja se muestran en la parte inferior. Un comando similar es **show wccp statistics**. Tenga en cuenta que "OE" se refiere a los dispositivos ANC aquí.

```
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
```

## Configuración y Verificación de la Interceptación WCCP en el Router

Para configurar la intercepción WCCP en cada router de la granja WCCP, siga estos pasos.

1. Configure el servicio WCCP en el router mediante el comando **ip wccp** router.

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

2. Configure la intercepción WCCP en las interfaces LAN y WAN del router. Puede configurar el mismo ID de servicio en ambas interfaces si utiliza un único ID de servicio en los ANC.

```
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 una interfaz de túnel si está utilizando una salida GRE genérica (sólo si eligió GRE para el método de redirección WCCP de 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 la configuración WCCP en cada router de la granja usando el 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 obtener más información, consulte estos documentos:

- Integración de red WCCP con Cisco Catalyst 6500: Recomendaciones de prácticas recomendadas para implementaciones satisfactorias
- Redirección del protocolo de comunicación de caché web de servicios de aplicaciones de área extensa de Cisco: Soporte de la plataforma del router de Cisco
- Configuración de Funciones WCCP Avanzadas en Routers, desde la *Guía de Configuración de Cisco Wide Area Application Services*
- Configuración de WCCP en WAEs, desde la *Guía de Configuración de Cisco Wide Area Application Services*

## Resolución de problemas de conectividad de red

Al resolver problemas de WAAS, puede ser útil determinar cómo se comporta la red con WAAS inhabilitado. Esto resulta útil cuando el tráfico no solo no se optimiza, sino que no se consigue acceder a él. En estos casos, puede resultar que el problema no esté relacionado con WAAS. Incluso en los casos en los que el tráfico está atravesando, esta técnica puede ayudar a determinar qué dispositivos WAAS requieren resolución de problemas.

Antes de probar la conectividad de Capa 3, verifique que el AppNav Controller Interface Module esté conectado a los puertos de switch adecuados. Si el switch conectado admite y tiene activado Cisco Discovery Protocol (CDP), ejecute el comando **show cdp neighbors detail** para verificar la conectividad adecuada con el switch de red.

La inhabilitación de WAAS puede no ser aplicable en todos los casos. Si se está optimizando cierto tráfico y algunos no, puede ser inaceptable desactivar WAAS, con lo que se interrumpirá el tráfico que se está optimizando correctamente. En tal caso, la ACL de intercepción o la política AppNav se pueden utilizar para pasar a través del tipo específico de tráfico que está experimentando problemas. Para obtener más información, vea la sección Paso a través de tráfico específico.

Para inhabilitar WAAS, se realizan diferentes pasos para el modo en línea que para el modo fuera de trayectoria:

- El modo en línea requiere colocar el puente de intercepción en el estado de paso a través. Para obtener más información, vea la sección Inhabilitación de un ANC en línea.
- El modo Off-path requiere desactivar el protocolo WCCP. Para obtener detalles, vea la sección Inhabilitación de un ANC Off-Path.

En los entornos de AppNav, sólo los ANC deben desactivarse. No es necesario que los WN estén inhabilitados, ya que no participan en la interceptación.

Una vez que WAAS esté inhabilitado, verifique la conectividad de red mediante métodos estándar.

- Verifique la conectividad de Capa 3 con herramientas como ping y traceroute.
- Comprobar el comportamiento de las aplicaciones para determinar la conectividad de capa superior
- Si la red experimenta los mismos problemas de conectividad que con WAAS habilitado, el problema probablemente no esté relacionado con WAAS.
- Si la red funciona correctamente con WAAS desactivado, pero ha tenido problemas de conexión con WAAS activado, es probable que haya uno o más dispositivos WAAS que requieran atención. El siguiente paso es aislar el problema a dispositivos WAAS específicos.
- Si la red tiene conectividad con y sin WAAS habilitado, pero no hay optimización, probablemente haya uno o más dispositivos WAAS que requieran atención. El siguiente paso es aislar el problema a dispositivos WAAS específicos.

Para comprobar el comportamiento de la red con WAAS habilitado, siga estos pasos:

1. Vuelva a habilitar la funcionalidad WAAS en los ANC WAAS y, si procede, en los routers WCCP.

2. Si ha determinado que hay un problema relacionado con WAAS, habilite cada clúster de AppNav y/o ANC individualmente, para aislarlo como causa potencial del problema observado.

3. Como cada ANC está habilitado, realice las mismas pruebas básicas de conectividad de red que en los pasos anteriores y observe si este ANC específico parece estar funcionando correctamente. No se preocupe por los propios WN en esta fase. El objetivo en esta etapa es determinar qué clústeres y cuáles ANC específicos están experimentando un comportamiento deseado o no deseado.

4. Dado que cada ANC está habilitado y probado, inhabilite de nuevo para que el siguiente pueda estar habilitado. La habilitación y prueba de cada ANC a su vez le permite determinar cuáles requieren más resolución de problemas.

Esta técnica de resolución de problemas es más aplicable en situaciones en las que la configuración WAAS parece no sólo no optimizar, sino también causar problemas con la conectividad de red normal.

### Paso a través de tráfico específico

Puede pasar a través de tráfico específico mediante una ACL de intercepción o mediante la configuración de la política de AppNav para el paso.

- Cree una ACL que niegue el tráfico específico que se debe pasar y permita todo lo demás. En este ejemplo, queremos pasar a través del tráfico HTTP (el puerto más pequeño 80). Establezca la lista de acceso de intercepción de ANC en la ACL definida. Las conexiones destinadas al puerto 80 se transmiten. Puede utilizar el comando **show statistics pass-through type appNav** para verificar que se está produciendo el paso a través de la verificación de que los contadores de ACL de intercepción PT están 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 la política de ANC para pasar el tráfico que coincida con clases específicas.

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

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

### Inhabilitación de un ANC en Línea

Hay varias maneras de inhabilitar un ANC en línea poniéndolo en estado de paso:

- Establezca la lista de VLAN de puente de intercepción en ninguno. En Central Manager, elija un dispositivo ANC y luego elija **Configure > Interception > Interception Configuration**. Seleccione la interfaz del puente y haga clic en el icono **Editar** barra de tareas. Establezca el campo VLAN en el valor "none".
- Inhabilite el contexto de servicio que contiene el ANC. En el Administrador central, elija un clúster y, a continuación, haga clic en la ficha AppNav Controllers, seleccione un ANC y haga clic en el icono de **Deshabilitar** barra de tareas.
- Aplique una ACL de intercepción con los criterios "deny ALL" (negar TODOS). Se prefiere este método. (Los dos primeros métodos interrumpen las conexiones optimizadas existentes.) Defina una ACL con los criterios deny ALL. En Central Manager, elija un dispositivo ANC, luego elija **Configure > Interception > Interception Access List**, y elija la lista de acceso deny ALL en la lista desplegable AppNav Controller Interception Access List.

Para inhabilitar la intercepción con una ACL desde la CLI, utilice los siguientes 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
```

Poniendo un ANC en estado de paso:

- Inhabilita la intercepción WAAS, no las interfaces.
- Inhabilita toda la optimización WAAS.
- Hace que todo el tráfico pase sin verse afectado.

### Inhabilitación de un ANC Off-Path

Para inhabilitar un ANC que se está ejecutando en modo fuera de trayectoria, inhabilite el protocolo WCCP para el ANC. Puede realizar esta acción en el ANC o en el router de redirección o en ambos. En el ANC, puede inhabilitar o eliminar los servicios WCCP, o puede quitar el

método de intercepción o cambiarlo de WCCP a otro método.

Para inhabilitar la intercepción WCCP, en el Administrador Central, elija un dispositivo ANC y luego elija **Configurar > Interceptación > Configuración de intercepción**. Desmarque la casilla de verificación Habilitar servicio WCCP o haga clic en el icono Quitar configuración de la barra de tareas para quitar completamente los parámetros de intercepción WCCP (se perderán).

Para inhabilitar la intercepción WCCP desde la CLI, utilice los siguientes comandos:

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

En algunos casos, puede haber varios ANC que reciben tráfico redirigido del mismo router. Por comodidad, puede optar por inhabilitar WCCP en el router, en lugar de los ANC. La ventaja es que puede quitar varios ANC de una granja WCCP en un solo paso. La desventaja es que no puede hacerlo desde WAAS Central Manager.

Para inhabilitar WCCP en el router, utilice la siguiente sintaxis:

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

Para volver a habilitar WCCP en el router, utilice la siguiente sintaxis:

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

En cada router WCCP, verifique que los ANC que eligió inhabilitar no aparezcan como clientes WCCP. El siguiente resultado se muestra cuando se han eliminado los servicios WCCP en el router.

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

## Solución de problemas del clúster de AppNav

Para resolver problemas de un clúster de AppNav, puede utilizar las siguientes herramientas:

- Alarmas de AppNav
- Supervisión de Central Manager
- Comandos CLI de AppNav para supervisar el estado del clúster y del dispositivo
- Comandos CLI de AppNav para monitorear las estadísticas de distribución de flujo
- Seguimiento de la conexión
- Registro de depuración de AppNav

### Alarmas de AppNav

El Cluster Membership Manager (CMM) provoca las siguientes alarmas debido a condiciones de error:

- Clúster degradado (crítico): visibilidad parcial entre ANC. ANC pasará por nuevas conexiones.
- Convergencia fallida (crítica): ANC no pudo converger en una vista estable de ANC y WN. ANC pasará por nuevas conexiones.
- Falló la unión de ANC (Crítica): ANC no pudo unirse a un clúster existente debido a la posible degradación del clúster con el ANC en él.
- ANC Mixed Farm (Minor): los ANC del clúster ejecutan versiones diferentes pero compatibles del protocolo de clúster.
- ANC inalcanzable (principal): un ANC configurado es inalcanzable.
- WN Unreachable (Major): un WN configurado es inalcanzable. Este WN no se utiliza para la redirección del tráfico.
- WN Excluded (Mayor): se puede alcanzar un WN configurado, pero se excluye porque uno o más ANC no pueden verlo. Este WN no se utiliza para la redirección del tráfico (nuevas conexiones).

Puede ver alarmas en el panel Alarmas de Central Manager o mediante el comando EXEC **show alarms** en un dispositivo.

**Nota:** El CMM es un componente interno de AppNav que administra la agrupación de ANC y WN en un clúster de AppNav asociado a un contexto de servicio.

### Supervisión de Central Manager

Puede utilizar el Administrador central para verificar, supervisar y resolver problemas de clústeres de AppNav. Central Manager tiene una vista global de todos los dispositivos WAAS registrados en su red y puede ayudarle rápidamente a localizar la mayoría de los problemas de AppNav.

En el menú Central Manager, elija **AppNav Clusters >** *cluster-name*. La ventana de inicio del clúster muestra la topología del clúster (incluidos los routers WCCP y de gateway), el estado general del clúster, el estado del dispositivo, el estado del grupo de dispositivos y el estado del enlace.

Primero, verifique que el estado general del clúster esté operativo.

Tenga en cuenta que los iconos ANC y WN que se muestran en este diagrama tienen el mismo nombre de dispositivo porque residen en el mismo dispositivo. En un ANC que también está optimizando el tráfico como un WN, estas dos funciones se muestran como iconos independientes en el diagrama de topología.

Se muestra un indicador de advertencia del triángulo naranja en cualquier dispositivo para el que el Administrador central puede no tener información actual porque el dispositivo no ha respondido en los últimos 30 segundos (el dispositivo podría estar desconectado o inalcanzable).

Puede obtener una vista de estado detallada de 360 grados de cualquier dispositivo ANC o WN pasando el cursor sobre el icono del dispositivo. La primera pestaña muestra alarmas en el dispositivo. Debe resolver cualquier alarma que esté inhibiendo el correcto funcionamiento del clúster.

Haga clic en la pestaña Interceptación para verificar el método de intercepción del dispositivo en cada ANC.

Si la intercepción está desactivada, el estado aparece como sigue:

Haga clic en la ficha Control de clúster para ver la dirección IP y el estado de cada dispositivo en el clúster que puede ver este ANC. Cada ANC del clúster debe tener la misma lista de dispositivos. Si no, indica un problema de configuración o de red.

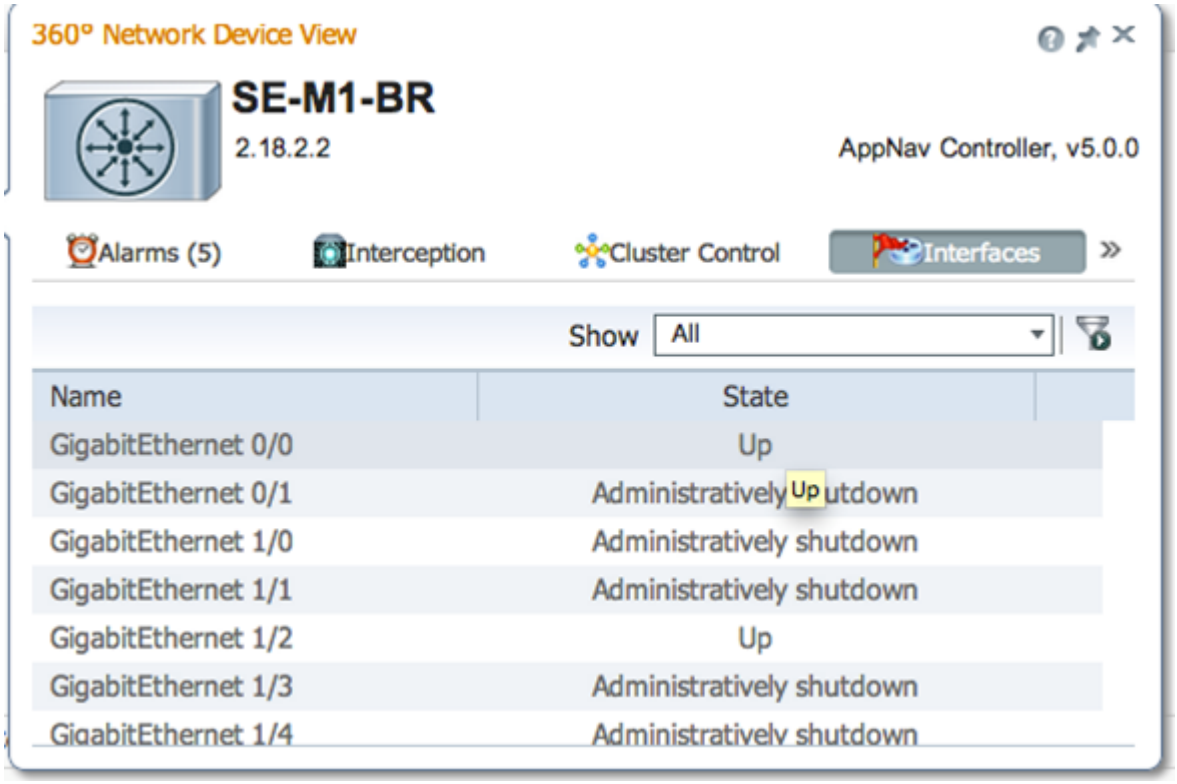
Si todos los ANC no se pueden ver entre sí, el clúster no está operativo y todo el tráfico pasa debido a la incapacidad del clúster para sincronizar los flujos.

Si todos los ANC están conectados pero tienen diferentes vistas de los WN, el clúster se encuentra en estado degradado. El tráfico todavía se distribuye, pero sólo a los WN que ven

todos los ANC.

Se excluyen todos los WN no vistos por todos los ANC.

Haga clic en la pestaña Interfaces para verificar el estado de las interfaces físicas y lógicas en el ANC.



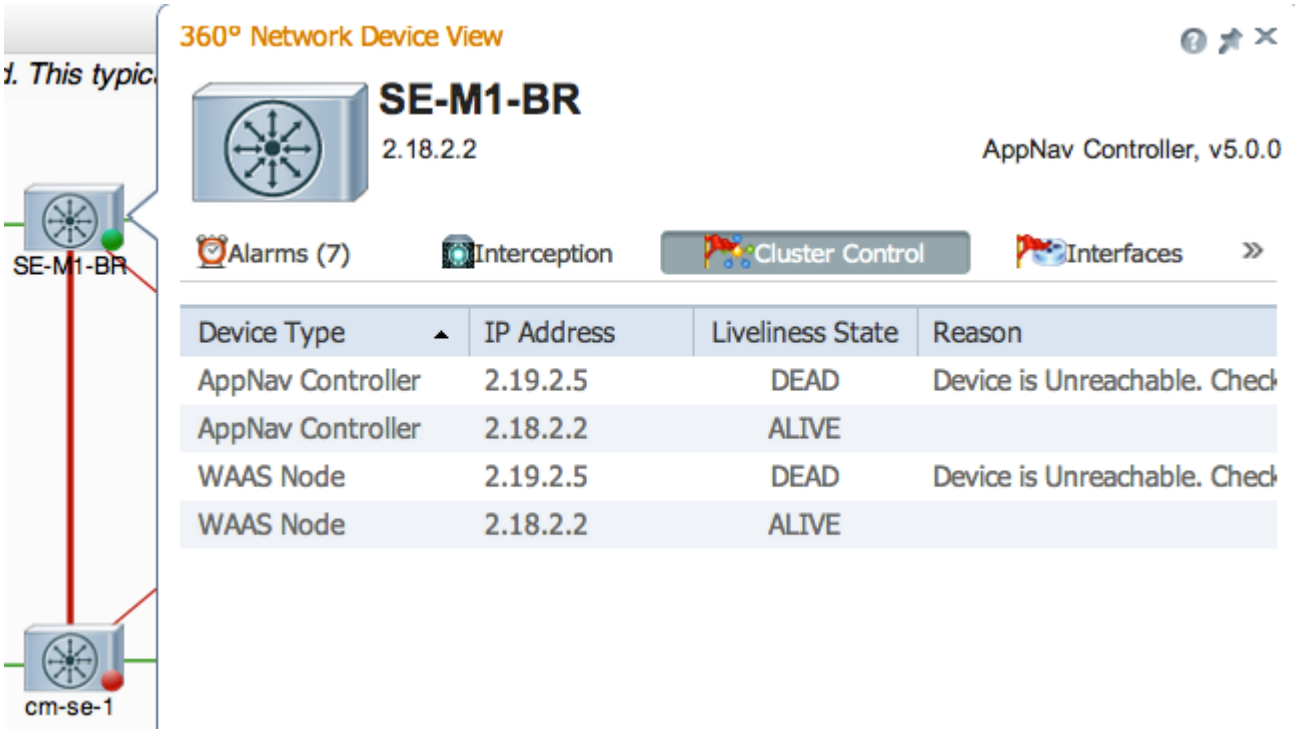

Observe la vista de 360 grados en cada WN del clúster y verifique el estado verde de todos los aceleradores en la pestaña Optimización. Un estado amarillo para un acelerador significa que el acelerador se está ejecutando pero no puede atender nuevas conexiones, por ejemplo, porque está sobrecargado o porque se ha eliminado su licencia. Un estado rojo indica que el acelerador no se está ejecutando. Si alguno de los aceleradores es amarillo o rojo, debe solucionar por separado esos aceleradores. Si falta la licencia Enterprise, la descripción indica que se ha revocado la licencia System. Instale la licencia Enterprise en la página **Admin > History > License Management** device.

Un agrupamiento dividido resulta de problemas de conectividad entre ANC en el agrupamiento. Si el Administrador Central puede comunicarse con todos los ANC, puede detectar un clúster dividido, sin embargo, si no puede comunicarse con algunos ANC, no puede detectar la división. La alarma "El estado de la administración está fuera de línea" se produce si Central Manager pierde la conectividad con cualquier dispositivo y el dispositivo se muestra como desconectado en Central Manager.

Es mejor separar las interfaces de administración de las interfaces de datos para mantener la conectividad de administración incluso si un link de datos está inactivo.

En un clúster dividido, cada subclúster de ANC distribuye de forma independiente los flujos a los WNG que puede ver, pero dado que los flujos entre los subclústeres no están coordinados, puede causar conexiones de reinicio y el rendimiento general del clúster se degrada.

Verifique la pestaña Control de Cluster de cada ANC para ver si uno o más ANC son inalcanzables. La alarma "Controlador de servicio es inalcanzable" se produce si dos ANC que alguna vez pudieron comunicarse entre sí pierden conectividad entre sí, pero esta situación no es la única causa de un clúster dividido, por lo que es mejor verificar la pestaña Control de clúster de cada ANC.




Si un ANC tiene una luz de estado gris, puede estar desactivado. Verifique que todos los ANC estén habilitados haciendo clic en la pestaña AppNav Controllers debajo del diagrama de topología. Si un ANC no está habilitado, su estado Habilitado es No. Puede hacer clic en el icono **Habilitar** barra de tareas para habilitar un ANC.

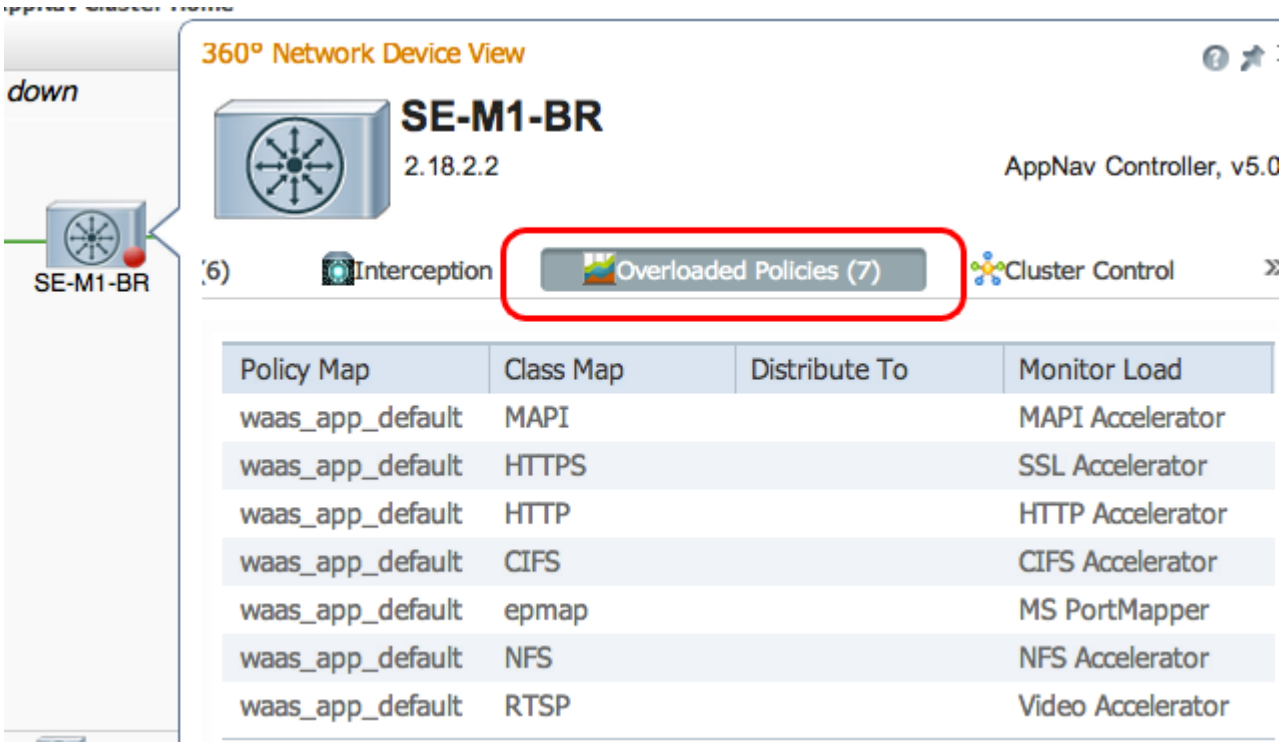
Verifique la política de AppNav en cada ANC que tenga algo que no sea una luz verde de estado. Si coloca el cursor sobre la luz de estado de un dispositivo, una sugerencia de herramienta le indicará el estado o el problema, si se detecta alguno.

Para verificar las políticas definidas, en el menú Administrador central, elija **Configurar > Políticas de AppNav** y luego haga clic en el **botón Administrar**.

Por lo general, debería haber una sola política asignada a todos los ANC en el clúster. La política predeterminada se denomina appNav_default. Seleccione el botón de opción junto a una directiva y haga clic en el icono **Editar** barra de tareas. El panel Política de AppNav muestra los ANC a los que se aplica la política seleccionada. Si no se muestran todos los ANC con una marca de verificación, haga clic en la casilla de verificación situada junto a cada ANC sin marcar para asignarle la política. Haga clic en **Aceptar** para guardar los cambios.

Después de verificar las asignaciones de directivas, puede verificar las reglas de políticas en la página Políticas de AppNav que se muestra. Seleccione cualquier regla de política y haga clic en el icono **Editar** barra de tareas para cambiar su definición.

Un ANC podría tener una luz de estado amarilla o roja si se sobrecarga una o más políticas. Verifique la pestaña Políticas sobrecargadas de la vista de 360 grados del dispositivo para ver una lista de políticas monitoreadas que están sobrecargadas.




Si un ANC se une al clúster, se muestra con una luz de estado amarilla y el estado de unión.

La pestaña Interceptación de la vista de dispositivo de 360 grados muestra que la trayectoria de interceptación está inactiva debido al estado de unión. La intercepción se detiene hasta que el ANC ha sincronizado sus tablas de flujo con los otros ANC y está listo para aceptar el tráfico. Este proceso normalmente no dura más de dos minutos.

Si elimina un ANC de un clúster, se sigue mostrando durante unos minutos en el diagrama de topología y como activo en la pestaña Control de Cluster, hasta que todos los ANC estén de acuerdo en la nueva topología del clúster. No recibe ningún flujo nuevo en este estado.

### Comandos CLI de AppNav para supervisar el estado del clúster y del dispositivo

Varios comandos CLI son útiles para la resolución de problemas en un ANC:

- **show run service-insertar**
- **show service-insertar service-context**
- **show service-insert appNav-controller-group**
- **show service-insertar service-node-group all**
- **show service-insert appNav-controller** *ip-address*
- **show service-insertar service-node** [*ip-address*]
- **show service-insertar service-node-group** *group-name*

Utilice estos comandos en un WN:

- **show run service-insertar**
- **show service-insertar service-node**

Puede utilizar el comando **show service-insert service-context** en un ANC para ver el estado del contexto del servicio y la vista estable de los dispositivos en el clúster:

```
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
```

Si el campo Estado de intercepción del dispositivo (anterior) muestra Apagar, significa que el CMM ha cerrado la intercepción debido a que este ANC no está listo para recibir flujos de tráfico. Por ejemplo, el ANC todavía podría estar en el proceso de unión y el clúster aún no ha sincronizado los flujos.

Los campos de Vista estable (arriba) enumeran las direcciones IP de los ANC y los WN que ve este dispositivo ANC en su última vista convergente del clúster. Esta es la vista utilizada para las operaciones de distribución. Los campos Vista actual enumeran los dispositivos anunciados por este ANC en sus mensajes de latido.

Puede utilizar el comando **show service-insert appNav-controller-group** en un ANC para ver el estado de cada ANC en el 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 obtener una lista de estados posibles de ANC y de unión, vea el comando **show service-insert** en la *Referencia de Comandos de Servicios de Aplicación de Área Amplia de Cisco*.

Puede utilizar el comando **show service-insert service-node** en un ANC para ver el estado de un WN particular en el clúster:

```
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
```

Puede utilizar el comando **show service-insert service-node-group** en un ANC para ver el estado de un WNG en particular en el clúster:

```
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
```

El primer WN del ejemplo anterior tiene el estado Excluded, lo que significa que el WN es visible

para el ANC pero se excluye del clúster porque uno o más ANC no pueden verlo.

La tabla Disponibilidad de SNG por AO muestra si cada AO puede prestar servicio a nuevas conexiones. Una AO está disponible si al menos un WN en el WNG tiene un estado VERDE para el AO.

Puede utilizar el comando **show service-insert service-node** en un WN para ver el estado del WN:

```
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
```

El estado monitoreado de un acelerador es su estado real, pero el estado informado puede diferir porque es el más bajo del estado del sistema o el estado del acelerador.

Para obtener más información sobre la resolución de problemas de optimización en un WN, vea los artículos Solución de problemas de optimización y resolución de problemas de aceleración de aplicaciones.

### Comandos CLI de AppNav para monitorear las estadísticas de distribución de flujo

Varios comandos CLI son útiles para la solución de problemas de políticas y distribución de flujo en un ANC:

- **show policy-map type appNav** *policy map-name*: muestra las reglas de política y los recuentos de visitas para cada clase en el policy map.
- **show class-map type appNav** *class-name*: muestra los criterios de coincidencia y los recuentos de aciertos para cada condición de coincidencia en el mapa de clase.
- **show policy-sub-class type appNav** *level1-class-name level2-class-name*: muestra los criterios de coincidencia y los recuentos de aciertos para cada condición de coincidencia en un mapa de clase en un mapa de política AppNav anidado.
- **show statistics class-map type appNav** *class-name* — Muestra las estadísticas de interceptación y distribución de tráfico para un mapa de clase.
- **show statistics policy-sub-class type appNav** *level1-class-name level2-class-name* — Muestra las estadísticas de interceptación y distribución del tráfico para un mapa de clase en un mapa de política AppNav anidado.
- **show statistics pass-through type appNav**: muestra las estadísticas de tráfico de AppNav para cada motivo de paso.
- **show appNav-controller flow-distribution** — Muestra cómo un ANC clasificaría y distribuiría un flujo hipotético específico, en función de la política definida y las condiciones de carga dinámica. Este comando puede ser útil para verificar cómo se manejará un flujo particular en un ANC y a qué clase pertenece.

Utilice estos comandos en un WN para resolver problemas de distribución de flujo:

- **show statistics service-insertar service-node** *ip-address* — Muestra estadísticas para aceleradores y tráfico distribuidos al WN.
- **show statistics service-insertar service-node-group name** *group-name* — Muestra estadísticas para aceleradores y tráfico distribuidos al WNG.

Puede utilizar el comando **show statistics class-map type appNav** *class-name* en un ANC para resolver problemas de distribución de flujo, por ejemplo para determinar por qué el tráfico puede

ser lento para una clase determinada. Podría ser un mapa de clase de aplicación como HTTP o, si todo el tráfico a una sucursal parece lento, podría ser un mapa de clase de afinidad de la sucursal. Este es un ejemplo para la clase 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
  ...
```

Las razones de paso de WN en la sección Indicado por SN aumentan solamente si la descarga de paso se configura en un WN. De lo contrario, el ANC no sabe que el WN está pasando por una conexión y no la cuenta.

Si las conexiones: El contador ANC interceptado no aumenta, hay un problema de interceptación. Puede utilizar la utilidad WAAS TcpTraceroute para resolver problemas de ubicación del ANC en la red, encontrar trayectos asimétricos y determinar la política aplicada a una conexión. Para obtener más información, vea la sección Seguimiento de conexiones.

## Comandos CLI de AppNav para depurar conexiones

Para depurar una conexión individual o un conjunto de conexiones en un ANC, puede utilizar el comando **show statistics appNav-controller connection** para mostrar la lista de conexiones activas.

```
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
```

Puede filtrar la lista especificando la dirección IP del cliente o servidor y/o las opciones de puerto y puede mostrar estadísticas detalladas sobre las conexiones especificando la palabra clave **detail**.

```
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
...
```

Puede especificar la opción summary para mostrar el número de conexiones activas distribuidas y de paso a través.

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

### Seguimiento de la conexión

Para ayudar a solucionar problemas de flujos de AppNav, puede utilizar la herramienta de seguimiento de conexiones en el Administrador central. Esta herramienta muestra la siguiente información para una conexión determinada:

- Si la conexión se pasó o se distribuyó a un WNG
- Motivo del paso, si procede
- WNG y WN a los que se distribuyó la conexión
- Acelerador supervisado para la conexión
- Mapa de clase aplicado

Para utilizar la herramienta Seguimiento de conexiones, siga estos pasos:

1. En el menú Central Manager, elija **AppNav Clusters >** *cluster-name* y luego elija **Monitor > Tools > Connection Trace**.

2. Elija el ANC, el dispositivo WAAS de peer, y especifique los criterios de coincidencia de conexión.

3. Haga clic en **Trace** para mostrar las conexiones coincidentes.

WAAS TCP Traceroute es otra herramienta no específica de AppNav que puede ayudarle a resolver problemas de conexión y red, incluidas las rutas asimétricas. Puede utilizarla para encontrar una lista de nodos WAAS entre el cliente y el servidor, y las políticas de optimización configuradas y aplicadas para una conexión. Desde el Administrador central, puede elegir cualquier dispositivo de la red WAAS desde el que ejecutar el traceroute. Para utilizar la herramienta Traceroute TCP de WAAS Central Manager, siga estos pasos:

1. En el menú WAAS Central Manager, elija **Monitor > Troubleshooting > WAAS Tcptraceroute**. Alternativamente, puede elegir primero un dispositivo y luego elegir este elemento de menú para ejecutar el traceroute desde ese dispositivo.

2. En la lista desplegable Nodo WAAS, elija un dispositivo WAAS desde el cual ejecutar el traceroute. (Este elemento no aparece si se encuentra en el contexto del dispositivo.)

3. En los campos Destination IP and Destination Port (IP de destino y Puerto de destino), introduzca la dirección IP y el puerto del destino al que desea ejecutar el traceroute

4. Haga clic en **Ejecutar TCPTraceroute** para mostrar los resultados.

Los nodos WAAS de la ruta de acceso rastreada se muestran en la tabla que se encuentra debajo de los campos. También puede ejecutar esta utilidad desde la CLI con el comando **waas-tcptrace**.

### Registro de depuración de AppNav

El siguiente archivo de registro está disponible para resolver problemas de AppNav cluster manager:

- Archivos de registro de depuración: /local1/errorlog/cmm-errorlog.current (y cmm-errorlog.*)

Para configurar y habilitar el registro de depuración del administrador del clúster de AppNav, utilice los siguientes comandos.

**NOTE:** El registro de depuración hace un uso intensivo de la CPU y puede generar una gran cantidad de resultados. Utilícelo de manera sensata y moderada en un entorno de producción.

Puede habilitar el registro detallado en el disco:

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

Las opciones para la depuración del administrador de clústeres (en la versión 5.0.1 y posteriores) son las siguientes:

```
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
```

Puede habilitar el registro de depuración para el administrador del clúster y, a continuación, mostrar el final del registro de errores de depuración de la siguiente manera:

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

También puede habilitar el registro de depuración para el administrador de distribución de flujo (FDM) o el agente de distribución de flujo (FDA) con estos comandos:

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

El FDM determina dónde distribuir los flujos según la política y las condiciones de carga dinámica de los WN. La FDA recopila información de carga de WN. Los siguientes archivos de registro están disponibles para resolver problemas de FDM y FDA:

- Archivos de registro de depuración: /local1/errorlog/fdm-errorlog.current (y fdm-errorlog.*)
- Archivos de registro de depuración: /local1/errorlog/fda-errorlog.current (y fda-errorlog.*)

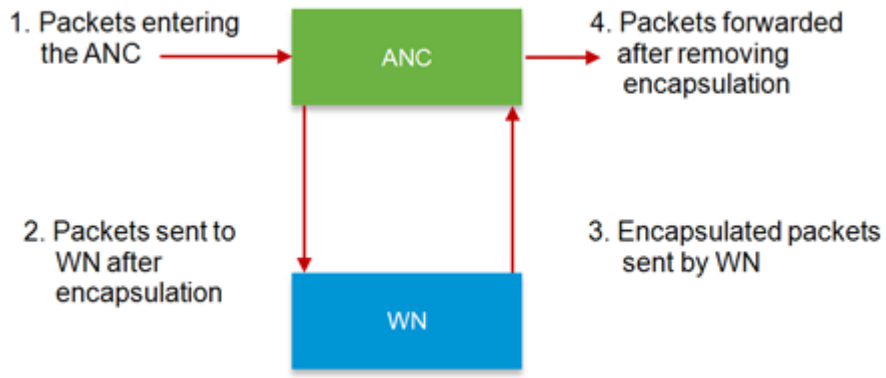
## Captura de paquetes AppNav

Se introduce un nuevo comando **packet-capture** para permitir la captura de paquetes de datos en las interfaces en el Cisco AppNav Controller Interface Module. Este comando también puede capturar paquetes en otras interfaces, y puede decodificar archivos de captura de paquetes. El comando **packet-capture** se prefiere sobre los comandos obsoletos **tcpdump** y **teetéreo**, que no pueden capturar paquetes en el Cisco AppNav Controller Interface Module. Consulte la *Referencia de Comandos de Cisco Wide Area Application Services* para obtener detalles sobre la

sintaxis de los comandos.

**Nota:** La captura de paquetes o la captura de depuración pueden estar activas, pero no ambas simultáneamente.

Los paquetes de datos enviados entre ANC y WN se encapsulan, como se muestra en el siguiente diagrama.




Si captura paquetes en los puntos 1 ó 4 del diagrama, se desencapsulan. Si captura paquetes en los puntos 2 ó 3, se encapsulan.

A continuación se muestra un ejemplo de salida para una captura de paquetes encapsulada:

```
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)
```

A continuación se muestra un ejemplo de salida para una captura de paquetes sin encapsular:

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

Directrices de captura de paquetes:

- Una ACL de captura de paquetes siempre se aplica al paquete IP interno para los paquetes encapsulados WCCP-GRE y SIA.
- La captura de paquetes se realiza en todas las interfaces ANC si no se proporciona la interfaz ANC para la captura de paquetes.

A continuación se muestra un ejemplo de salida para una captura de paquetes en una interfaz WN:

```
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 ...
```

Este es un ejemplo de descodificación de un archivo de captura de paquetes:

```
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
```

Puede especificar un src-ip/dst-ip/src-port/dst-port para filtrar los paquetes:

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
```