CHAPTER 4

Configuring AppNav

This chapter describes how to configure Cisco WAAS AppNav, which is a hardware and software solution that simplifies network integration of WAN optimization and overcomes challenges with provisioning, visibility, scalability, asymmetry, and high availability.

This chapter includes the following topics:

Information About AppNav

AppNav greatly reduces dependency on the intercepting switch or router by distributing traffic among WAAS devices for optimization using a powerful class and policy mechanism. You can use WAAS nodes (WNs) to optimize traffic based on sites and/or applications.

The AppNav solution has the ability to scale up to available capacity by taking into account WAAS device utilization as it distributes traffic among nodes. Also, the solution provides for high availability of optimization capacity by monitoring node overload and liveliness and by providing configurable failure and overload policies.

This section includes the following sections:

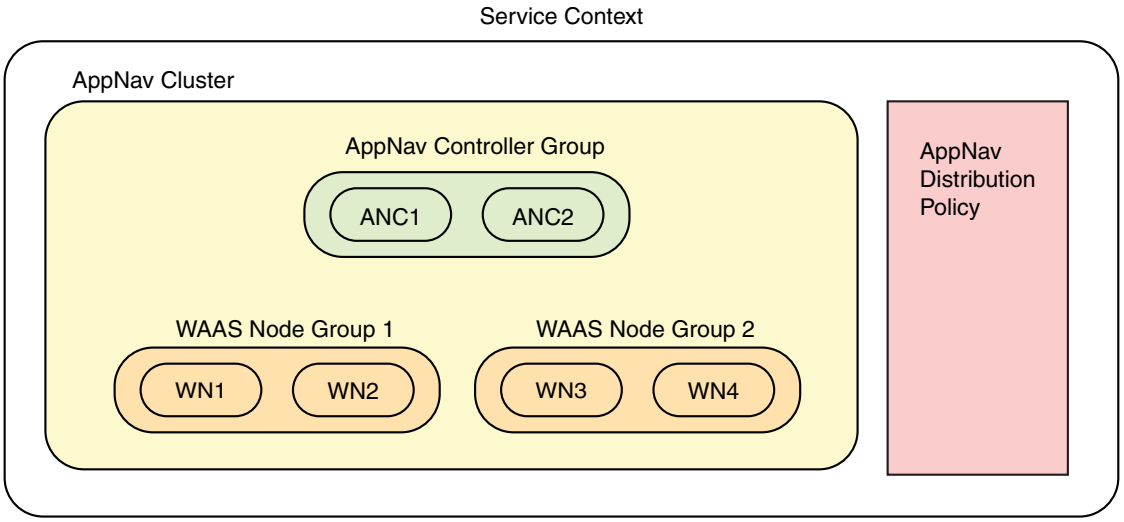
System Components

The AppNav solution consists of the following components (see Figure 4-1):

- AppNav Controller (ANC)—A WAAS appliance with a Cisco AppNav Controller Interface Module that intercepts network traffic and, based on an AppNav policy, distributes that traffic to one or more WAAS nodes (WNs) for optimization.

- AppNav Controller Group (ANCG)—A group of AppNav Controllers within one service context that together provide the necessary intelligence for handling asymmetric flows and providing high availability. The ANCG is configured on the ANC. An ANCG can have up to eight ANCs.
- WAAS Node (WN)—A WAAS optimization engine (WAE or WAVE appliance, NME-WAE or SM-SRE network module, or vWAAS instance, but not a WAAS Express device) that optimizes and accelerates traffic according to the optimization policies configured on the device. You can have up to 32 WNs in the service context. (In the CLI, a WAAS node is also known as a service node.)
- WAAS Node Group (WNG)—A group of WAAS nodes within a service context that services a particular set of traffic flows identified by AppNav policies. The WNG is configured on the ANC. You can have up to 32 WNGs in the service context. (In the CLI, a WAAS node group is also known as a service node group.)
- AppNav Cluster—The group of all ANC and WN devices within a service context.
- Service Context—The topmost entity that groups together one AppNav Controller Group (ANCG), one or more WAAS node groups (WNGs), and an associated AppNav policy. The service context is configured on the ANC.

Figure 4-1 AppNav Solution Components



Within a service context, WAAS devices can operate in one of two modes:

- Application accelerator—The device serves only as a WN within the service context. It receives traffic from the ANC, optimizes the traffic, and returns the traffic to the ANC to be delivered to its destination. The WN can be any kind of WAAS device or vWAAS instance.
- AppNav Controller—The device operates as an ANC that intercepts network traffic and, based on a flow policy, distributes that traffic to one or more WNs for optimization. Only a WAVE appliance that contains a Cisco AppNav Controller Interface Module can operate as an ANC. An ANC can also operate as a WN and optimize traffic as part of a WNG.

AppNav Controller Deployment Models

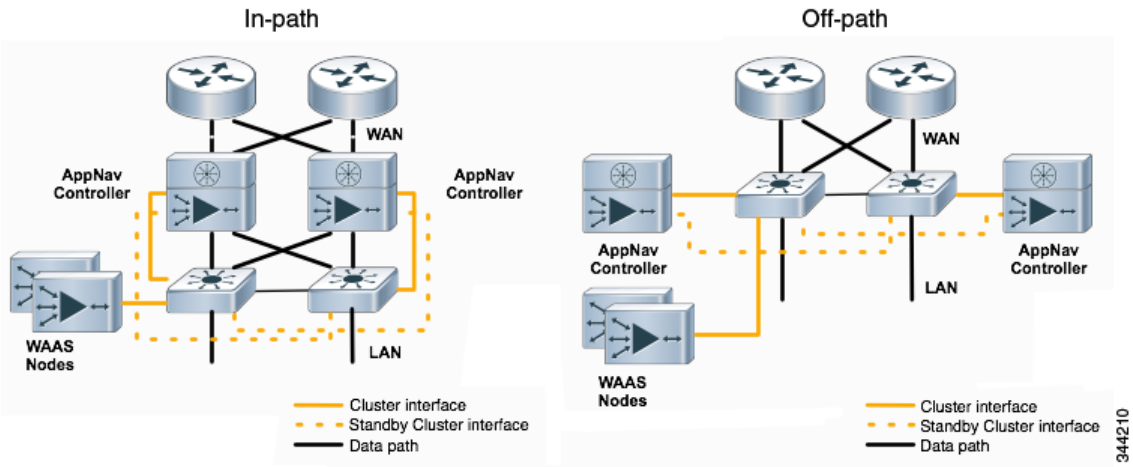
You can deploy AppNav Controllers in your network in two ways (see Figure 4-2):

- In-path—The ANC is physically placed between one or more network elements, enabling traffic to traverse a bridge group configured on the device in inline mode.
- Off-path—The ANC works with the network infrastructure to intercept traffic through the Web Cache Communication Protocol (WCCP).

The ANC provides the same features in both in-path and off-path deployments. In either case, only ANCs participate in interception from the switch or router. The ANCs then distribute flows to WNs using a consistent and predictable algorithm that considers configured policies and WN utilization.

In Figure 4-2, WAAS Nodes could be attached to either or both switches in the diagrams.

Figure 4-2 Deployment Models



AppNav Controller Interface Modules

A WAAS appliance operating as an ANC requires a Cisco AppNav Controller Interface Module, which is similar to a standard WAVE appliance interface module but contains additional hardware, including a network processor and high speed ternary content addressable memory (TCAM), to provide intelligent and accelerated flow handling. The following AppNav Controller Interface Modules are supported:

- 1-GB copper 12-port AppNav Controller Interface Module
- 1-GB SFP 12-port AppNav Controller Interface Module
- 10-GB SFP+ 4-port AppNav Controller Interface Module

AppNav Controller Interface Module interfaces are configured differently to support either in-path or off-path models of deployment:

- In-path—The ANC operates in inline interception mode with at least one inline bridge group configured on the AppNav Controller Interface Module. A bridge group consists of two or more physical or logical (port channel) interfaces.
- Off-path—The ANC operates in WCCP interception mode with one physical or logical (standby or port channel) interface configured with an IP address.

Interfaces on the AppNav Controller Interface Module can have three functions:

- Interception—Used to receive traffic intercepted from the network and egress traffic to the network. The interception interface is implied based on the AppNav Controller placement and does not require explicit configuration for this function.
- Distribution—Used to distribute traffic to the WNs and receive egressed traffic from the WNs. The distribution interface is explicitly configured as the cluster interface for intra-cluster traffic and must be assigned an IP address.
- Management—A management interface can be optionally and exclusively designated for management traffic and isolated from the normal data path. We recommend that you use one of the appliance's built-in interfaces for management traffic and reserve the high performance interfaces on the AppNav Controller Interface Module for interception and distribution.

You should use separate interfaces for interception and distribution for best performance, but you can use the same interface for both functions.

AppNav Controller Interface Modules support port channel and standby logical interfaces. A port channel allows you to increase the bandwidth of a link by combining multiple physical interfaces into a single logical interface. A standby interface allows you to designate a backup interface in case of a failure.

Interfaces on the AppNav Controller Interface Module support the following:

- A maximum of seven port channels with up to eight physical interfaces combined into a single port channel group.
- A maximum of five bridge groups configured over the physical or logical interfaces.

Interfaces on the AppNav Controller Interface Module do not support the following:

- Fail-to-wire capability
- Bridge virtual interfaces (BVIs)

AppNav Policy

The AppNav policy is a flow distribution policy that allows you to control how ANCs distribute traffic to the available WNs.

The AppNav policy consists of class maps that classify traffic according to one or more match conditions and a policy that contains rules that specify distribution actions to WNGs for each of the classes.

This section includes the following topics:

Class Maps

AppNav class maps classify traffic according to one or more of the following match conditions:

- Peer device ID—Matches traffic from one peer WAAS device, which could be handling traffic from a single site or a group of sites.

For example, you can use this kind of matching to classify all traffic from a peer device that serves one branch office.

- 3-tuple of source IP, and/or destination IP, and/or destination port (matches traffic from a specific application).

  For example, you can use this kind of matching to classify all HTTP traffic that uses port 80.

- A mix of one peer device ID and the source IP, and/or destination IP, and/or destination port (matches application-specific traffic from one site).

  For example, you can use this kind of matching to classify all HTTP traffic that is from a peer device that serves the one branch office.

The class-default class map is a system-defined default class map that is defined to match any traffic. By default, it is placed in the last rule in each policy to handle any traffic that is not matched by other classes.

Policies

An AppNav Controller matches incoming flows to class maps and the policy rules in a policy associate class maps with actions, such as distributing a flow to a particular WNG for optimization. The order in which rules are listed in the policy is important. Starting at the top of the policy, the first rule that matches a flow determines to which WNG it is distributed.

A policy rule can specify four kinds of actions to take on a flow:

- Specify the primary WNG to which to distribute the flow (required).
- Specify a backup WNG for distribution if the primary WNG is unavailable or overloaded (optional).

  The primary WNG receives all traffic until all WNs within the group become overloaded (reach 95 percent of the maximum number of transport flow optimization [TFO] connections) or are otherwise unavailable, and then traffic is distributed to the backup WNG. If a WN in the first WNG becomes available, traffic is again distributed there. If all WNs in both WNGs become overloaded, traffic is passed through unoptimized.

- Monitor the load on the application accelerator that corresponds to the application traffic matched by the class (optional).

  If the monitored application accelerator on one WN in a WNG becomes overloaded (reaches 95 percent of its maximum number of connections), the WN is considered overloaded and traffic is directed to another WN in the group. If all WNs become overloaded, traffic is distributed to the backup WNG. This application accelerator monitoring feature is useful for ensuring optimization for critical applications and is recommended for the MAPI and SMB accelerators.

- Specify a nested policy to apply to the flow (optional).

  For more information, see the "Nested Policies" section on page 4-6.

Within a WNG, flows are distributed evenly among WNs. If a WN reaches its maximum capacity or becomes unavailable, it is not sent new flows. New flows are sent to other available WNs in the WNG so that they can be optimized successfully.

Note If a WN that is doing MAPI or ICA application acceleration becomes overloaded, flows associated with existing MAPI and ICA sessions continue to be sent to the same WN due to the requirement that the same WN handle these types of flows. New MAPI and ICA flows, however, are distributed to other WNs.

The AppNav policy is specific to each ANC, though typically all ANCs in a cluster have the same policy. Each ANC consults its AppNav policy to determine which WNG to use for a given flow. Different ANCs in a cluster can have different AppNav policies, which allows you to customize distribution in certain cases. For example, when a cluster contains ANCs and WNs that are in different locations, it may be more desirable for an ANC to distribute traffic to WNs that are closer to it.

Nested Policies

A policy rule can specify one nested policy, which allows traffic identified in a class to be subdivided and handled differently. Nested policies provide two advantages:

- It allows another policy to be used as a common subclassification tool.

  For example, you can define a policy that contains monitoring actions and apply it as a subpolicy to multiple classes in the primary policy.

- It provides a method of including class maps with both match-any and match-all characteristics into a single subclass.

The nested policy feature is designed for use with site-based classes (matched by peer ID) at the first level and application-based subclasses (matched by IP address/port) at the second level. Only the first level policy can contain classes that use match peer conditions.

Site and Application Affinity

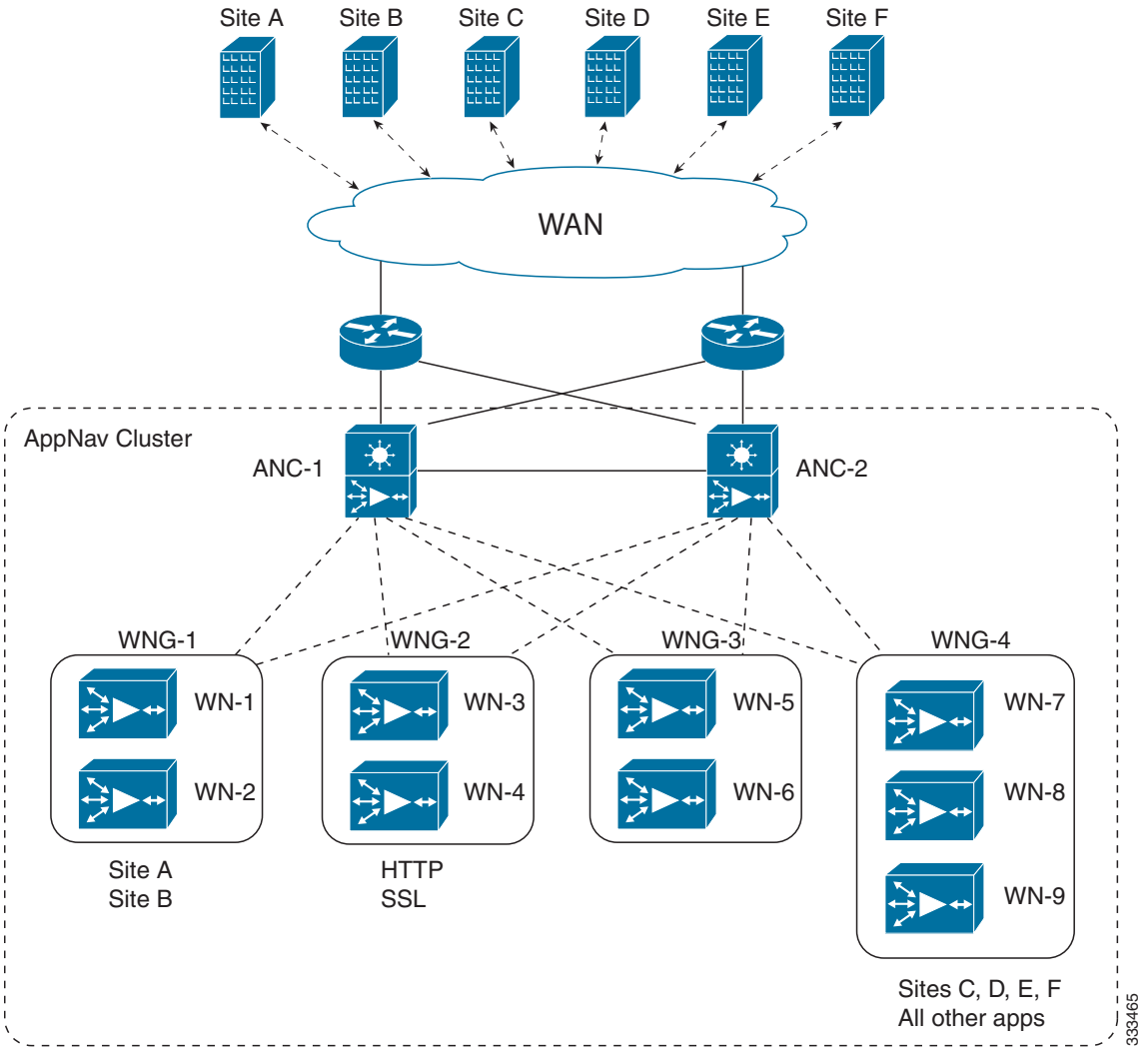
You can provision a WNG for serving specific peer locations (site affinity) or applications (application affinity) or a combination of the two. Using a WNG for site or application affinity provides the following advantages:

- Provisioning—Localize a class of traffic to achieve control over provisioning and performance monitoring. For example, a business-critical application like Sharepoint or a business-critical site can be given assured capacity and monitored closely for performance.
- Enhanced application performance—Better compression performance is achieved by limiting data that belongs to a site to one or a few WNs, which results in better utilization of the Data Redundancy Elimination (DRE) cache.

Figure 4-3 depicts how sites and applications can be associated with node groups. The following WNGs are defined:

- WNG-1—Consists of two WNs that process flows coming only from sites A and B.
- WNG-2—Consists of two WNs that process HTTP and SSL flows from any site. Whether HTTP and SSL flows from Site A and Site B should be processed by WNG-2 or WNG-1 is determined by the order of rules in the policy.
- WNG-3—Consists of two WNs that process MAPI flows coming from any site. Whether MAPI flows from Site A and Site B should be processed by WNG-3 or WNG-1 is determined by the order of rules in the policy.
- WNG-4—Consists of three WNs. The class-default class is applied to this WNG so that it is sent all flows that do not match any other class map.

Figure 4-3 Flow Distribution Using Site and Application Affinity



The following sections provide more details about these topics:

- Site Affinity, page 4-7
- Application Affinity, page 4-8

Site Affinity

Site affinity gives you the ability to always send all traffic from one site to a specific WNG, which allows you to reserve optimization capacity for critical sites and to improve compression performance through better utilization of the DRE cache.

Traffic from any location, not just a single site, can be matched in a class map and associated with a WNG.

You can implement site affinity by configuring a class map that matches the device ID of the WAE in the site. If a site has more than one WAE in a WCCP farm or a serial inline cluster, specify multiple device IDs in the class map. Next, associate the class map with a distribution action to a WNG in a policy rule.

You can also identify sites using source IP addresses or subnets in the class map, if you know what IP addresses are used in the site and keep the policy configuration consistent with site IP addresses. However, we recommend that you use peer device IDs in configuring site affinity.

Note A peer ID-based class map works only for matching flows that carry the WAAS auto discovery TCP options. If you configure a class to match a site peer ID at the data center, the same class does not match flows that originate in the other direction, such as those flows that originate from the data center and go back to the same site. Such flows are usually small in number compared to the site to data center flows.

If you want flows in both directions to go to the same WNG, you must configure two class maps: one to match in the site to data center direction, typically using the site device ID; and another to match the data center to site direction, using destination IP subnets belonging to the site. Both class maps can be configured to distribute traffic to the same WNG. A mesh network is a specific use case where flows can originate in either direction.

If the site WAE is in overload or does not mark the SYN packet with auto discovery options for any other reason, the ANC cannot match it to the peer match class map.

Application Affinity

Application affinity gives you the ability to always send certain application traffic to a specific WNG, which allows you to reserve optimization capacity for different applications depending on business priorities.

In the context of AppNav flow distribution, an application is defined using a three-tuple of the source IP, destination IP, and destination TCP port. The actual type of traffic does not matter for flow distribution. For example, you can use separate WNGs for HTTP traffic that is addressed to different destination ports or different server IP addresses. Destination IP and ports are most useful in using application affinity, but having the source IP also helps you to define the traffic of interest.

A small number of protocols, such as FTP, use dynamic destination ports. An FTP server in active mode originates a data connection back to the FTP client using a dynamic destination port. This port is exchanged over the control channel from client to server using the well-defined destination port 21. Consider trying to define a class map for FTP. Because the destination port is not known in advance, you cannot map both control and data connections to the same class. In this case, we recommend that you use the client IP addresses or subnets to match against destination IP addresses for the data connections. You must configure two class maps: one for the control channel, using destination port 21, and another for the data channel, using destination IP addresses. You can configure policy rules so that both class maps distribute traffic to the same WNG.

You can further classify traffic from a site into applications by combining the peer matches with three-tuple matches in a match-all class map, called a Custom class map type in the Central Manager. You can define separate WNGs, for example, for HTTP traffic from a particular site and CIFS traffic from the same site.

Default Policy Behavior

The following default class maps are provided:

- CIFS—Matches traffic for destination ports 139 and 445
- Citrix-ICA—Matches traffic for destination port 1494
- Citrix-CGP—Matches traffic for destination port 2598

- epmap—Matches traffic for destination port 135
- HTTP—Matches traffic for destination ports 80, 3128, 8000, 8080, and 8088
- HTTPS—Matches traffic for destination port 443
- MAPI—Matches traffic for the MS RPC MAPI application (dynamic port assignment)
- NFS—Matches traffic for destination port 2049
- RTSP—Matches traffic for destination ports 554 and 8554
- class-default—Matches any TCP traffic (this class map cannot be edited or deleted)

If you use the Central Manager AppNav Cluster Wizard to create an AppNav Cluster, the wizard creates a default policy named appnav_default. This policy is assigned by default to all ANCs in a cluster and contains only the class-default policy rule that has the following characteristics:

- Matches class-default (any TCP) traffic.
- Distributes class-default traffic to the default WNG, which includes all WNs created by the wizard, with no backup WNG specified.
- Contains the waas_app_default nested policy, which provides application monitoring for each of the default class maps, except video (RTSP).

  When you use the Central Manager to define a policy rule for any class that uses peer matching or source or destination IP address matching (but not port matching), it automatically adds the waas_app_default policy as a nested policy. The waas_app_default policy is created by the system and monitors all application accelerators (except video), so you do not need to manually add application accelerator monitoring to your policy rules, unless it is for the video accelerator.

If you do not use the Central Manager AppNav Cluster Wizard to create a cluster, there is no default flow distribution, so if an incoming flow does not match any class in the AppNav policy, it is not distributed to any WNG; instead, it is passed through.

If a WNG is defined but is not used in any policy rule, it does not receive any flows. If a policy is defined but not applied to an ANC, it does not take effect.

The default action for a policy rule is none, which is context dependent: in a top level policy it means pass through and if the policy is nested, it means inherit the parent policy rule action.

Prerequisites for AppNav Deployment

AppNav has the following prerequisites:

- Each WAAS appliance to be used as an AppNav Controller must contain a Cisco AppNav Controller Interface Module.
- Each AppNav Controller must be configured in appnav-controller device mode.

Guidelines and Limitations

AppNav has the following configuration guidelines and limitations:

- An AppNav Cluster can contain a maximum of the following:
  - 8 ANCs
  - 32 WNs

  - 32 WNGs
- All ANCs in an ANCG must have the same set of ANCs and WNGs in their configuration.
- All WNs in one WNG must have identical optimization policies configured on them.
- AppNav class maps and policies can be configured only at the cluster level, not at the device level, from the Central Manager. At the device level, class maps and policies may only be viewed.
- You can define the following maximum policy entities within a service context:
  - 1024 match conditions
  - 512 AppNav class maps
  - 64 rules per AppNav policy
  - 64 AppNav policies, though only one policy is actively bound to the service context and used for flow distribution on a given ANC
- There is no fail-to-wire capability on AppNav Controller Interface Module interfaces configured in bridge groups for inline mode, which would allow traffic to bypass the interface if the device fails or loses power. Therefore, if you are using inline mode, we recommend that you deploy two or more AppNav Controller appliances to provide high availability.
- Virtual blades are not supported on WAAS appliances that are operating as AppNav Controllers.

Configuring an AppNav Cluster

This section contains the following topics:

Task Flow for Configuring an AppNav Cluster

You must complete the following steps to configure an AppNav Cluster:

1. Install and configure the individual ANC and WN devices with basic network settings. See the "Configuring WAAS Device Interfaces" section on page 4-11.
2. Use the Central Manager AppNav Cluster Wizard to create a cluster and configure the interception mode, configure cluster settings, choose cluster devices, configure traffic interfaces, and configure WCCP settings if you are using WCCP. See the "Creating a New AppNav Cluster with the Wizard" section on page 4-14.

3. (Optional) Configure AppNav class maps. This step is necessary only if you want to customize the default class map configuration. The system adds several default class maps that match traffic corresponding to most of the application accelerators and a class-default class map that matches all traffic. See the "Configuring AppNav Class Maps" section on page 4-19.
4. (Optional) Configure an AppNav policy. This step is necessary only if you want to customize the default policy. The system adds a default policy that distributes all traffic to the WNG-Default WNG, which is the node group into which all WNs are grouped by default. See the "Configuring Rules Within an AppNav Policy" section on page 4-22.
5. (Optional) Configure WAAS node optimization class maps and policy rules. This step is necessary only if you want to customize the default optimization policy that is listed in Appendix A, "Predefined Optimization Policy."
6. (Optional) Configure an interception ACL on the ANCs. See the "Configuring AppNav Controller ACLs" section on page 4-26.

Configuring WAAS Device Interfaces

Before you can use the AppNav Cluster wizard to create an AppNav Cluster, you must connect the WAAS device interfaces and configure the management interfaces. Configuration differs depending on whether management traffic uses a separate interface or shares the traffic handling interface.

This section contains the following topics:

For more information about device interface configuration, see Chapter 6, "Configuring Network Settings." For more information about configuring a bridge group for inline interception mode, see the "Configuring Inline Operation on ANCs" section on page 5-49.

Interface Configuration with a Separate Management Interface

If you want management traffic to use a dedicated interface, separate from the traffic data path, connect and configure the devices as described in this section.

AppNav Controller

Step 1 Connect the last AppNav Controller Interface Module port to the switch/router port for the cluster traffic. For example, this port is GigabitEthernet 1/11 on a 12-port module or TenGigabitEthernet 1/3 on a 4-port module.

Step 2 Connect a built-in Ethernet port to the switch/router port for the management interface.

Step 3 For an in-path (inline) deployment, connect the first pair of ports on the AppNav Controller Interface Module (for example, GigabitEthernet 1/0 [LAN] and GigabitEthernet 1/1 [WAN] for bridge 1) to corresponding switch/router ports.

If the ANC is connected to a second router for a dual inline deployment, connect the second pair of ports on the AppNav Controller Interface Module (for example, GigabitEthernet 1/2 [LAN] and GigabitEthernet 1/3 [WAN] for bridge 2) to corresponding switch/router ports.

Step 4 Use the device **setup** command to configure the following settings:

- Configure the device mode as AppNav Controller.
- Configure the IP address and netmask of the built-in management port.
- Configure the built-in management port as the primary interface.
- Configure the other network and basic settings (default gateway, DNS, NTP server, and so forth).
- Register the device with the Central Manager by entering the Central Manager IP address.

Step 5 Configure the IP address and netmask of the last AppNav Controller Interface Module port. You can also configure these settings through the AppNav Cluster wizard, if desired.

WAAS Node

Step 1 Connect a built-in Ethernet port to the switch/router port for the management interface.

Step 2 Use the device **setup** command to configure the following settings:

- Configure the device mode as Application Accelerator.
- Configure the IP address and netmask of the built-in management port.
- Configure the built-in management port as the primary interface.
- Configure the other network and basic settings (default gateway, DNS, NTP server, and so forth).
- Register the device with the Central Manager by entering the Central Manager IP address.

Interface Configuration with a Shared Management Interface

If you want management traffic to use an interface shared by the traffic data path, connect and configure the devices as described in this section.

AppNav Controller

Step 1 Connect the last AppNav Controller Interface Module port to the switch/router port for the cluster traffic. For example, this port is GigabitEthernet 1/11 on a 12-port module or TenGigabitEthernet 1/3 on a 4-port module.

Step 2 For an in-path (inline) deployment, connect the first pair of ports on the AppNav Controller Interface Module (for example, GigabitEthernet 1/0 [LAN] and GigabitEthernet 1/1 [WAN] for bridge 1) to corresponding switch/router ports.

If the ANC is connected to a second router for a dual inline deployment, connect the second pair of ports on the AppNav Controller Interface Module (for example, GigabitEthernet 1/2 [LAN] and GigabitEthernet 1/3 [WAN] for bridge 2) to corresponding switch/router ports.

Step 3 Use the device **setup** command to configure the following settings:

- Configure the device mode as AppNav Controller.
- Configure the IP address and netmask of the last AppNav Controller Interface Module port.
- Configure the last AppNav Controller Interface Module port as the primary interface.

– Configure the other network and basic settings (default gateway, DNS, NTP server, and so forth).
– Register the device with the Central Manager by entering the Central Manager IP address.

WAAS Node

Step 1 Connect a built-in Ethernet port to the switch/router port for the management interface.

Step 2 Use the device **setup** command to configure the following settings:

– Configure the device mode as Application Accelerator.
– Configure the IP address and netmask of the built-in management port.
– Configure the built-in management port as the primary interface.
– Configure the other network and basic settings (default gateway, DNS, NTP server, and so forth).
– Register the device with the Central Manager by entering the Central Manager IP address.

Interface Configuration Considerations

The following guidelines concern WAAS device interface configuration:

- On an ANC, the intercepted traffic must go through an interface on the AppNav Controller Interface Module.
- On an ANC that also serves as a WN, the cluster interface is the same as the interception interface.
- On a WN, cluster traffic can be handled on any interface, either built-in or on an interface module.
- To simplify AppNav deployment, the AppNav Cluster Wizard uses the following conventions for configuring the AppNav Controller Interface Module ports on an ANC:
  – The default port for cluster traffic is the last port on the module (for example, GigabitEthernet 1/11 on a 12-port module or TenGigabitEthernet 1/3 on a 4-port module).
  – For an in-path (inline) deployment, the default interception bridge is the first pair of ports on the module (for example, GigabitEthernet 1/0 [LAN] and GigabitEthernet 1/1 [WAN] for bridge 1). If the ANC is connected to a second router for a dual inline deployment, the default second interception bridge is the second pair of ports on the module (for example, GigabitEthernet 1/2 [LAN] and GigabitEthernet 1/3 [WAN] for bridge 2).

The AppNav Cluster Wizard uses four predefined deployment models to help simplify configuration. Each deployment model expects interfaces to be connected and configured in a particular way, except for the Custom option, which allows you to configure interfaces in any way. Before you run the wizard with one of the four predefined models, the needed interfaces must be in either of these states:

- Not configured with an IP address and netmask and not used as part of another logical interface. (However, the last port on the AppNav Controller Interface Module can be configured with an IP address because it is the default port for cluster traffic.)

  The wizard configures all needed traffic interface settings.
- Configured as expected by the wizard according to the following deployment model expectations.

The following sections describe the interface configurations used by each of the four predefined deployment models.

Single AppNav Controller WCCP Interception

With a 12-port AppNav Controller Interface Module:

- Port channel 1—Contains ports GigabitEthernet 1/10 and 1/11
- Cluster interface—Port channel 1

With a 4-port AppNav Controller Interface Module:

- Cluster interface—GigabitEthernet 1/3

Dual AppNav Controllers WCCP Interception

With a 12-port AppNav Controller Interface Module:

- Port channel 1—Contains ports GigabitEthernet 1/10 and 1/11
- Port channel 2—Contains ports GigabitEthernet 1/8 and 1/9
- Standby group 1—Contains interfaces Port channel 1 (primary) and Port channel 2
- Cluster interface—Standby Group 1

With a 4-port AppNav Controller Interface Module:

- Standby group 1—Contains ports GigabitEthernet 1/2 and 1/3 (primary)
- Cluster interface—Standby Group 1

Single AppNav Controller Inline Interception

- Interception bridge 1—Contains ports GigabitEthernet 1/0 (LAN) and 1/1 (WAN)
- Cluster interface—GigabitEthernet 1/11

Dual AppNav Controllers Inline Interception

- Interception bridge 1—Contains ports GigabitEthernet 1/0 (LAN) and 1/1 (WAN)
- Interception bridge 2—Contains ports GigabitEthernet 1/2 (LAN) and 1/3 (WAN)
- Standby group 1—Contains ports GigabitEthernet 1/10 and 1/11 (primary)
- Cluster interface—Standby Group 1

Creating a New AppNav Cluster with the Wizard

Prerequisites

- Set up the individual ANC and WN devices as described in the "Configuring WAAS Device Interfaces" section on page 4-11.
- Ensure that all ANCs are configured for AppNav Controller device mode. If you need to change the device mode, see the "Changing Device Mode" section on page 2-16.
- Use the Central Manager to configure basic settings for all devices such as NTP server, AAA, logging, and so on.

Detailed Steps

To create a new AppNav Cluster by using the wizard, follow these steps:

Step 1 From the WAAS Central Manager menu, choose **AppNav Clusters > All AppNav Clusters**.

The Manage AppNav Clusters window appears.

Step 2 Click the **AppNav Cluster Wizard** icon in the taskbar of the Manage AppNav Clusters area. The Cluster Wizard window appears.

Step 3 In the Deployment model drop-down list, choose one of the following deployment models that matches your deployment:

- **Single AppNav Controller WCCP interception**
- **Dual AppNav Controllers WCCP interception**
- **Single AppNav Controller Inline interception**
- **Dual AppNav Controllers Inline interception**
- **Custom**—For a deployment that does not match one of the choices above

Click **Next**.

Step 4 (Optional) If you chose the Custom deployment model, from the Interception method drop-down list, choose the **WCCP** or **Inline interception** method and click **Next**.

Step 5 Define the cluster settings by entering the following information:

- In the Name field, enter a name for the cluster. Use only letters, numbers, hyphen, and underscore, up to a maximum of 32 characters and beginning with a letter.
- (Optional) In the Description field, enter a description of the cluster. Use only letters and numbers, up to a maximum of 200 characters.
- Check the **Disable Distribution** check box if you want make the cluster operate in monitoring mode, otherwise, it is activated when the wizard finishes. In monitoring mode, all traffic is passed through instead of being distributed to WNs.

Click **Next**.

Step 6 Choose the ANC and WN devices that you want to be part of the cluster:

a. Choose up to eight ANCs in the AppNav Controller device list by clicking the check box next to the device names. You can use the filter settings in the taskbar to filter the device list.

b. (Optional) If you want to enable optimization on the ANC devices, check the **Enable WAN optimization on selected AppNav Controller(s)** check box (it may be enabled or disabled by default, depending on the deployment model you chose).

c. Choose up to 32 WNs in the WAAS Nodes device list by clicking the check box next to the device names. You can use the filter settings in the taskbar to filter the device list.

If there are devices that are ineligible to join the cluster, click **Show Ineligible Devices** to see them and the reasons why they are ineligible. You can use the filter settings to filter the list.

d. Click **Next**.

Step 7 Verify the cluster interface, IP address, and netmask for each device in the cluster. The wizard automatically selects recommended cluster interfaces that should be configured. To edit the IP address and netmask settings for a device, choose the device and click the **Edit** taskbar icon. This screen does not appear if you are configuring a custom cluster.

Click **Finish** if you are using inline interception (and you are done) or click **Next** if you are using WCCP interception (and continue with the following steps for WCCP).

Step 8 (Optional) Configure the WCCP settings for the ANC. This screen does not appear if you are configuring an inline cluster.

For details about configuring WCCP, see the "Configuring WCCP on WAEs" section on page 5-11.

a. Ensure the **Enable WCCP Service** check box is checked if you want to enable WCCP. This item appears only if you are defining a custom cluster.

b. Verify the single WCCP service ID of 61 (default) or change it if desired.

   You need to configure only this single WCCP service on both the ingress and egress ports of the router doing WCCP redirection to this ANC.

c. (Optional) If you want to enable two WCCP services, uncheck the **Enable Single Service Mode** check box (it is checked by default because two WCCP services are not needed). The automatically assigned second service ID number is shown in the Service ID2 field.

d. From the Redirect Method drop-down list, choose the WCCP L2 or WCCP GRE redirect method. For details on the redirect method, see the "Configuring or Viewing the WCCP Settings on ANCs" section on page 5-22. This item appears only if you are defining a custom cluster.

e. (Optional) If you do not want to use the default gateway defined on the device, uncheck the **Use Default Gateway as WCCP Router** check box. Enter the address of one or more WCCP routers, separated by commas, in the WCCP Routers field.

f. Click **Advanced WCCP Settings** to configure additional settings as needed. For more information on these fields, see the "Configuring or Viewing the WCCP Settings on ANCs" section on page 5-22. This item appears only if you are defining a custom cluster.

g. Click **Next**. If you are configuring multiple ANCs, a similar screen is shown for each ANC.

Step 9 Configure the interception and cluster interface settings for each device. The Cluster Interface Wizard appears only if you are defining a custom cluster, with one screen for each device in the cluster:

a. Configure individual interfaces, port channels, standby interfaces, and bridge interfaces (for inline only) as needed on the device by using the graphical interface wizard. If you are configuring an inline ANC, you must define a bridge interface with two physical or port-channel interfaces (or one of each). For details on how to use the wizard, see the "Configuring Interfaces with the Graphical Interface Wizard" section on page 4-17.

b. From the Cluster Interface drop-down list, choose the interface to be used for intra-cluster traffic.

c. Click **Next**. If you are configuring multiple devices, a similar screen is shown for each device.

Step 10 Click **Finish** to save the cluster configuration.

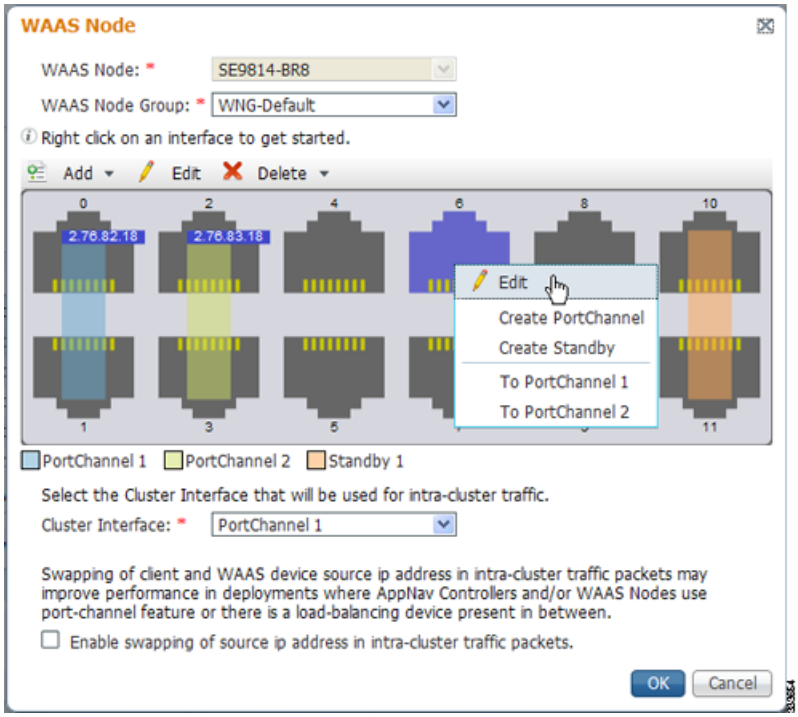
By default, the wizard assigns all WNs to a default WNG named WNG-Default. You can create additional WNGs as described in the "Adding a New WAAS Node to the Cluster" section on page 4-32. You can reassign WNs to different WNGs as described in the "Configuring WAAS Node Settings" section on page 4-29.

After you create an AppNav Cluster, it is shown in the Manage AppNav Clusters list. For details on monitoring the cluster, see the "Monitoring an AppNav Cluster" section on page 4-34.

Configuring Interfaces with the Graphical Interface Wizard

You can easily configure interfaces on AppNav Controller Interface Modules that are installed in devices that are part of an AppNav Cluster by using the graphical interface wizard (see Figure 4-4).

Figure 4-4 Graphical Interface Wizard



The graphical interface wizard appears when you are editing the settings for a WN or ANC in the AppNav Cluster context. The top two fields, WAAS Node and WAAS Node Group, do not appear when configuring ANC interfaces.

In the graphical interface view, hover over a physical or logical interface to see its identifier (for example, GigabitEthernet 1/0). Port channels, bridge groups, and standby groups are indicated by colored blocks or dotted outlines. The IP address of each configured physical or logical interface is shown in a small blue highlight. The legend below the table indicates port channel, bridge group, and standby interfaces.

Right click on an interface to choose from the following actions:

- Edit—To display a pane where you can edit the interface description, IP address, netmask, and shutdown status.
- Create PortChannel—To create a new port channel with this interface. This choice displays a pane where you can configure the port channel number, description, IP address, netmask, and shutdown status.
- Create Bridge—To create a new bridge group with this interface. This choice displays a pane where you can configure the bridge group number and description and enable link state propagation. This choice appears only when configuring a device for inline interception. A bridge interface consists of two physical or port-channel interfaces (or one of each)

- Create Standby—To create a new standby group with this interface. This choice displays a pane where you can configure the standby group number, description, IP address, netmask, and shutdown status.
- To PortChannel *n*—To add this interface to an existing port channel, where *n* is the port channel number.
- To Standby *n*—To add this interface to an existing standby group, where *n* is the standby group number.
- To Bridge *n*—To add this interface to an existing bridge group, where *n* is the bridge group number.
- For standby interfaces (right-click within the standby interface group indicator):
  - Edit—To edit the standby group settings such as the description, IP address, netmask, primary interface, and shutdown status.
  - Delete Standby *n*—To delete the standby group.
- For port channel interfaces (right-click within the port channel indicator):
  - Edit—To edit the port channel settings such as the port channel number, description, IP address, netmask, and shutdown status.
  - Remove from Standby *n*—To remove the port channel from standby group *n*.
  - Delete PortChannel *n*—To delete the port channel.
- For bridge group interfaces (right-click within the bridge group indicator):
  - Edit—To edit the bridge group settings such as the bridge group number, description, and link state propagation status.
  - Delete Bridge *n*—To delete the standby group.

To select an interface:

- Individual interface—Click and selection is indicated by a blue color.
- Standby group—Click on colored or dotted line indicator and selection is indicated by a thick dotted blue outline around all interfaces in the standby group.
- Port channel or bridge group—Click on colored indicator and selection is indicated by a thick dotted blue outline around all interfaces in the port channel or bridge group.

You can also perform actions by selecting an interface and clicking the following taskbar icons:

- Add (choices differ depending on the selected entity):
  - Create PortChannel—To create a new port channel with this interface.
  - Create Bridge—To create a new bridge group with this interface.
  - Create Standby—To create a new standby group with this interface.
  - To PortChannel *n*—To add this interface to an existing port channel, where *n* is the port channel number.
  - To Standby *n*—To add this interface to an existing port channel, where *n* is the port channel number.
- Edit—To edit the selected interface.
- Delete (choices differ depending on the selected entity):
  - Remove from Standby *n*—To remove the port channel from standby group *n*.
  - Delete PortChannel *n*—To delete the port channel.
  - Delete Standby *n*—To delete the standby group.

– Delete Bridge *n*—To delete the bridge group.

Use the Cluster Interface drop-down list to select the interface to be used for intra-cluster traffic (between the ANCs and WNs).

To enable swapping of client and WAAS device source IP address fields in intra-cluster traffic, check the **Enable swapping of source IP address in intra-cluster traffic** check box. You may want to enable this option if you are using a port channel for the cluster interface or there is a load balancing device between the ANC and WN. This option may improve the load balancing of traffic that the ANC distributes to WNs for optimization because it load balances based on the client IP address rather than the ANC IP address. (For traffic from the server to the client, it swaps the server IP address with the ANC IP address.)

Note If you are using WCCP, the WCCP control messages must pass through the ANC interface that receives intercepted traffic from the routers. If WCCP control messages are routed to the ANC management interface, the cluster does not operate.

Configuring AppNav Policies

This section contains the following topics:

Configuring AppNav Class Maps

To configure AppNav class maps, follow these steps:

Step 1 From the WAAS Central Manager menu, choose **AppNav Clusters** > *cluster-name*.

Step 2 Choose **Configure** > **AppNav Cluster** > **AppNav Class-Map**.

The AppNav Class-Maps window appears, listing the existing class maps.

From this window, you can perform the following tasks:

- Use the filter settings in the Show drop-down list to filter the class map list as needed. You can use a quick filter or show all class maps.
- Edit a class map by selecting it and clicking the **Edit** taskbar icon.
- Delete one or more class maps by selecting them and clicking the **Delete** taskbar icon.
- Add a new class map as described in the steps that follow.

Step 3 Click the **Add Class-Map** taskbar icon.

Step 4 In the Name field enter a name for the class map.

Step 5 (Optional) In the Description field enter a description for the class map.

Step 6 From the Type drop-down list, choose the class map type:

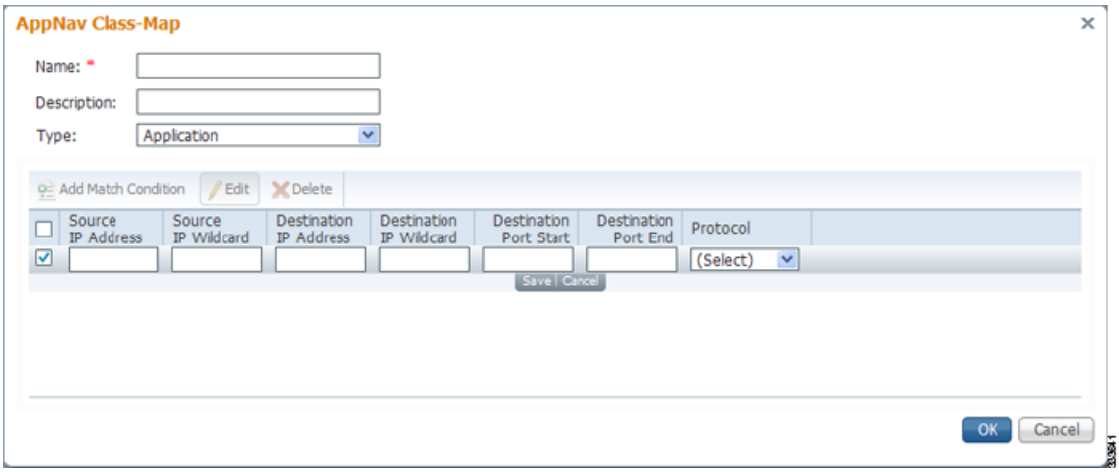
- **Application**—Matches traffic for a particular application based on source and/or destination IP addresses and/or ports, or the Microsoft RPC application identifier (for applications that use dynamic port allocation). Continue with Step 7.

- **Site**—Matches traffic from particular WAAS peer devices, for site affinity. Continue with Step 8.
- **Custom**—Mixes application and site affinity. Matches traffic for a particular application from one specific peer WAAS device. Continue with Step 9.
- **Any TCP**—Matches any TCP traffic as a catch-all classifier. If you choose this type, there are no other fields to set. Click **OK** to finish and return to the class maps list.

The match conditions shown in the lower part of the pane change depending on the class map type.

Step 7 (Optional) For an Application class map type, enter one or more match conditions. You can perform the following tasks in this pane:

- Edit a match condition by selecting it and clicking the **Edit** taskbar icon.
- Delete one or more match conditions by selecting them and clicking the **Delete** taskbar icon.
- Add a new match condition as described in the steps that follow.



a. Click the **Add Match Condition** taskbar icon.

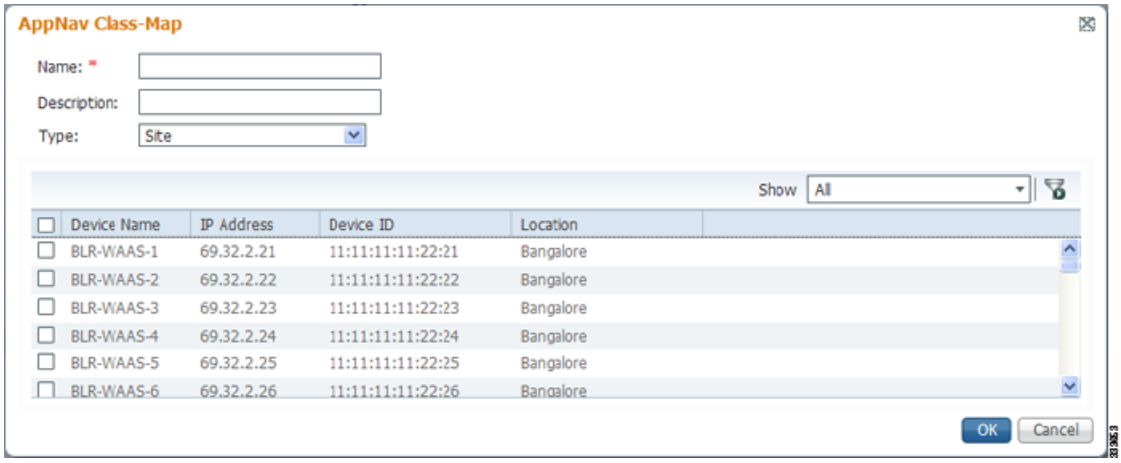
b. Enter values in one or more fields to create a condition for a specific type of traffic. For example, to match all traffic going to ports 5405–5407, enter **5405** in the Destination Port Start field and **5407** in the Destination Port End field. You can use the IP address wildcard fields to specify a range of IP addresses using a wildcard subnet mask in dotted decimal notation (such as 0.0.0.255 for /24).

c. If you want to match Microsoft RPC traffic that uses dynamic port allocation, choose the RPC application identifier from the Protocol drop-down list. For example, to match Microsoft Exchange Server traffic that uses the MAPI protocol, choose **mapi**.

d. Click **Save** to save the match condition.

e. Add additional match conditions as needed and click **OK** to save the class map and return to the class maps list. If any one of the conditions is matched, the class is considered matched.

Step 8 (Optional) For a Site class map type, select one or more peer devices. Follow these steps to create the class map:

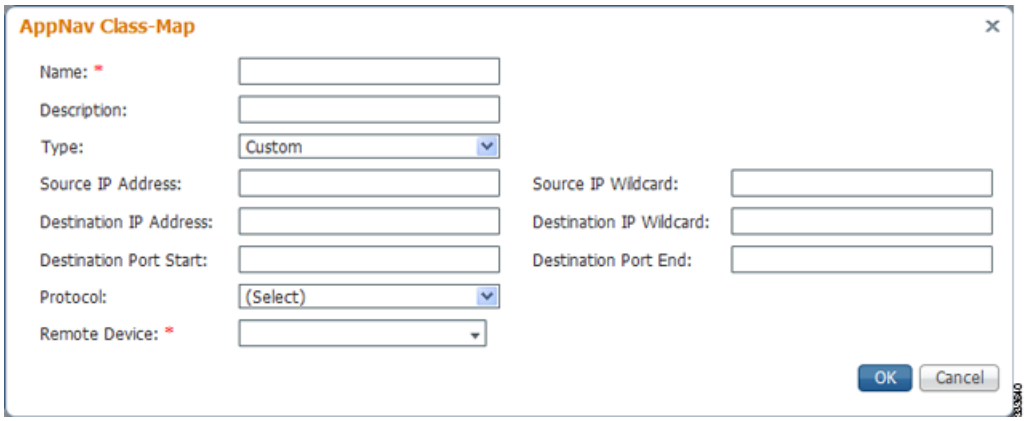


a. Use the filter settings in the Show drop-down list to filter the device list as needed. You can use a quick filter, show all devices, or show all assigned devices.

b. Check the box next to each device that you want to match traffic from. You can check the box next to the column titles to select all devices and uncheck it to deselect all devices. If any one of the selected devices is matched, the class is considered matched.

c. Click **OK** to save the class map and return to the class maps list.

Step 9 (Optional) For a Custom class map type, you must enter one match condition based on IP address/port or Microsoft RPC application ID and you must choose one WAAS peer device. All specified matching criteria must be satisfied for the class to be considered matched. Follow these steps to create the class map:



a. Enter values in one or more IP address and/or port fields to create a condition for a specific type of traffic. For example, to match all traffic going to ports 5405–5407, enter **5405** in the Destination Port Start field and **5407** in the Destination Port End field. You can use the IP address wildcard fields to specify a range of IP addresses using a wildcard subnet mask in dotted decimal notation (such as 0.0.0.255 for /24).

b. (Optional) If you want to match Microsoft RPC traffic that uses dynamic port allocation, choose the RPC application identifier from the Protocol drop-down list. For example, to match Microsoft Exchange Server traffic that uses the MAPI protocol, choose **mapi**.

c. You must choose one WAAS peer device from the Remote Device drop-down list.

d. Click **OK** to save the class map and return to the class maps configuration window.

Configuring Rules Within an AppNav Policy

To configure rules in an AppNav policy, follow these steps:

Step 1 From the WAAS Central Manager menu, choose **AppNav Clusters** > *cluster-name*.

Step 2 Choose **Configure** > **AppNav Cluster** > **AppNav Policies**.

The AppNav Policy window appears.

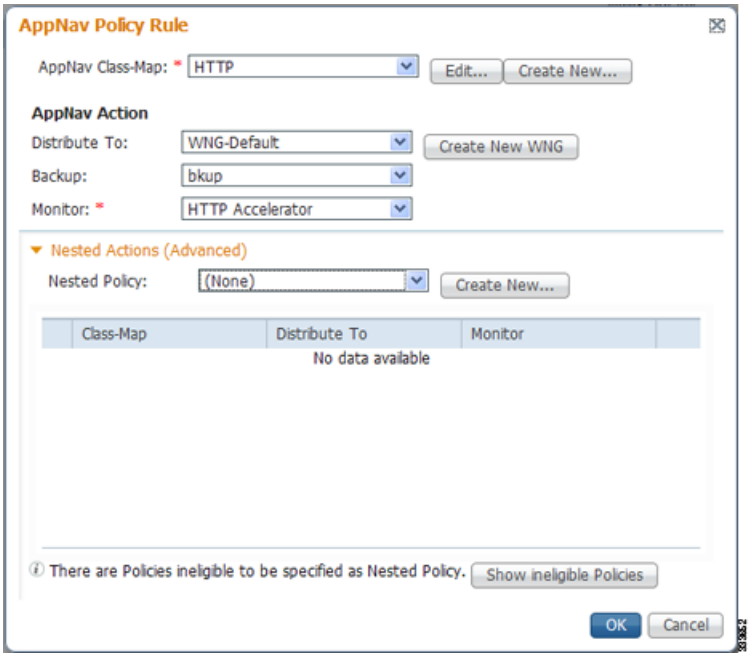
Step 3 Choose the policy to configure from the **AppNav Policy** drop-down list at the top.

You can click **Manage** to create or delete a policy or configure the ANCs to which a policy is applied. For details see the "Managing AppNav Policies" section on page 4-24.

From the AppNav Policy Rules area, you can perform the following tasks:

- Use the filter settings in the Show drop-down list to filter the rule list as needed. You can use a quick filter or show all rules.
- Edit a rule by selecting it and clicking the **Edit** taskbar icon.
- Delete one or more rules by selecting them and clicking the **Delete** taskbar icon.
- Move one or more selected rules to a new position by clicking the **Move To** taskbar icon. After moving the rows, click **Save Moved Rows** to save the change.
- Move one or more selected rules up or down one position by clicking the **Up** or **Down Arrow** taskbar icons, then click **Save Moved Rows** to save the change.
- Save rows that you have moved with the Move To or Up and Down Arrow functions by clicking the **Save Moved Rows** taskbar icon.
- Insert a new rule before the selected row by clicking the **Insert** taskbar icon. The workflow for inserting is the same as for adding (described in the following steps).
- Add a new rule at the end of the list as described in the steps that follow. (The class-default rule is always pushed to the last position.)

Step 4 Click the **Add Policy Rule** taskbar icon.



Step 5 From the AppNav Class-Map drop-down list, choose the class map to which this policy rule applies.

If you want to edit the class map, click **Edit**, or if you want to create a new class map, click **Create New**. The workflow is the same as described in the "Configuring AppNav Class Maps" section on page 4-19.

Step 6 From the Distribute To drop-down list, choose the distribution action to apply to the class map. The list includes all defined WNGs and the choices (None), for no action, and (Passthrough), to pass through this type of traffic. The meaning of (None) is context dependent: in a top level policy it means pass through and if this policy is nested, it means inherit the parent policy rule action.

When you choose a WNG, other settings appear. If you want create a new WNG, click **Create New**. The workflow is the same as described in the "Adding a New WAAS Node Group to the Cluster" section on page 4-34. The newly created WNG appears in both the Distribute To and Backup drop-down lists.

Step 7 (Optional) From the Backup drop-down list, choose the backup WNG to use for distribution if the primary WNG is unavailable.

Step 8 (Optional) From the Monitor drop-down list, choose the application accelerator to monitor. When you monitor an application accelerator, the ANC checks for overload on that application accelerator and does not send new flows to a WN that is overloaded. If you choose None, a specific application accelerator is not monitored, only the maximum connection limit of the device is monitored.

Step 9 (Optional) If you want to apply a nested policy within this rule, click **Nested Actions (Advanced)** to expand this area.

Step 10 (Optional) From the Nested Policy drop-down list, choose the policy to nest, or choose **None** to select no policy. When you choose a policy, the policy rules are displayed in a table.

If there are policies that are ineligible to be specified as a nested policy, click **Show Ineligible Policies** to display them and the reasons they are ineligible. A policy is ineligible if it already has a nested policy, because only one level of nesting is allowed.

To edit the chosen policy, click **Edit**, or to create a new policy for nesting, click **Create New**. The workflow for both editing and creating is the same.

a. In the Name field enter the policy name. This field is not editable for the waas_app_default policy.

b. Click the **Add Policy Rule** taskbar icon.

   A new row is added, showing fields for configuring the rule.

c. From the Class-Map drop-down list, choose the class map to which this rule applies.

d. From the Distribute To drop-down list, choose the distribution action to apply to the class map. The list includes all defined WNGs and the choices (Inherit), to inherit this action from the parent policy, and (Passthrough), to pass through this type of traffic.

e. (Optional) From the Backup drop-down list, choose the backup WNG to use for distribution if the primary WNG is unavailable.

f. (Optional) From the Monitor drop-down list, choose the application accelerator to monitor.

g. Click **OK** to save the policy rule and return to the AppNav Policy Rule pane for the primary policy rule you are creating.

Step 11 Click **OK** to create the policy rule and return to the policy configuration window.

Note If all AppNav policies have been deleted and you add a new policy rule, the policy rule is added to a new appnav_default policy, which is created automatically.

Managing AppNav Policies

To create or delete AppNav policies or configure the ANCs to which policies apply, follow these steps:

Step 1 From the WAAS Central Manager menu, choose **AppNav Clusters** > *cluster-name*.

Step 2 Choose **Configure** > **AppNav Cluster** > **AppNav Policies**.

The AppNav Policy window appears.

Step 3 Choose the policy to view from the AppNav Policy drop-down list at the top.

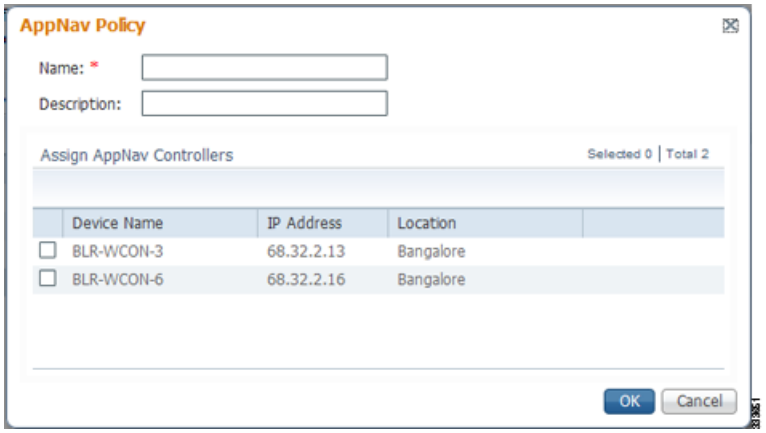
For details on using the AppNav Policy Rules area see the "Configuring Rules Within an AppNav Policy" section on page 4-22.

Step 4 Click **Manage**.

From the Manage AppNav Policies pane, you can perform the following tasks:

- Use the filter settings in the Show drop-down list to filter the policy list as needed. You can use a quick filter or show all policies.
- Edit a policy and configure the ANCs to which it applies by selecting it and clicking the **Edit** taskbar icon.
- Delete a policy by selecting it and clicking the **Delete** taskbar icon.
- Add a new policy as described in the steps that follow.

Step 5 Click the **Add Policy** taskbar icon.



Step 6 In the Name field enter a name for the policy.

Step 7 (Optional) In the Description field enter a description for the policy.

Step 8 (Optional) Check the box next to each ANC that you want to assign to this policy. To unassign any assigned devices, uncheck the box.

Assigning the policy to an ANC makes the policy active on that ANC (only one policy can be active on an ANC) and removes the association of any previously active policy on that ANC. It is not necessary to assign the policy to an ANC if you want to create the policy as an alternate. You can assign it to ANCs later as needed.

Step 9 Click **OK** to save the policy and return to the Manage AppNav Policies pane.

Step 10 Click **Close** to return to the policy configuration window.

Step 11 Add policy rules to the new policy as described in the "Configuring Rules Within an AppNav Policy" section on page 4-22.

Configuring WAAS Node Optimization Policy

The WAAS node optimization policy controls how traffic that is distributed to the WAAS nodes is optimized. The optimization policy is configured on the WNs and any ANCs that are also acting as optimizing nodes.

All WNs in one WNG must have an identical optimization policy configured on them. Otherwise, optimization of flows is not predictable. The optimization policy can be different for different WNGs.

For information on how to configure the optimization policy, see Chapter 13, "Configuring Application Acceleration."

The default optimization policy is listed in Appendix A, "Predefined Optimization Policy."

Configuring AppNav Controller ACLs

An AppNav Controller ACL controls what traffic is intercepted by an ANC. You may want to configure an ANC interception ACL for each ANC in an AppNav Cluster.

For information on how to configure an ANC interception ACL, see the "Configuring Interception Access Control Lists" section on page 5-28.

Configuring AppNav Cluster Settings

To configure AppNav Cluster settings, follow these steps:

Step 1 From the WAAS Central Manager menu, choose **AppNav Clusters > All AppNav Clusters**.

The Manage AppNav Clusters window appears, which shows the status of each cluster.

From this window, you can perform the following tasks:

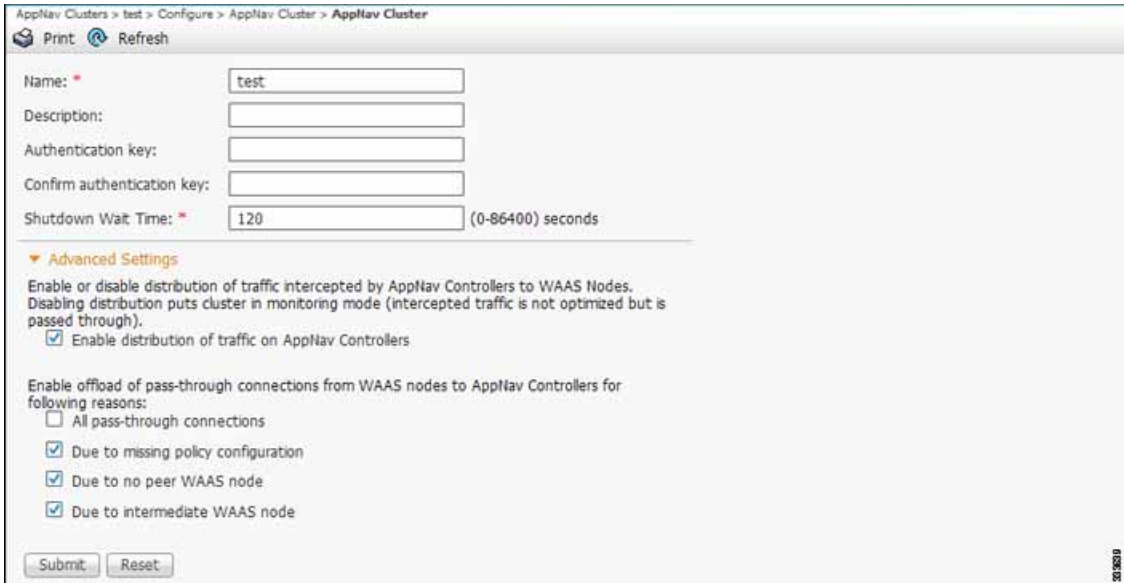
- View an AppNav Cluster topology and edit its settings by clicking on a cluster name.
- Delete an AppNav Cluster by selecting an AppNav Cluster and clicking the **Delete** icon in the taskbar of the Manage AppNav Clusters area.
- Create a new AppNav Cluster as described in the steps that follow.

Step 2 Click the name of the cluster whose settings you want to edit.

The cluster topology diagram appears.

Step 3 Choose **Configure > AppNav Cluster > AppNav Cluster**.

The Cluster Configuration window appears.



Step 4 In the Name field, enter a new name for the cluster if you want to rename it.

Step 5 (Optional) In the Description field, enter the cluster description. Use only letters and numbers, up to a maximum of 200 characters.

Step 6 (Optional) In the Authentication Key and Confirm Authentication Key fields, enter an authentication key that is used to authenticate communications between the WAAS devices in the cluster. Use only letters and numbers, up to a maximum of 64 characters.

Step 7 (Optional) In the Shutdown Wait Time field, enter the number of seconds that WNs in the cluster should wait for all connections to terminate before shutting down. The default is 120 seconds.

Step 8 (Optional) To configure cluster distribution and off-loading of pass-through connections, expand the **Advanced Settings** section by clicking it.

Step 9 (Optional) To enable distribution of traffic from the ANCs in the cluster to WNs, ensure that the **Enable distribution of traffic on AppNav Controllers** check box is checked. To disable distribution of traffic, uncheck this box. When distribution is disabled, the cluster operates in monitoring mode where it continues to intercept traffic and, instead of distributing it to WNs, passes it through. This mode can be useful for monitoring traffic statistics without optimizing the traffic.

Step 10 (Optional) To configure offloading of pass-through connections from WNs to ANCs, check the check boxes in the **Enable offload of pass-through connections from WAAS nodes to AppNav Controllers for following reasons** section. This feature allows pass-through connections to be passed through at the ANC instead of being distributed to the WN and then passed-through. Configure pass-through offload as follows:

a. To offload all pass-through connections, which includes connections passed through due to error conditions, check the **All pass-through connections** check box. Check this box only if you do not need application visibility on the WNs into pass-through traffic due to error conditions. The default is unchecked.

b. To offload connections passed through due to missing policy configuration, check the **Due to missing policy configuration** check box. The default is checked.

c. To offload connections passed through due to no peer WN, check the **Due to no peer WAAS node** check box. The default is checked.

d. To offload connections passed through due to an intermediate WN, check the **Due to intermediate WAAS node** check box. The default is checked.

e. If some of the WNs use different pass-through offload settings, you can synchronize the settings on all WNs to match the configuration shown here by checking the **Synchronize settings on all devices** check box. This check box is shown only if the settings on some WNs are different. The default is unchecked.

Step 11 Click **Submit**.

The lower part of this window shows lists of the ANCs, WNs, and WNGs that are part of the cluster. The controls in these parts of this window work as described in the following sections:

- AppNav Controllers—Configuring AppNav Controller Settings, page 4-28
- WAAS Nodes—Configuring WAAS Node Settings, page 4-29
- WAAS Node Groups—Configuring WAAS Node Group Settings, page 4-30

Configuring AppNav Controller Settings

To configure ANC settings, follow these steps:

Step 1 From the WAAS Central Manager menu, choose **AppNav Clusters** > *cluster-name*.

Step 2 Click the **AppNav Controllers** tab below the topology diagram.

All ANCs in the cluster are listed, showing the name, location, IP address, interface used for intra-cluster traffic, and enabled status.

From this list, you can perform the following tasks:

- Edit the interface settings for an ANC by choosing the ANC and clicking the **Edit** taskbar icon.
- Delete an ANC by choosing the ANC and clicking the **Delete** taskbar icon.
- Add a new ANC to the cluster by clicking the **Add AppNav Controller** taskbar icon. See the "Adding an ANC to a Cluster" section on page 4-31.
- Enable a disabled ANC by choosing the cluster and clicking the **Enable** taskbar icon.
- Disable an ANC by choosing the ANC and clicking the **Disable** taskbar icon.

Step 3 Click the radio button next to the ANC that you want to edit and click the **Edit** taskbar icon.

The Edit AppNav Controller pane appears.

Step 4 If you want to enable optimization on the ANC, check the **Enable WAN optimization (Internal WAAS Node)** check box.

Step 5 If you enabled WAN optimization, from the **WAAS Node Group** drop-down list, choose the WNG to which the internal WN should belong.

Step 6 Click **Next**.

Step 7 (Optional) Configure the WCCP settings for the ANC. This screen does not appear if the ANC is configured for inline interception. For more information on the WCCP fields, see the "Configuring or Viewing the WCCP Settings on ANCs" section on page 5-22.

When finished with the WCCP settings, click **Next**. The graphical interface wizard appears.

Step 8 In the graphical interface view, configure interfaces on the AppNav Controller Interface Module as needed. For details on how to use the wizard, see the "Configuring Interfaces with the Graphical Interface Wizard" section on page 4-17.

Step 9 From the Cluster Interface drop-down list, select the interface to be used for intra-cluster traffic.

Step 10 (Optional) To enable swapping of client and WAAS device source IP address fields in intra-cluster traffic, check the **Enable swapping of source IP address in intra-cluster traffic** check box.

You may want to enable this option if you are using a port channel for the cluster interface or there is a load balancing device between the ANC and WN. This option may improve the load balancing of traffic that the ANC distributes to WNs for optimization because it load balances based on the client IP address rather than the ANC IP address. (For traffic from the server to the client, it swaps the server IP address with the ANC IP address.) The Central Manager enables this feature automatically if any existing ANCs have port channel cluster interfaces.

Step 11 Click **Finish**.

Configuring WAAS Node Settings

All WNs in the cluster must be configured with application-accelerator device mode and appnav-controller interception mode. If you created the cluster with the Central Manager AppNav Wizard, both of these settings are already done. (The wizard sets the interception mode and the device mode would have been set before running the wizard.)

From within the AppNav Cluster context, you can configure the following settings for a WN:

- WNG to which the WN belongs
- AppNav Controller Interface Module interface settings (including configuring port channel, standby, and bridge group interfaces)
- Choose the cluster interface used for intra-cluster traffic

To configure WN settings, follow these steps:

Step 1 From the WAAS Central Manager menu, choose **AppNav Clusters** > *cluster-name*.

Step 2 Click the **WAAS Nodes** tab below the topology diagram.

All WNs in the cluster are listed, showing the name, location, IP address, interface in use, WNG to which the node belongs, and enabled status.

From this list, you can perform the following tasks:

- Edit the settings for a WN by choosing the WN and clicking the **Edit** taskbar icon.
- Delete a WN by choosing the WN and clicking the **Delete** taskbar icon.
- Add a new WN to the cluster by clicking the **Add WAAS Node** taskbar icon. See the "Adding a New WAAS Node to the Cluster" section on page 4-32.
- Enable a disabled WN by choosing the node and clicking the **Enable** taskbar icon.
- Disable a WN by choosing the node and clicking the **Disable** taskbar icon.

Step 3 Click the radio button next to the WN that you want to edit and click the **Edit** taskbar icon.

The WAAS Node pane appears.

Step 4 From the WAAS Node Group drop-down list, choose the WNG to which you want to assign the node.

Step 5 In the graphical interface view, configure interfaces on the AppNav Controller Interface Module as needed. For details on how to use the wizard, see the "Configuring Interfaces with the Graphical Interface Wizard" section on page 4-17.

Step 6 From the Cluster Interface drop-down list, select the interface to be used for intra-cluster traffic.

Step 7 (Optional) To enable swapping of client and WAAS device source IP address fields in intra-cluster traffic, check the **Enable swapping of source IP address in intra-cluster traffic** check box.

You may want to enable this option if you are using a port channel for the cluster interface or there is a load balancing device between the ANC and WN. This option may improve the load balancing of traffic that the ANC distributes to WNs for optimization because it load balances based on the client IP address rather than the ANC IP address. (For traffic from the server to the client, it swaps the server IP address with the ANC IP address.) The Central Manager enables this feature automatically if any existing ANCs have port channel cluster interfaces.

Step 8 Click **OK** to save the settings.

Configuring WAAS Node Group Settings

To configure WNG settings, follow these steps:

Step 1 From the WAAS Central Manager menu, choose **AppNav Clusters** > *cluster-name*.

Step 2 Click the **WAAS Node Groups** tab below the topology diagram.

All WNGs in the cluster are listed, showing the name, description, and the WNs contained in the group.

From this list, you can perform the following tasks:

- Edit the settings for a WNG by choosing the WNG and clicking the **Edit** taskbar icon.
- Delete a WNG by choosing the WNG and clicking the **Delete** taskbar icon.
- Add a new WNG to the cluster by clicking the **Add WAAS Node Group** taskbar icon. See the "Adding a New WAAS Node Group to the Cluster" section on page 4-34.

Step 3 Click the radio button next to the WNG that you want to edit and click the **Edit** taskbar icon.

Step 4 (Optional) In the Description field, enter a description of the WNG.

Step 5 Click **Save** to save the settings.

Adding and Removing Devices from the AppNav Cluster

This section includes these topics:

Adding an ANC to a Cluster

To add a new ANC to an AppNav Cluster, follow these steps:

Step 1 Configure basic device and network settings on the new ANC, and ensure that the device mode is set to appnav-controller.

Step 2 From the WAAS Central Manager menu, choose **AppNav Clusters** > *cluster-name*.

Step 3 Click the **AppNav Controllers** tab below the topology diagram.

Step 4 Click the **Add AppNav Controller** taskbar icon.

The Add AppNav Controllers pane appears.

Step 5 Select one or more ANCs in the AppNav Controller device list by checking the check boxes next to the device names. You can use the filter settings in the taskbar to filter the device list.

If there are devices that are ineligible to join the cluster, you can click **Show Ineligible Devices** to see them and the reasons why they are ineligible. You can use the filter settings to filter the list.

Step 6 Click **Next**.

Step 7 Configure the interception method, policy, WCCP settings (if using WCCP interception), and interfaces for each ANC device you are adding:

a. From the Interception Method drop-down list, choose **WCCP** or **Inline**.

b. From the AppNav Policy-Map drop-down list, choose the AppNav policy to apply to the ANC.

c. (Optional) If you want to enable optimization on the ANC devices, check the **Enable WAN optimization (Internal WAAS Node)** check box.

d. (Optional) If you enabled WAN optimization, from the WAAS Node Group drop-down list, choose the WNG to which the internal WN should belong.

e. Click **Next**.

f. (Optional) If you chose WCCP interception, configure the WCCP settings on the WCCP settings pane that appears. For details on WCCP settings, see the "Configuring or Viewing the WCCP Settings on ANCs" section on page 5-22. Remember to check the **Enable WCCP Service** check box to enable WCCP.

g. If you configured WCCP settings, click **Next**.

h. Use the Cluster Interface Wizard graphical interface to configure the ANC interfaces. If you chose inline interception, you must configure a bridge group interface. For details on using this wizard, see the "Configuring Interfaces with the Graphical Interface Wizard" section on page 4-17.

i. From the Cluster Interface drop-down list, select the interface to be used for intra-cluster traffic.

j. (Optional) To enable swapping of client and WAAS device source IP address fields in intra-cluster traffic, check the **Enable swapping of source IP address in intra-cluster traffic** check box.

You may want to enable this option if you are using a port channel for the cluster interface or there is a load balancing device between the ANC and WN. This option may improve the load balancing of traffic that the ANC distributes to WNs for optimization because it load balances based on the client IP address rather than the ANC IP address. (For traffic from the server to the client, it swaps the server IP address with the ANC IP address.) The Central Manager enables this feature automatically if any existing ANCs have port channel cluster interfaces.

k. Click **Next** to save the settings and continue with the next ANC you are adding. If this is the last ANC being added, click **Finish**.

After a convergence waiting period of up to two minutes, the new ANCs are available in the cluster for traffic interception and distribution. Traffic interception on the new ANCs is prevented until the devices have fully joined the cluster. You can monitor the ANC status as described in the "Monitoring an AppNav Cluster" section on page 4-34.

Removing an ANC from a Cluster

To gracefully remove an ANC from an AppNav Cluster, follow these steps:

Step 1 Disable the traffic interception path on the ANC. For an inline ANC, shut down the in-path interfaces, and for an ANC using WCCP, disable WCCP.

Traffic previously routed to this ANC is rerouted to other ANCs in the cluster.

Step 2 Disable the ANC:

a. From the WAAS Central Manager menu, choose **AppNav Clusters** > *cluster-name*.

b. Click the **AppNav Controllers** tab below the topology diagram.

c. Click the radio button next to the ANC that you want to disable and then click the **Disable** taskbar icon.

The ANC is disabled and the service unreachable alarm is raised on the other ANCs in the cluster.

Step 3 (Optional) To permanently remove the ANC, click the radio button next to the ANC that you want to remove and then click the **Delete** taskbar icon.

This action removes the ANC from the ANCG on all other ANCs and clears the service unreachable alarm on the other ANCs. If the ANC is configured for WCCP interception, all WCCP settings on the device are removed. If the ANC is also configured as a WN, the WN is removed from the cluster.

Step 4 (Optional) Power down the ANC.

Adding a New WAAS Node to the Cluster

To add a new WAAS node (WN) to a cluster, follow these steps:

Step 1 From the WAAS Central Manager menu, choose **AppNav Clusters** > *cluster-name*.

Step 2 Click the **WAAS Nodes** tab below the topology diagram.

Step 3 Click the **Add WAAS Node** taskbar icon.

The Add WAAS Nodes pane appears.

Step 4 Select one or more WNs in the WAAS Nodes device list by checking the check boxes next to the device names. You can use the filter settings in the taskbar to filter the device list.

If there are devices that are ineligible to join the cluster, click **Show Ineligible Devices** to see them and the reasons why they are ineligible. You can use the filter settings to filter the list.

Step 5 Click **Next**.

Step 6 Configure the WNG and interfaces for each WN device you are adding.

a. From the WAAS Node Group drop-down list, choose the WNG to which you want to add the new WNs. The list shows defined WNGs.

b. Click **Next**.

c. Use the Cluster Interface Wizard graphical interface to configure the WN interfaces. For details on using this wizard, see the "Configuring Interfaces with the Graphical Interface Wizard" section on page 4-17.

d. From the Cluster Interface drop-down list, select the interface to be used for intra-cluster traffic.

e. (Optional) To enable swapping of client and WAAS device source IP address fields in intra-cluster traffic, check the **Enable swapping of source IP address in intra-cluster traffic** check box.

You may want to enable this option if you are using a port channel for the cluster interface or there is a load balancing device between the ANC and WN. This option may improve the load balancing of traffic that the ANC distributes to WNs for optimization because it load balances based on the client IP address rather than the ANC IP address. (For traffic from the server to the client, it swaps the server IP address with the ANC IP address.) The Central Manager enables this feature automatically if any existing ANCs have port channel cluster interfaces.

f. Click **Next** to save the settings and continue with the next WN you are adding. If this is the last WN being added, click **Finish**.

Step 7 Configure and enable optimization on the WNs. For details on configuring optimization, see Chapter 13, "Configuring Application Acceleration."

After a convergence waiting period of up to two minutes, the new WNs are available on all the ANCs for optimization.

Removing a WAAS Node from a Cluster

To remove a WAAS node (WN) from a cluster, follow these steps:

Step 1 From the WAAS Central Manager menu, choose **AppNav Clusters** > *cluster-name*.

Step 2 Click the **WAAS Nodes** tab below the topology diagram.

Step 3 Choose the node and click the **Disable** taskbar icon.

This causes a graceful exit of the WN from the cluster, where the ANCs stop sending new flows to the WN but continue to distribute existing flows to it until the connection count reaches zero or the maximum shutdown wait time expires.

Note The default shutdown wait time is 120 seconds. You can configure it from the Shutdown Wait Time field in the AppNav Cluster tab.

Step 4 (Optional) When the graceful exit process on the WN is complete (all existing connections have terminated), remove the WN from the WNG on the ANCs by choosing the node and clicking the **Delete** taskbar icon.

You can monitor the node status in the topology diagram in the upper part of the window. The colored status light indicator on the device turns gray when the node is no longer processing connections.

Step 5 (Optional) Power down the WN.

Adding a New WAAS Node Group to the Cluster

To add a new WNG to a cluster, follow these steps:

Step 1 From the WAAS Central Manager menu, choose **AppNav Clusters** > *cluster-name*.

Step 2 Click the **WAAS Node Groups** tab below the topology diagram.

Step 3 Click the **Add WAAS Node Group** taskbar icon.

The Add WAAS Node Group pane appears.

Step 4 In the Name field, enter the name of the WNG.

Step 5 (Optional) In the Description field, enter a description of the WNG.

Step 6 Click **OK** to save the settings.

Step 7 Add one or more WNs to the new WNG. To add a new WN, see the "Adding a New WAAS Node to the Cluster" section on page 4-32, or to reassign an existing WN to the new WNG, see the "Configuring WAAS Node Settings" section on page 4-29.

After a convergence waiting period of up to two minutes, the new WNG is available on all the ANCs for optimization.

Removing a WAAS Node Group from a Cluster

To remove a WAAS node group (WNG) from a cluster, follow these steps:

Step 1 From the WAAS Central Manager menu, choose **AppNav Clusters** > *cluster-name*.

Step 2 Click the **WAAS Nodes** tab below the topology diagram.

Step 3 For each WN in the WNG, click the radio button next to the node name and click the **Disable** taskbar icon. This causes a graceful exit of each WN from the cluster.

Step 4 After all WNs have completed a graceful exit from the cluster, click the **WAAS Node Groups** tab.

You can monitor the node status in the topology diagram in the upper part of the window. The colored status light indicator on a device turns gray when the node is no longer processing connections.

Step 5 (Optional) Choose the WNG you want to remove and click the **Delete** taskbar icon.

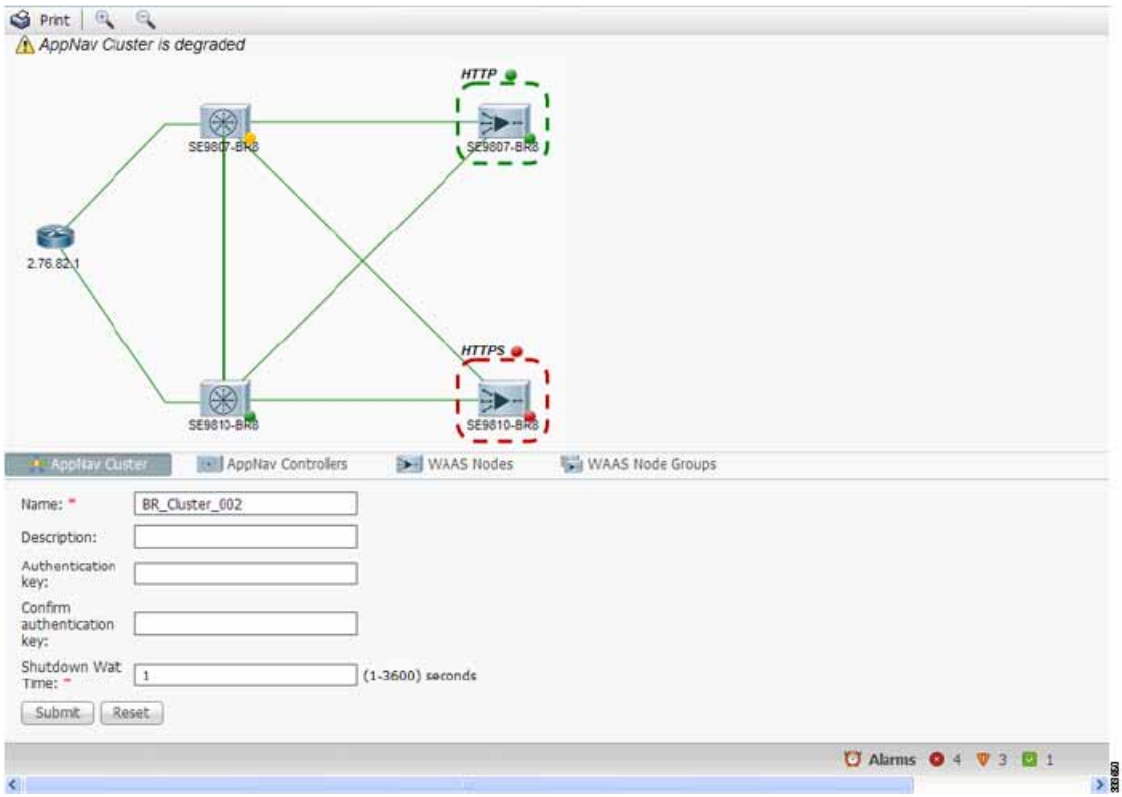
Monitoring an AppNav Cluster

To monitor an AppNav Cluster, follow these steps:

Step 1 From the WAAS Central Manager menu, choose **AppNav Clusters** > *cluster-name*.

The cluster home window displays the cluster topology and device status (see Figure 4-5).

Figure 4-5 AppNav Cluster Topology and Status



To zoom in or out on the topology diagram, click the + or – magnifying glass icons in the taskbar. You can also click on the diagram and drag it within the window to reposition it.

To change the cluster settings, edit any of the fields below the topology diagram and click **Submit**.

To see all ANCs, click the **AppNav Controllers** tab below the diagram. From this tab, you can edit, delete, add, enable, or disable an ANC in the cluster.

To see all WNs, click the **WAAS Nodes** tab below the diagram. From this tab, you can edit, delete, add, enable, or disable a WN in the cluster.

To see all WNGs, click the **WAAS Node Groups** tab below the diagram. From this tab, you can edit, delete, or add a WNG in the cluster.

The overall cluster status is shown in the top left corner of the diagram, as follows:

- Green—All ANCs are operational with no error conditions.
- Yellow—Degraded because one or more ANCs have operational issues. This is also the initial state before all nodes have sent status updates.
- Red—Cluster is down because all ANCs are down or indicates a split cluster where there is no connectivity between one or more ANCs.

The overall cluster status does not include administratively disabled ANCs.

The colored status light indicators on each device and dotted lines around each WNG show the status of the device or group:

- Green—Operational with no error conditions

- Yellow—Degraded (overloaded, joining cluster, or has other noncritical operational issues)
- Red—Critical (one or more processes is in a critical state)
- Gray—Disabled
- Black—Unknown status

The colored lines between each device show the status of the link between devices:

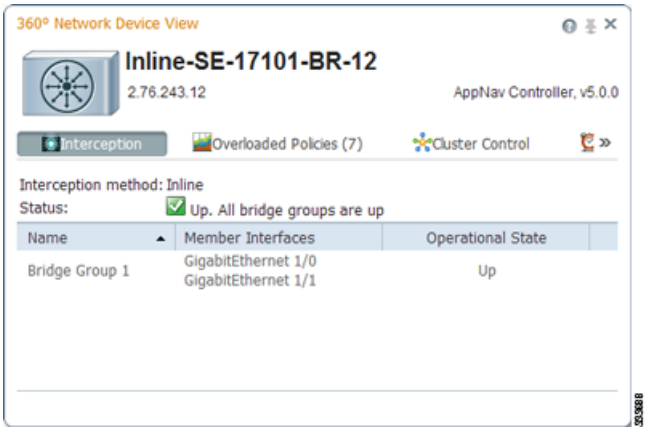
- Green—Operational with no error conditions
- Red—Link is down
- Black—Unknown status

An orange triangle warning indicator is shown on any device for which the Central Manager may not have current information because the device has not responded within the last 30 seconds (the device could be offline or unreachable).

Note A recently removed device still appears in the topology diagram for a few minutes until all devices agree on the new cluster topology.

To view a more comprehensive device status display, hover your cursor over a device icon to see the 360-degree Network Device View popup window (Figure 4-6). The popup window for a WN device is similar.

Figure 4-6 ANC 360-Degree Network Device View



The 360-degree Network Device View shows the following status information:

- Device name and IP address
- Device type and software version
- (ANC only) Interception tab that displays the interception method: Inline or WCCP. For inline, this tab shows the bridge groups defined for interception, their member interfaces, and their status. For WCCP, this tab lists the defined WCCP service IDs, their associated client IP addresses, router IP address, and notes about problems.
- (ANC only) Overloaded Policies tab that lists any monitored AppNav policies that are overloaded.
- (ANC only) Cluster Control tab that lists all devices in the cluster, with device name, IP address, service type, liveliness state, and reason for any error condition

- (WN only) Optimization tab that lists the application accelerators and their status
- Alarms tab that lists pending alarms on the device
- Interfaces tab that lists the device interfaces and status. You can filter the list by choosing a filter type from the drop-down list above the interface list, entering filter criteria, and clicking the filter icon.

You can pin the status popup window so it stays open by clicking the pin icon in the upper right corner. You can also drag the popup to any location within your browser window.

For additional cluster status, you can view the Monitor > AppNav > AppNav Report as described in the "AppNav Report" section on page 17-43.

If you have multiple AppNav Clusters, you can see brief status for all at once by choosing **AppNav Clusters > All AppNav Clusters** from the menu.

To trace connections, see the "AppNav Connection Tracing" section on page 4-37.

Note You may see a taskbar icon named Force Settings on all Devices in a Group if the configuration across all ANCs in the cluster becomes unsynchronized. If you see the icon, the cluster settings, ANC configuration, WN configuration, and WNG configuration do not match on all ANCs in the cluster. This problem can occur if you configure a device outside the Central Manager by using the CLI. Click this taskbar icon to update all devices with the configuration that is currently shown in the Central Manager for the cluster.

AppNav Connection Tracing

To assist in troubleshooting AppNav flows, you can use the Connection Trace tool in the Central Manager. This tool shows the following information for a particular connection:

- If the connection was passed through or distributed to a WNG
- Pass-through reason, if applicable
- The WNG and WN to which the connection was distributed
- Accelerator monitored for the connection
- Class-map applied

To use the Connection Trace tool, follow these steps:

Step 1 From the WAAS Central Manager menu, choose **AppNav Clusters >** *cluster-name*.

Step 2 Choose **Monitor > Tools > Connection Trace**.

Step 3 In the AppNav Controller drop-down list, choose the ANC that has the connection you want to trace.

Step 4 From the Site (Remote Device) drop-down list, choose the peer WAAS device at the remote site.

Step 5 In one or more of the Source IP, Source Port, Destination IP, and Destination Port fields, enter matching criteria for one or more connections.

Step 6 Click **Trace** to display the connections that match the IP address and port criteria.

Connections are displayed in the Connection Tracing Results table below the fields. Use the filter settings in the Show drop-down list to filter the connections as needed. You can use a quick filter to filter on any value or show all connections.

You can display flow distribution information from the CLI by using the **show appnav-controller flow-distribution** EXEC command.

Another troubleshooting tool that you can use to trace connections is the WAAS Tcptraceroute tool. For details, see the "Using WAAS TCP Traceroute" section on page 17-61.