Cisco Wide Area Application Services (WAAS) Software Version 4.2 for Inline Topologies

Deployment Guide

Contents

Cisco Wide Area Application Services (WAAS)

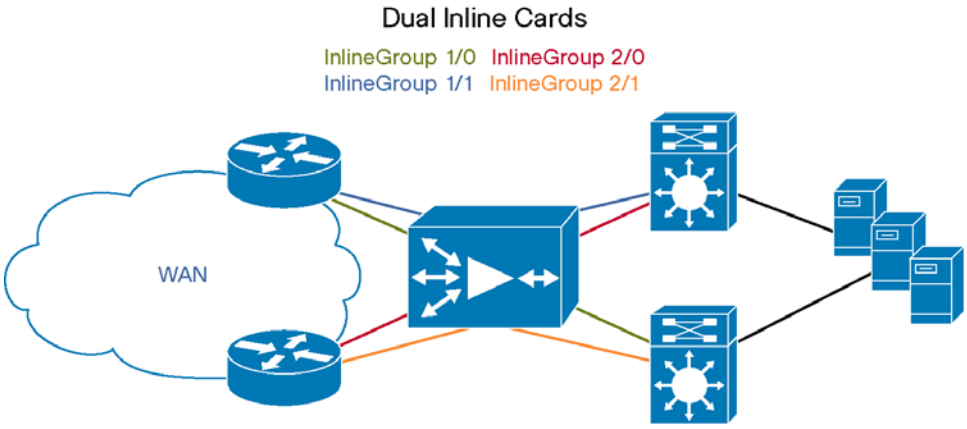
What You Will Learn

With Cisco® Wide Area Application Services (WAAS) Software Version 4.2, Cisco has enhanced features for inline deployments to enable advanced implementation of WAN optimization with the widest possible choices. Coupled with award-winning Cisco global support and advanced services, Cisco WAAS gives customers a significant set of resources to help ensure full network integration while reducing maintenance costs and deployment time. This document discusses the advanced features in Cisco WAAS 4.2 that further enhance inline deployments.

Dual Inline Card Support

Cisco WAAS 4.2 adds the capability to support multiple inline devices, enabling further scalability of inline intercepted links, and additional routing paths for asymmetric interception. Figure 1 shows a single Cisco WAAS device connected to two routers on the WAN side and two switches on the LAN side.

Figure 1. Dual Inline Card Connection



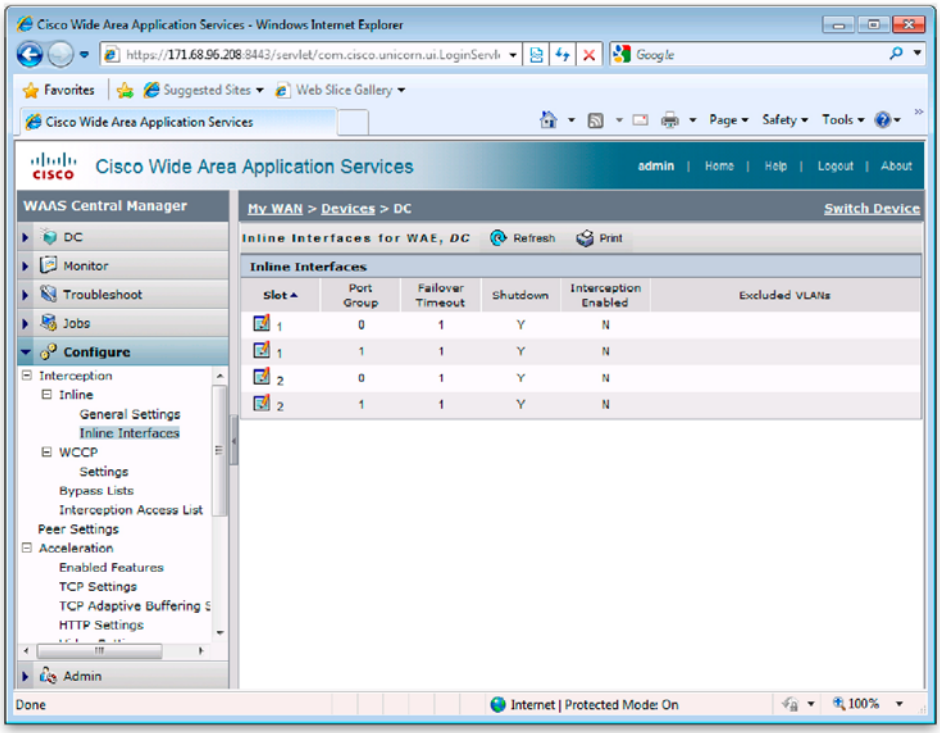
A maximum of two inline cards per device is supported, for a total of four inline port groups, or eight physical inline ports. Multiple inline cards are supported only on the Cisco WAE-674, WAE-7341, and WAE-7371 Wide Area Application Engine hardware.

Note: Dual inline cards are supported only on Cisco WAAS 4.2 or higher. Downgrading to an earlier release will require removal of the second inline card.

If the dual inline cards are not preinstalled, you will need to install one or both of the inline cards in the Cisco WAE device. For more information about adapter installation, see the Cisco WAE hardware installation guide for the Cisco WAE-7371, WAE-7341, and WAE-674.

After the adapters are installed, they will appear as Inline Group 1/0, 1/1, 2/0, and 2/1 (see Figure 2). These inline devices can then be configured using the same methods as for standard inline interfaces. For more information, please see the section "Using Inline Mode" in the Cisco WAAS configuration guide.

Figure 2. Inline Interface Menu

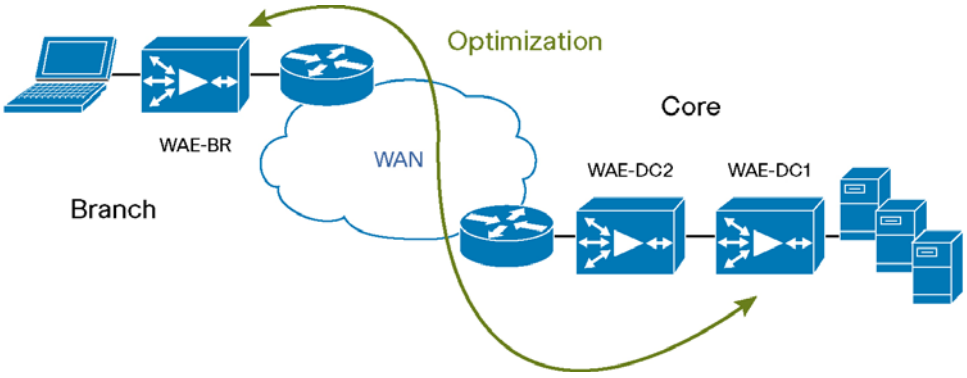


Serial Inline Clustering

Cisco WAAS 4.2 adds support for high-availability clustering with inline deployment. This feature enables flexible and redundant deployment for both data center and branch offices.

In a serial inline cluster, two Cisco WAAS devices are connected back to back through inline interfaces. Because of the autonegotiation capabilities inherent in Cisco WAAS, only the devices closest to the traffic endpoints participate in optimization. In the example shown in Figure 3, only WAE-BR and WAE-DC1 will optimize traffic. WAE-DC2 will pass through all traffic without optimizing and will optimize traffic only in the event of a failure on WAE-DC1.

Figure 3. Serial Inline Cluster



Serial inline clustering is designed for high-availability failover only. It is not designed to provide load balancing or a method for scaling traffic beyond the capacity of a single Cisco WAAS device. Because of the nature of the failure recovery built into serial inline clustering, some overflow sessions will be serviced by the redundant inline Cisco WAAS device. This overload capability is not recommended or supported. If traffic load balancing or scalability

beyond a single device is desired, you should use Web Cache Communication Protocol (WCCP) or a hardware load balancer such as Cisco Application Control Engine (ACE).

Note: When placing multiple Cisco WAAS devices in an inline configuration, you should not place more than two devices inline on the same local segment.

During operation of the serial inline cluster, all traffic will be optimized between the remote Cisco WAAS devices and the second device in from the WAN on the serial inline cluster. For example, in Figure 3 all optimization would happen between WAE-BR and WAE-DC1.

After a failure event occurs, all optimization shifts immediately from WAE-DC1 to WAE-DC2 in the serial inline cluster. If WAE-DC1 recovers, all new sessions will begin being optimized on WAE-DC1. Existing sessions will continue to be serviced by WAE-DC2 until those session time out.

Traffic passing through the intermediate device (WAE-DC2) will be classified as Pass-Through Intermediate (PT Intermediate). No optimization will be performed by this device except in the event of WAE-DC1 failure.

When you use serial inline clustering, each of the two Cisco WAAS devices in the cluster needs to be aware of its peer device and configured accordingly. This non-optimizing peer configuration allows the Cisco WAAS devices to disable optimization for traffic that transits only the two devices in the serial inline cluster. Traffic destined to sites with no Cisco WAAS peer device should automatically be set to Pass Through when transiting the serial inline cluster. Traffic to these sites will be classified as either no peer (PT No Peer) or non-optimizing peer (PT Non-optimizing Peer).

To configure non-optimizing peers for your serial inline cluster, follow these steps:

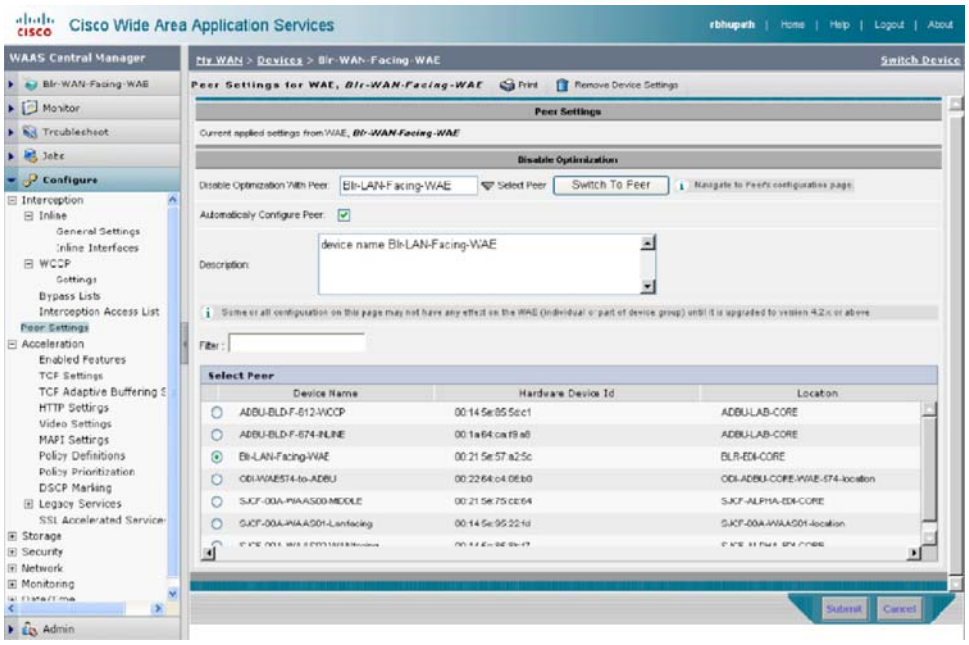
Step 1. From the Cisco WAAS Central Manager GUI navigation pane, choose **My WAN > Manage Devices**.

Note: You can specify peer settings only on individual Cisco WAAS devices, not on device configuration groups.

Step 2. Click the **Edit** icon next to the Cisco WAE device that you want to configure.

Step 3. From the navigation pane, choose **Configure > Interception > Peer Settings.** The Peer Settings window appears (Figure 4).

Figure 4. Peer Settings Window



Step 4. Ensure that the **Automatically Configure Peer** check box is checked. This setting synchronizes the peer device settings with those of the device currently being configured.

Note: If the **Automatically Configure Peer** check box is not checked, you will need to manually repeat these configuration steps on the peer device to include its partner device as a non-optimizing peer.

Step 5. Click the arrow ( ) next to **Select Peer.** This arrow expands the Select Peer box at the bottom of the page, which lists all possible device peers.

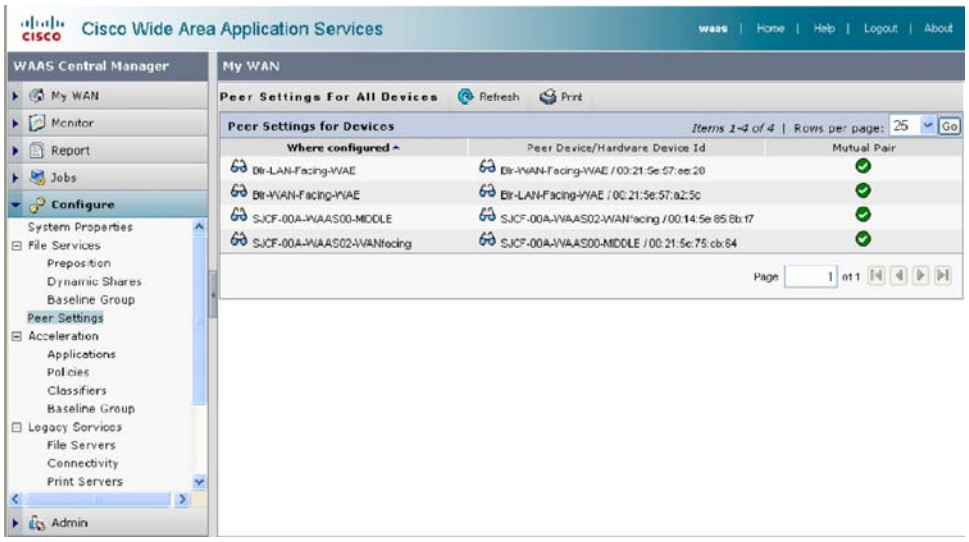
Step 6. Choose the appropriate peer in the **Select Peer** list at the bottom of the page. When selected, the peer name should appear in the **Disable Optimization With Peer** window.

Step 7. (Optional) Enter a description in the **Description** field. It is highly recommended that the description include the peer device name. By default, a description including the device name is provided.

Step 8. Click **Submit** to submit your changes.

Step 9. After the settings are configured, you can verify your peer settings using the global My WAN peer settings menu. Choose **My WAN > Configure > Peer Settings.** The My WAN Peer Settings page lists all devices with an inline peer configuration (Figure 5).

Figure 5. My WAN Peer Settings Window



If peers are configured correctly, each entry will have a green check mark ( ) in the **Mutual Peer** column. If a configuration mismatch occurs, no check boxes will be present. If a device is missing a green check box, remove or verify its peer configuration and verify that the configured peer has a matching configuration.

A mismatched peer configuration will also write notifications to any configured syslog service:

```
%WAAS-SYS-4-900000: AD: Serial Mode configuration mismatch with peer_id=00:21:5e:27:a8:80
```

Note: In the event of a full Cisco WAAS device replacement due to failure or other event, the device ID used by the non-optimized peer will change. This change will require reconfiguration of the peer settings to make serial inline clustering function correctly.

Location-Based Reporting

Cisco WAAS includes the capability to aggregate traffic and optimization statistics from multiple devices at a single location in a single report, by using location-based reporting.

Prior to Cisco WAAS 4.2, reports were scheduled and created using either device groups or single devices. Cisco WAAS 4.2 allows reports to be created and viewed using device locations as criteria. This capability enables simple statistics aggregation without the need to create and manage additional device groups. Location-based reporting is useful in locations with multiple Cisco WAAS devices, because a single device report may lack data from other devices in the inline or WCCP cluster.

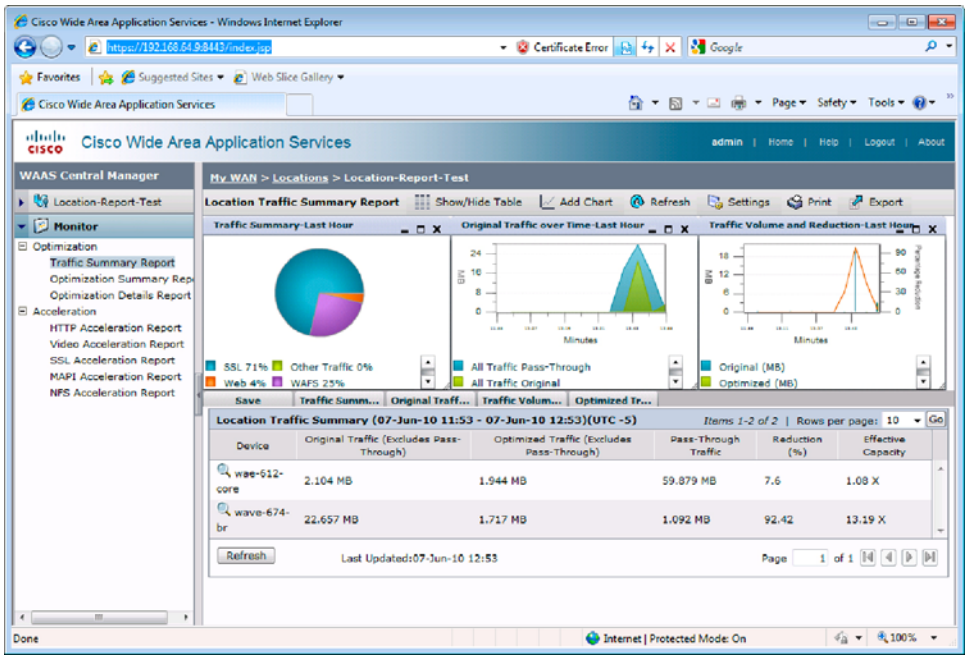
To view standard reports by location, perform the following steps:

Step 1. From the Cisco WAAS Central Manager GUI navigation pane, choose **My WAN > Manage Locations**.

Step 2. Click the **Edit** icon next to the Cisco WAE location that you want to configure.

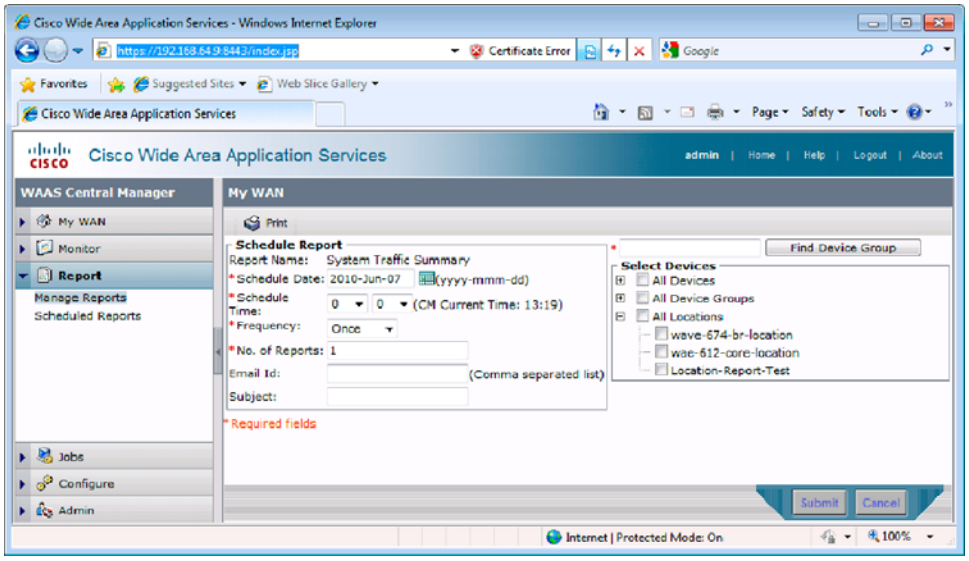
Step 3. From the navigation pane, choose **Monitor**. The location-based monitoring window appears (Figure 6). From here, you can view standard monitoring reports that contain statistics for all devices at the location.

Figure 6. Location-Based Monitoring



In addition to standard monitoring reports, location-based reporting can now be used for scheduled reporting. When creating a scheduled report, you now have the option of selecting device locations as participants in the report (Figure 7). For more information about scheduled reports, see the section "Scheduling Reports" in the Cisco WAAS configuration guide.

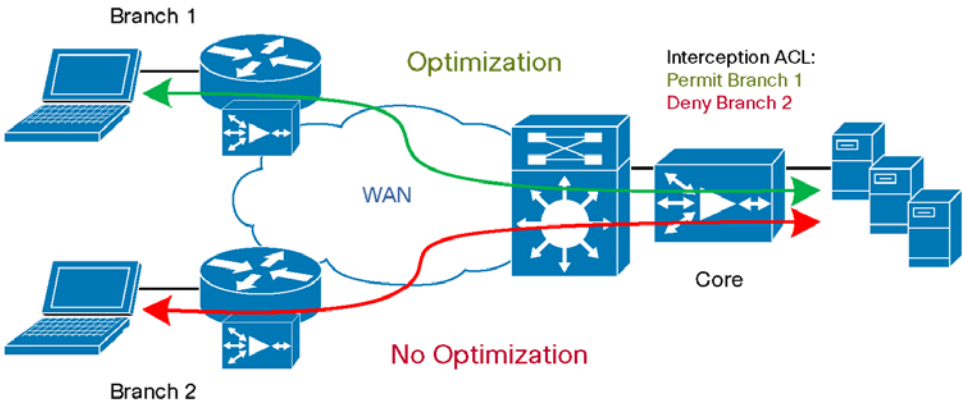
Figure 7. Scheduled Reports Window



Interception Access Control Lists

Interception access control lists (ACLs) allow an extra method of control to include or exclude traffic for optimization. These ACLs will be applied prior to any policy processing, and they offer a flexible tool for gradually introducing, excluding, or scaling optimization. In Figure 8, the ACL permits traffic from Branch 1 to be evaluated for optimization while it denies traffic from Branch 2.

Figure 8. Interception ACL



Interception ACLs are part of the Cisco WAAS IP ACL infrastructure. An IP ACL must first be created and then applied as an interception ACL. IP ACLs can be entered in standard Cisco IOS® Software ACL format through the command-line interface (CLI) of the Cisco WAE or through the Cisco WAAS Central Manager GUI.

Adding the IP ACLs

To add the IP ACLs in the Cisco WAAS Central Manger GUI, perform the following steps:

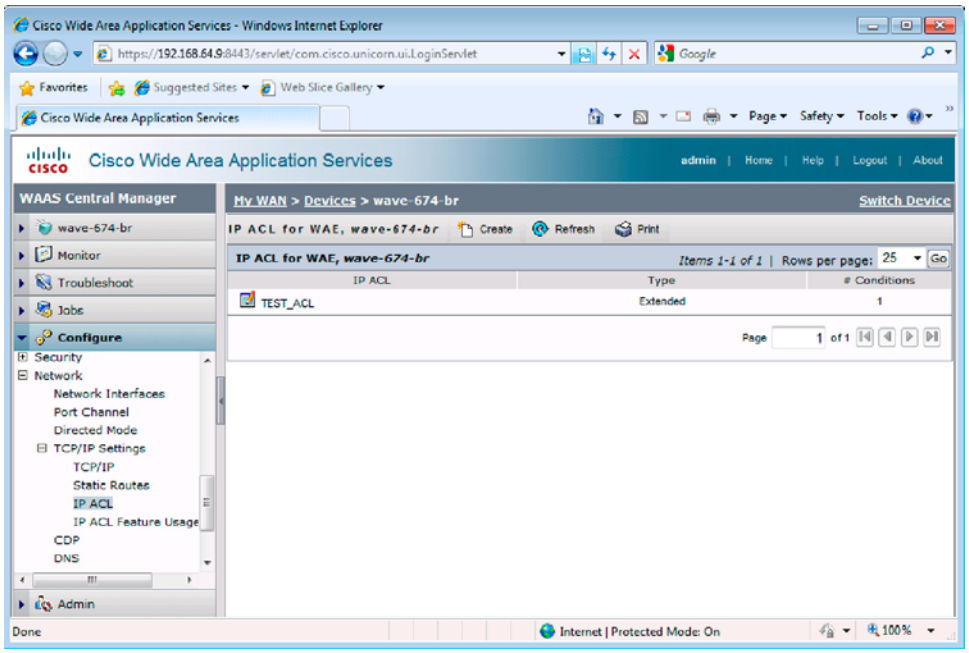
Step 1. From the Cisco WAAS Central Manager GUI navigation pane, choose **My WAN > Manage Devices**.

Step 2. Click the **Edit** icon next to the WAE device that you want to configure.

Note: You can configure IP ACLs only on individual Cisco WAAS devices, not device configuration groups.

Step 3. From the navigation pane, **choose Configure > Network > TCP/IP > IP ACL**. The IP ACL for WAE window appears (Figure 9).

Figure 9. IP ACL for WAE Window



Step 4. In the taskbar, click the **Create** icon.

The Creating New IP ACL window appears. Fill in the fields as follows:

a. In the Name field, enter a name (for example, TEST_ACL), observing the naming rules for IP ACLs.

By default, this new IP ACL is created as a standard ACL.

Note: IP ACL names must be unique within the device, must be limited to 30 characters, and cannot contain any white spaces or special characters.

b. If you want to change this default setting and create this new ACL as an extended ACL, choose **Extended** from the ACL Type drop-down list.

Step 5. Click **Submit** to save the IP ACL.

IP ACLs without any conditions defined do not appear on the individual devices. You will now need to add conditions to the IP ACL you created.

Step 6. Add conditions to the IP ACL:

a. In the taskbar, click the **Create New Condition** icon.

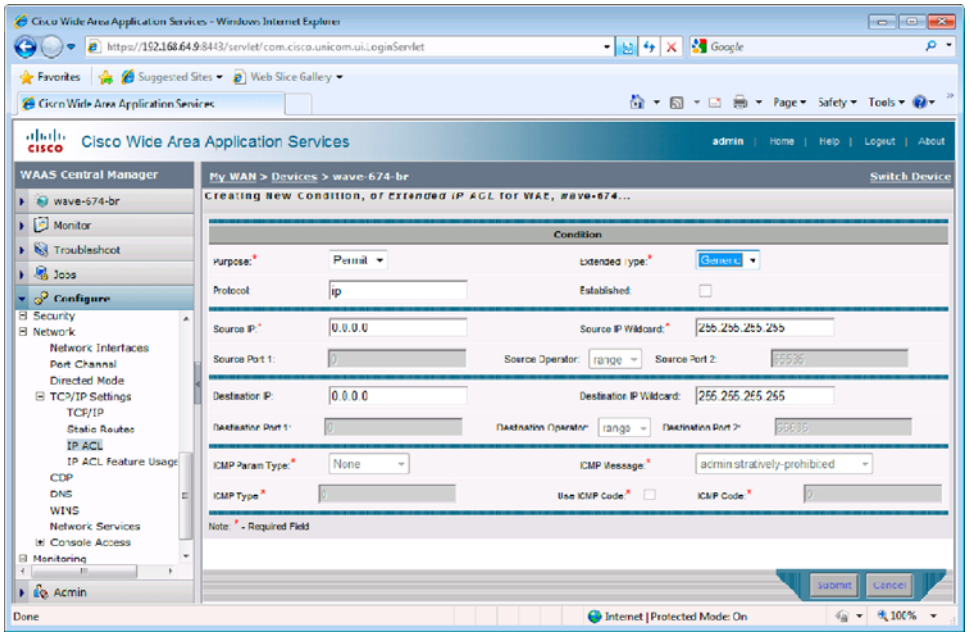
The Creating New Condition window appears (Figure 10).

Note: The number of available fields for creating IP ACL conditions depends on the type of IP ACL that you have created: either standard or extended.

b. Enter values for the properties that are enabled for the type of IP ACL that you are creating, as follows:

- To set up conditions for a standard IP ACL, go to Step 7.
- To set up conditions for an extended IP ACL, go to Step 8.

Figure 10. Creating New Condition Window



Step 7. To create a **Standard IP ACL**:

a. From the drop-down list, choose a purpose (**Permit** or **Deny**).

b. In the **Source IP** field, enter the source IP address.

c. In the **Source IP Wildcard** field, enter a source IP wildcard address.

d. Click **Submit** to save the condition.

The Modifying IP ACL window reappears, displaying the condition and its configured parameters in tabular format.

e. To add another condition to the IP ACL, repeat the steps.

f. To reorder your list of conditions from the Modifying IP ACL window, use the up and down arrows in the Move column, or click a column heading to sort by any configured parameter.

Note: The order of the conditions listed in the Cisco WAAS Central Manager GUI will be the order in which IP ACLs are applied to the device.

g. When you have finished adding conditions to the IP ACL and you are satisfied with all your entries and the order in which the conditions are listed, click **Submit** in the Modifying IP ACL window to commit the IP ACL to the device database.

Step 8. To create an **Extended IP ACL**:

a. From the drop-down list, choose a purpose (**Permit** or **Deny**).

b. From the **Extended Type** drop-down list, choose **Generic, TCP, UDP,** or **ICMP**.

After you choose a type of extended IP ACL, various options become available in the GUI, depending on what type you choose.

c. In the fields that are enabled for the chosen type, enter the appropriate data for each condition.

d. Click **Submit** to save the condition.

The Modifying IP ACL window reappears, displaying the condition and its configured parameters in tabular format.

e. To add another condition to the IP ACL, repeat the steps.

f. To reorder your list of conditions from the Modifying IP ACL window, use the up and down arrows in the **Move** column, or click a column heading to sort by any configured parameter.

Note: The order of the conditions listed in the Cisco WAAS Central Manager GUI will be the order in which IP ACLs are applied to the device.

g. When you have finished adding conditions to the IP ACL and you are satisfied with all your entries and the order in which the conditions are listed, click **Submit** in the Modifying IP ACL window to commit the IP ACL to the device database.

Setting an Interception ACL

After the appropriate IP ACLs have been added to the Cisco WAAS device, an ACL can be set as an interception ACL. To make an IP ACL an interception ACL in the Cisco WAAS Central Manager GUI, follow these steps:

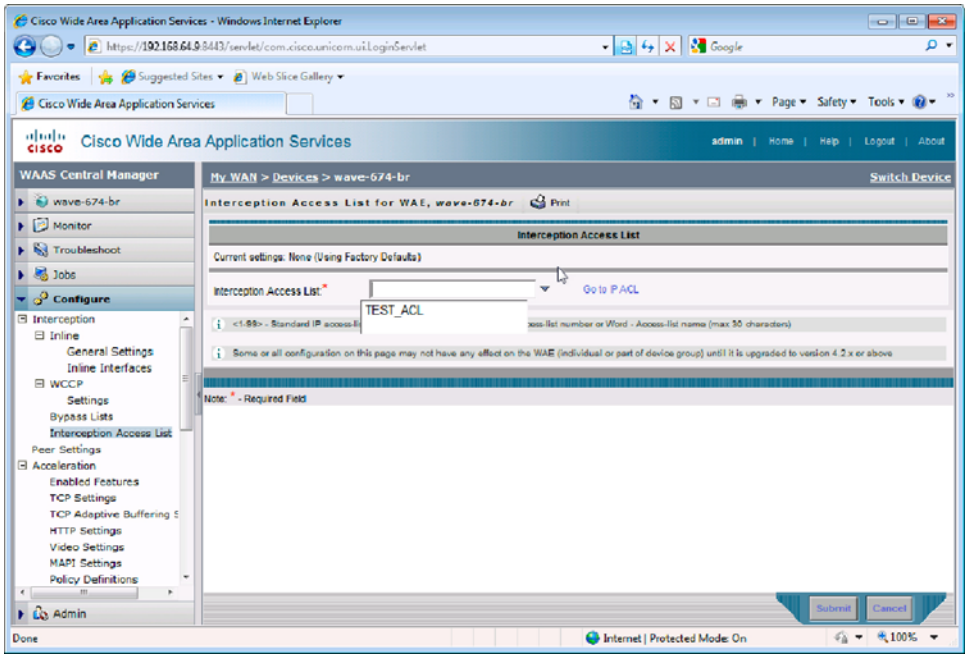
Step 1. From the Cisco WAAS Central Manager GUI navigation pane, choose **My WAN > Manage Devices.**

Step 2. Click the **Edit** icon next to the Cisco WAE device that you want to configure.

Note: Interception ACLs must be configured on individual Cisco WAAS devices, not device groups.

Step 3. From the navigation pane, choose **Configure > Interception > Interception Access List**. The Interception Access List for WAE window appears (Figure 11).

Figure 11. Interception Access List for WAE Window



Step 4. Click the arrow (▾) next to the **Interception Access List** field. This arrow displays a list of IP ACLs that are defined on the Cisco WAAS device.

Step 5. Select the appropriate IP ACL to be applied as an interception access list.

Step 6. Click **Submit** to apply the interception access list configuration.

If there are no IP ACLs, or if a new IP ACL is needed, click the **Go to IP ACL** link to go directly to the IP ACL creation window.

After the interception ACL is configured and submitted, the new ACL policy will be applied to all new sessions. Interception ACLs match only on the initial connection setup TCP SYN packet, thereby allowing current established sessions to finish uninterrupted.

Inline Deployment Best-Practice Recommendations

Cisco WAAS 4.2 adds several enhancements to the inline deployment and operation of a network that supports Cisco WAAS. The following recommendations are considered best practices:

- When designing a serial inline cluster, you should use the same Cisco WAAS model for both units of the serial inline cluster.
- When you use a serial inline cluster, you should disable optimization between the two serial inline cluster devices. You do this through the nonoptimizing peer configuration. Disabling optimization prevents unnecessary session load on the serial cluster.
- If you use an interception ACL to limit the traffic intercepted, make sure that the interception ACL is created to match traffic flow bidirectionally on the device. Interception ACLs need to match only the TCP SYN packet to exclude a session from optimization. Considering both directions of traffic flow will help limit unanticipated optimization traffic.

- Serial inline clustering is meant only to provide high-availability failover of Cisco WAAS services. It is not designed, intended, or supported to provide load balancing of Cisco WAAS optimized traffic. If a load-balanced Cisco WAAS deployment with multiple devices participating in an active-active scenario is desired, use other deployment methods such as WCCP or policy-based routing (PBR) or use a hardware load balancer such as Cisco ACE.
- Use the Cisco WAAS Central Manager for configuration and management of a serial inline cluster. The Cisco WAAS Central Manager provides automatic peer configuration, peer-configuration verification, and access to location-based reporting. These features help eliminate errors and complexity that can arise in large inline deployments.

For More Information

Refer to the following documents for additional information and guides on Cisco WAAS inline features:

Cisco WAAS 4.2.1 Configuring Traffic Interception Guide

Cisco WAE 674/7341/7371 Installing Hardware Options Guide

Cisco WAAS 4.2.1 Monitoring and Troubleshooting Guide

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA C11-609128-00 10/10