CHAPTER 12

Configuring Application Acceleration

This chapter describes how to configure the application policies on your WAAS system that determine the types of application traffic that is accelerated over your WAN.

Note Throughout this chapter, the term WAAS device is used to refer collectively to the WAAS Central Managers and WAEs in your network. The term WAE refers to WAE appliances and WAE Network Modules (the NME-WAE family of devices).

This chapter contains the following topics:

About Application Acceleration

The WAAS software comes with over 150 default application policies that determine the type of application traffic your WAAS system optimizes and accelerates. These default policies cover the most common type of application traffic on your network.

Each application policy contains the following elements:

- **Application definition**—Identifies general information about a specific application, such as the application name and whether the WAAS Central Manager collects statistics about this application.
- **Classifier**—Contains a matching condition that identifies specific types of traffic. For example, the default HTTP classifier matches all traffic going to ports 80, 8080, 8000, 8001, and 3128. You can create up to 512 classifiers and 1024 matching conditions.
- **Policy**—Combines the application definition and classifier into a single policy. This policy also determines what optimization and acceleration features (if any) a WAAS device applies to the defined traffic. You can create up to 512 policies.

You can use the WAAS Central Manager GUI to modify the default policies and to create additional policies for other applications.

For a list of the default policies, see Appendix A, "Default Application Policies."

Creating a New Traffic Application Policy

Table 12-1 provides an overview of the steps you must complete to create a new traffic application policy.

Table 12-1 Checklist for Creating a New Application Policy

Task	Additional Information and Instructions
1. Prepare for creating an application policy.	Provides the tasks you need to complete before creating a new application policy on your WAAS devices. For more information, see the "Preparing to Create an Application Policy" section on page 12-2.
2. Create an application definition.	Identifies general information about the application you want to optimize, such as the application name and whether the WAAS Central Manager collects statistics about this application. This step also allows you to assign the application definition to a device or device group. For more information, see the "Creating an Application Definition" section on page 12-2.
3. Create an application policy.	Determines the type of action your WAAS device or device group performs on specific application traffic. This step requires you to do the following: • Create application classifiers that allow a WAAS device to identify specific types of traffic. For example, you can create a condition that matches all traffic going to a specific IP address. • Specify the type of action your WAAS device or device group performs on the defined traffic. For example, you can specify that WAAS should apply TFO and LZ compression to all traffic for a specific application. For more information, see the "Creating an Application Policy" section on page 12-5.

Preparing to Create an Application Policy

Before you create a new application policy, complete the following preparation tasks:

- Review the list of application policies on your WAAS system and make sure that none of these policies already cover the type of traffic you want to define. To view a list of the default policies that come bundled with the WAAS system, see Appendix A, "Default Application Policies."
- Identify a match condition for the new application traffic. For example, if the application uses a specific destination or source port, you can use that port number to create a match condition. You can also use a source or destination IP address for a match condition.
- Identify the device or device group that requires the new application policy. We recommend you create application policies on device groups so the policy is consistent across multiple WAAS devices.

Creating an Application Definition

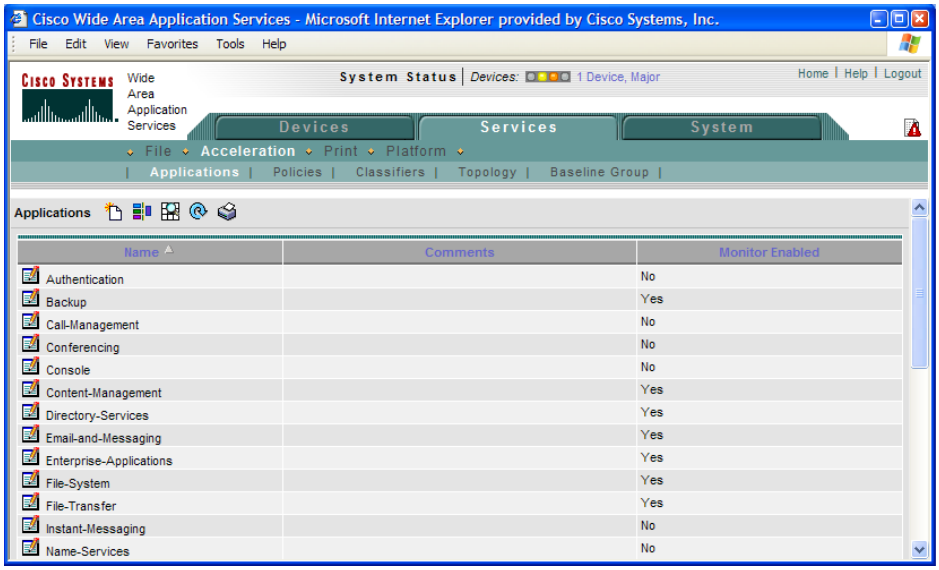
The first step in creating an application policy is to set up an application definition that identifies general information about the application, such as the application name and whether you want the WAAS Central Manager to collect statistics about the application. After creating the application definition, you assign it to a device or device group. You can create up to 256 application definitions on your WAAS system.

To create an application definition, follow these steps:

Step 1 From the WAAS Central Manager GUI, choose **Services > Acceleration > Applications**.

The Applications window appears, which displays a list of all applications on your WAAS system. (See Figure 12-1.)

Figure 12-1 List of Defined Applications



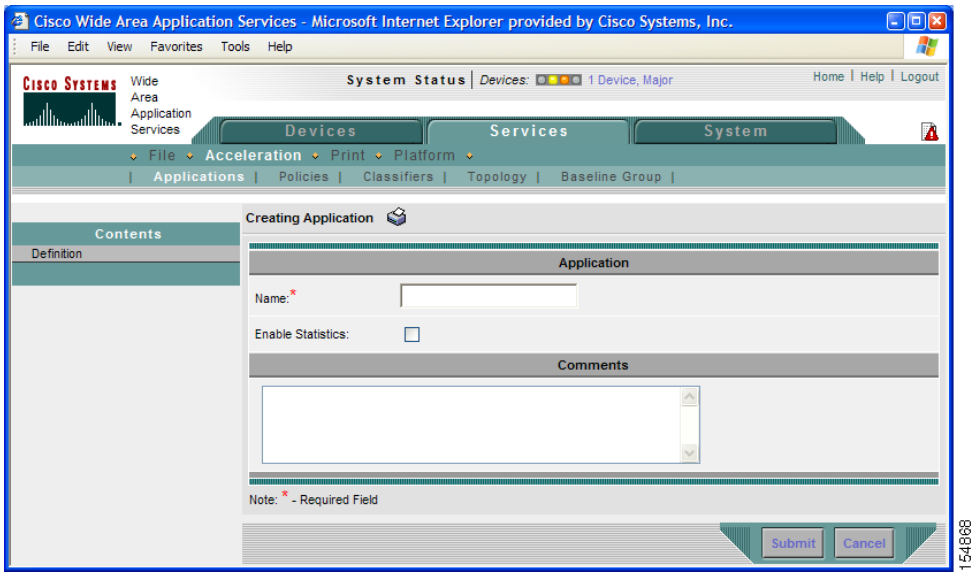
From this window, you can perform the following tasks:

- Click the **Edit** icon next to an application to modify or delete the definition.
- Determine if your WAAS system is collecting statistics on an application. The Monitor Enabled column displays Yes if statistics are being collected for the application.
- Create a new application as described in the steps that follow.

Step 2 Click the **Create New Application** icon in the taskbar.

The Creating Application window appears. (See Figure 12-2.)

Figure 12-2 Creating a New Application Definition



Step 3 Enter a name for this application.

The name cannot contain spaces and special characters.

Step 4 Check the **Enable Statistics** check box to allow the WAAS Central Manager to collect data for this application. To disable data collection for this application, uncheck this box.

The WAAS Central Manager GUI can display statistics for up to 20 applications, and an error message is displayed if you try to enable statistics for the twenty-first application. However, you can use the WAAS CLI to view statistics for all applications that have policies on a specific WAAS device. For more information, refer to the *Cisco Wide Area Application Services Command Reference*.

If you are collecting statistics for an application and decide to disable statistics collection, then reenable statistics collection at a later time, the historical data will be retained, but a gap in data will exist for the time period when statistics collection was disabled. However, if you delete an application that you are collecting statistics for, then later recreate the application, the historical data for the application will be lost. Only data since the recreation of the application will be displayed.

Note The WAAS Central Manager does not start collecting data for this application until you finish creating the entire application policy.

Step 5 (Optional) Enter a comment in the **Comments** field.

The comment you enter appears in the Applications window shown in Figure 12-1 on page 12-3.

Step 6 Click **Submit**.

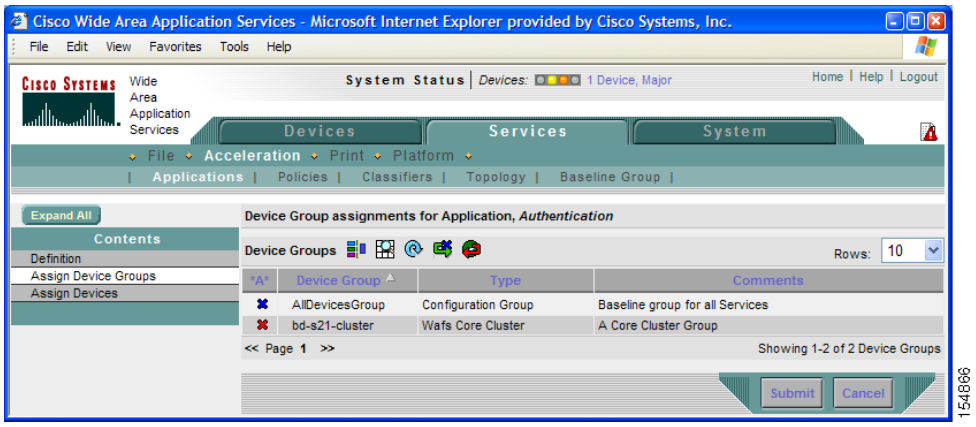
The application definition is saved, and options appear in the Contents pane that allow you to assign the application to a device or device group.

Step 7 From the Contents pane, click one of the following options:

- **Assign Device Groups**—Assigns the application to one or more device groups.
- **Assign Devices**—Assigns the application to one or more WAAS devices.

The Device Groups Assignments window or the WAE Assignments window appears depending on the selected option. Figure 12-3 shows an example of the Device Group Assignments window.

Figure 12-3 Assigning an Application to a Device Group



Step 8 Select the devices or device groups that you want to assign to this application. To select the devices, use one of the following procedures:

- Click in the taskbar to assign all available WAAS devices or device groups.
- Click next to each WAAS device or device group that you want to assign. The icon changes to when selected. To unassign a device or device group, click the icon again.

Step 9 Click **Submit**.

The icon next to the selected devices changes to , showing that the application has been successfully assigned to the devices.

Creating an Application Policy

After you create an application definition, you need to create an application policy that determines the action a WAAS device takes on the specified traffic. For example, you can create an application policy that makes a WAAS device apply TCP optimization and compression to all application traffic that travels over a specific port or to a specific IP address. You can create up to 512 application policies on your WAAS system.

The traffic matching rules are contained in the application classifier. These rules, known as match conditions, use Layer 2 and Layer 4 information in the TCP header to identify traffic.

To create an application policy, follow these steps:

Step 1 From the WAAS Central Manager GUI, choose **Devices > Devices** or **Devices > Device Groups**.

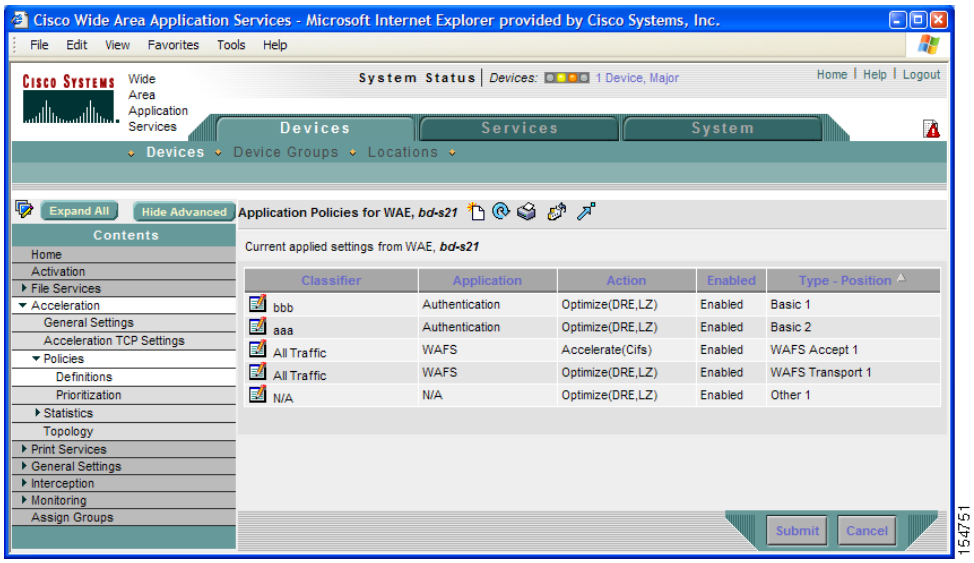
Step 2 Click the **Edit** icon next to the device or device group on which you want to create an application policy.

The Device Home window or the Modifying Device Group window appears.

Step 3 From the Contents pane, select **Acceleration > Policies > Definitions**.

The Application Policies window appears. (See Figure 12-4.)

Figure 12-4 Application Policies Window



This window displays information about all the application policies that reside on the selected device or device group. The first column shows the type of policy (Basic, WAFS Accept, WAFS transport, Port Mapper, or Other) as well as the position of the policy within that type. The position determines the order in which WAAS refers to that policy when determining how to handle application traffic. To change the position of a policy, see the "Modifying the Position of an Application Policy" section on page 12-16. This window also displays the application definition, classifier, and action assigned to each policy.

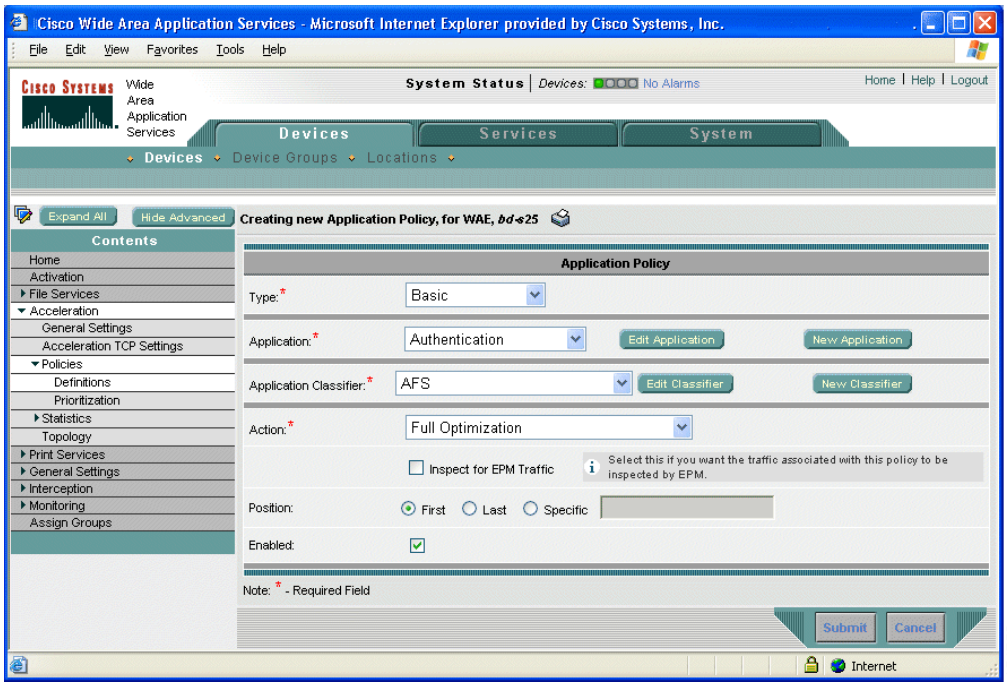
From the Application Policies window, you can perform the following tasks:

- Click the **Edit** icon next to an application policy to modify or delete that policy.
- Restore basic policies and classifiers. For more information, see the "Restoring Application Policies and Classifiers" section on page 12-13.
- Restore default policies and classifiers. For more information, see the "Restoring Application Policies and Classifiers" section on page 12-13.
- Create a new application policy as described in the steps that follow.

Step 4 Click the **Create New Policy** icon in the taskbar to create a new application policy.

The Creating New Application Policy window appears. (See Figure 12-5.)

Figure 12-5 Creating a New Application Policy



Step 5 From the **Type** drop-down list, select the type of application policy.

Table 12-2 describes the types of application policies.

Table 12-2 Application Policy Types

Option	Description
Basic	The standard type of application policy. Choose this option if none of the other types apply. When you choose the Basic option, the Inspect for EPM Traffic check box is enabled under the Action drop-down list. Check this check box if you want the traffic associated with this policy to be inspected by the EPM service.
WAFS Accept	When you enable wide area file services (WAFS), the Edge WAE automatically accelerates all CIFS traffic it accepts. The **WAFS Accept** option allows you to change this default behavior so the Edge WAE takes another action (such as passthrough) for accepted CIFS traffic. When you choose the WAFS Accept option, the Accelerate Using CIFS Adapter check box is enabled under the Action drop-down list. Check this option to apply acceleration techniques to CIFS-based application traffic. These CIFS acceleration techniques include intelligent message suppression and operation prediction and batching. For more information about the acceleration techniques, see the "Application-Specific Acceleration" section on page 1-6. For information on enabling file services, see Chapter 11, "Configuring WAFS."

Table 12-2 Application Policy Types (continued)

Option	Description
WAFS Transport	When you enable wide area file services (WAFS), all CIFS traffic going between an Edge WAE and a core cluster is optimized. Choose the **WAFS Transport** option to specify another action (such as passthrough) for CIFS traffic traveling between edge and core devices. For more information on enabling file services, see Chapter 11, "Configuring WAFS."
EPM	The type of policy for EPM-based applications. EndPoint Mapper (EPM) is a service that dynamically allocates server ports to certain applications. Unlike most applications that always use the same port, applications that rely on the EPM service can be assigned a different port at every request. Because EPM applications do not use a static port, you must specify the application's UUID as a way to identify the application traffic to your WAAS system. When you select the EPM option, the UUID field is enabled so that you can select a preconfigured EPM application or enter the UUID for a custom application.

Step 6 If you selected EPM for the policy type, choose one of the following EPM applications from the **UUID** drop-down list:

- **MAPI**—Uses the predefined UUID associated with the MAPI application, which is a4f1db00-ca47-1067-b31f-00dd010662da.
- **MS-SQL-RPC**—Uses the predefined UUID associated with the SQL Session Manager application, which is 3f99b900-4d87-101b-99b7-aa0004007f07.
- **MS-AD-Replication**—Uses the predefined UUID associated with the Active Directory application, which is e3514235-4b06-11d1-ab04-00c04fc2dcd2.
- **MS-FRS**—Uses the predefined UUID associated with the file replication service, which is f5cc59b4-4264-101a-8c59-08002b2f8426.
- **custom**—Allows you to enter the UUID for a custom EPM application.

Step 7 Specify the application that you want to be associated with this policy by doing either of the following:

- From the Application drop-down list, select an existing application like the one you created in the "Creating an Application Definition" section on page 12-2. This list displays all default and new applications on your WAAS system.

  To modify an existing application, select the application from the drop-down list and click **Edit Application**. You can then change the application's name, add or remove comments, and enable or disable statistics collection for the application. After making the necessary changes, click **Submit** to save your changes and return to the Application Policy window.
- Click **New Application** to create a new application. After specifying the application details, click **Submit** to save the new application and return to the Application Policy window. The new application is automatically assigned to this device or device group.

Step 8 Choose the classifier from the **Application Classifier** drop-down list to select an existing classifier for this policy.

To modify an existing classifier, select the classifier from the drop-down list and click **Edit Classifier**. You can then change classifier's name, add or remove comments, create a new match condition, or edit the existing match condition. After making the necessary changes, click **Submit** to save your changes and return to the Application Policy window.

Step 9 Click **New Classifier** to create a new classifier for this policy.

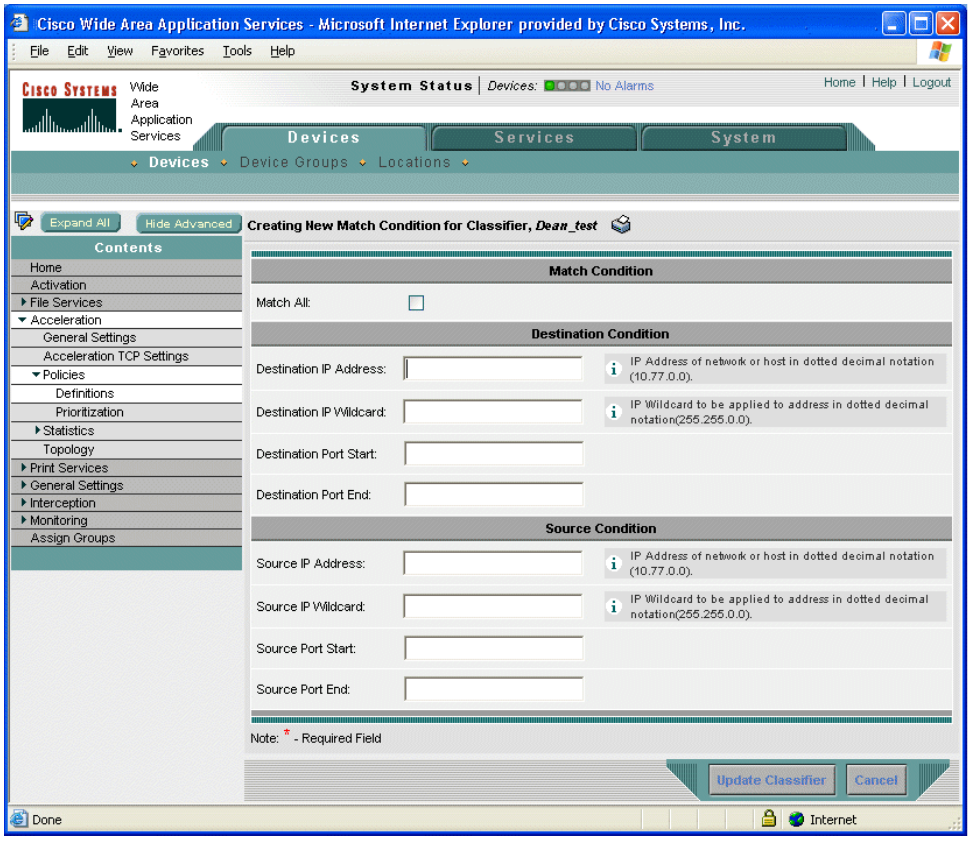
The Creating New Application Classifier window then appears so that you can create a new classifier. Complete the following steps to create a new classifier:

a. Enter a name for this application classifier. The name cannot contain spaces or special characters.

b. (Optional) Enter a comment that will appear on the Application Policies window shown in Figure 12-4 on page 12-6.

c. In the Configure Match Conditions section, click the **Create New Match Condition** icon. The Creating New Match Condition window appears. (See Figure 12-6.)

Figure 12-6 Creating a New Match Condition



d. Check the **Match All** check box to create a condition that matches all traffic. Checking the Match All check box automatically disables all other fields in the window.

e. Enter a value in one of the destination or source condition fields to create a condition for a specific type of traffic.

For example, to match all traffic going to IP address 10.10.10.2, enter that IP address in the Destination IP Address field.

Note To specify a range of IP addresses, enter a subnet range in either the destination or source IP Wildcard field.

f. Click **Update Classifier**. You return to the Creating New Application Classifier window. The new match condition appears at the bottom of this window.

g. Click **Submit**. You return to the Creating New Application Policy window.

Step 10 From the Action drop-down list, choose the action that your WAAS device should take on the defined traffic. Table 12-3 describes each action.

Table 12-3 Action Descriptions

Action	Description
Passthrough	Prevents the WAAS device from optimizing the application traffic defined in this policy. All traffic that matches this policy will be passed through the WAAS system unoptimized.
TFO Only	Applies a variety of transport flow optimization (TFO) techniques to matching traffic. TFO techniques include BIC-TCP, window size maximization and scaling, and selective acknowledgement. For a more detailed description of the TFO features, see the "TFO Optimization" section on page 1-4.
TFO with Data Redundancy Elimination	Applies both TFO and data redundancy elimination (DRE) to matching traffic. DRE removes redundant information before sending the shortened data stream over the WAN. DRE operates on large data streams (tens to hundreds of bytes or more).
TFO with LZ Compression	Applies both TFO and the LZ compression algorithm to matching traffic. LZ compression functions similarly to DRE but uses a different compression algorithm to compress smaller data streams and maintains a limited compression history.
Full Optimization	Applies TFO, DRE, and LZ compression to matching traffic.
None	Does not apply any action to the application traffic. This option is only available for Basic and WAFS Accept policy types.

Step 11 Choose one of the following positions for this application policy:

- **First**—Places this policy at the top of the position list so that the WAAS device tries to classify traffic using this policy before moving onto the second policy in the list. If you already have a policy in the first position, that policy moves down to number two in the list.
- **Last**—Places this policy at the bottom of the position list, making it the last policy that the WAAS device uses to classify traffic. If you already have a policy in the last position, that policy becomes the second to last in the list.
- If a device goes through all the policies in the list without making a match, then the WAAS device passes through the traffic unoptimized.
- **Specific**—Allows you to enter a specific position for this policy. If you already have a policy in the specified position, that policy moves down one in the list.

Step 12 Check the **Enabled** check box to activate this policy. To disable this policy, uncheck this box.

Step 13 Click **Submit**.

The new policy appears in the Application Policies window. (See Figure 12-4 on page 12-6.)

Managing Application Acceleration

This section contains the following topics:

Viewing a List of Applications

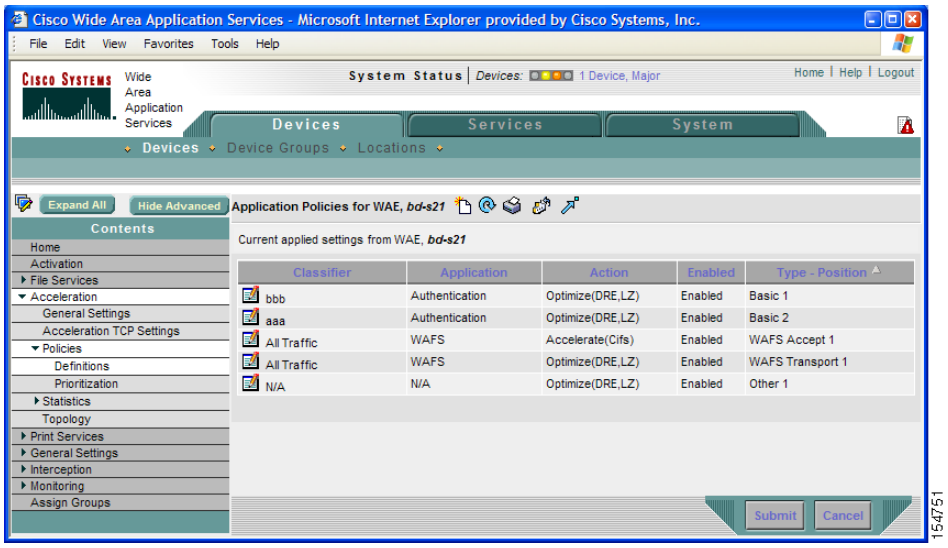
To view a list of applications that reside on a WAE device or device group, follow these steps:

Step 1 From the WAAS Central Manager GUI, choose **Devices > Devices** or **Devices > Device Groups**.

Step 2 Click the **Edit** icon next to the device or device group on which you want to view applications.

Step 3 From the Contents pane, choose **Acceleration >Policies > Definitions**. The Application Policies window displays. (See Figure 12-7.)

Figure 12-7 Viewing List of Applications



Step 4 Click the Application column header to sort the column by application name so you can more easily locate a specific application.

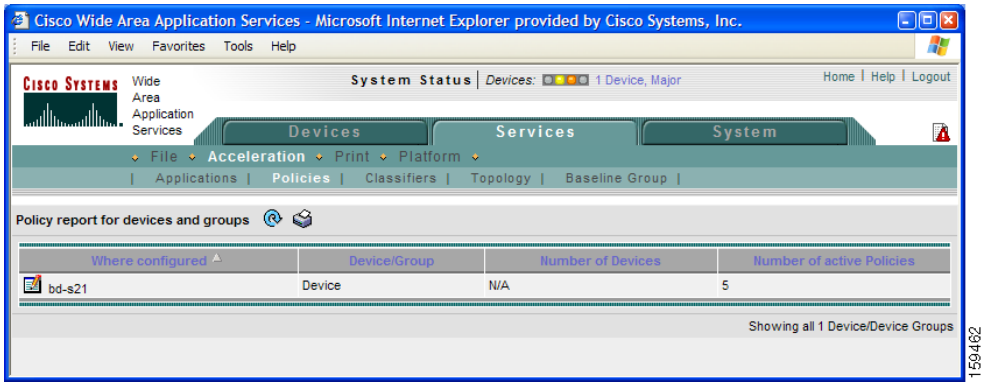
Viewing a Policy Report

To view a report of the policies that reside on each WAE device or device group, follow these steps:

Step 1 From the WAAS Central Manager GUI, choose **Services > Acceleration > Policies**.

The policy report appears. (See Figure 12-8.) It lists each device or device group and the number of active policies on the device or device group.

Figure 12-8 Policy Report



Step 2 Click the **Edit** icon next to a device or group to see the application policies that are defined on it. (See Figure 12-7.)

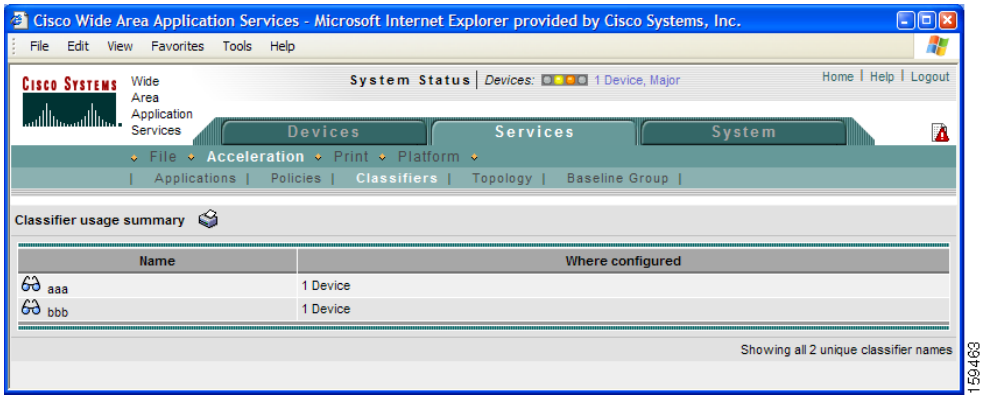
Viewing a Classifier Report

To view a report of the classifiers that reside on each WAE device or device group, follow these steps:

Step 1 From the WAAS Central Manager GUI, choose **Services > Acceleration > Classifiers**.

The classifier report appears. (See Figure 12-9.) It lists each classifier that is defined, and the number of devices on which it is configured.

Figure 12-9 Classifier Report



Step 2 Click the **View** icon next to a classifier to see a report of the devices and device groups on which the classifier is configured.

Step 3 Click the **Edit** icon next to a device or group to see the application policies that are defined on it. (See Figure 12-7.)

Restoring Application Policies and Classifiers

The WAAS system allows you to restore the following types of policies and classifiers:

- **Default**—The policies and classifiers that shipped with the WAAS system. For a list of the default policies, see Appendix A, "Default Application Policies."

  If you made changes to the default policies that have negatively impacted how a WAAS device handles application traffic, you can override your changes by restoring the default policy settings.

- **Basic**—A limited set of polices and classifiers that only optimize WAFS traffic. All other types of traffic pass through the WAAS device unoptimized.

  You may want to restore basic policies on a WAAS device when the only purpose of that device is to provide file services (WAFS) to branch office users. For information on enabling file services, see Chapter 11, "Configuring WAFS."

To restore default or basic policies and classifiers, follow these steps:

Step 1 From the WAAS Central Manager GUI, choose **Devices > Devices** or **Devices > Device Groups**.

Step 2 Click the **Edit** icon next to the device or group on which you want to restore policies.

Step 3 From the Contents pane, choose **Acceleration > Policies**.

The Application Policies window appears.

Step 4 Click one of the following icons in the taskbar:

- **Apply Defaults**—Restores over 150 policies and classifiers that shipped with the WAAS software and removes any new policies that were created on the system. If a default policy has been changed, these changes are lost and the original settings are restored.
- **Restore Basic Policies and Classifiers**—Restores a minimal set of policies and classifiers that optimize WAFS traffic only. When you select this option, all the default policies and classifiers are removed as well as any new policies and classifiers created on the system.

Monitoring Applications

After you create an application policy, you should monitor the associated application to make sure your WAAS system is handling the application traffic as expected. To monitor an application, you must have enabled statistics collection for that application, as described in the "Creating an Application Definition" section on page 12-2.

You can use the System-Wide Traffic Statistics Report to monitor a specific application. For more information, see the "Viewing the System-Wide Traffic Statistics Report" section on page 15-21.

Viewing Connections and Peer Devices

The WAAS Central Manager GUI lets you view a list of the all the peer devices connected to a specific WAE so that you can see the relationship between devices in your WAAS network. You can also use the WAAS Central Manager GUI to view a topology map so that you see a graphical representation of all the connections between the WAE devices. For example, if you are interested in seeing the WAEs that have participated in TFO connections with Device A, you can use the topology map or the device list to view these connections.

Note The WAAS Central Manager device does not have any peers because it does not participate with any WAEs to optimize traffic. For this reason, the topology feature is not available on the WAAS Central Manager device.

To view the topology for a WAE device, follow these steps:

Step 1 From the WAAS Central Manager GUI, choose **Devices > Devices**.

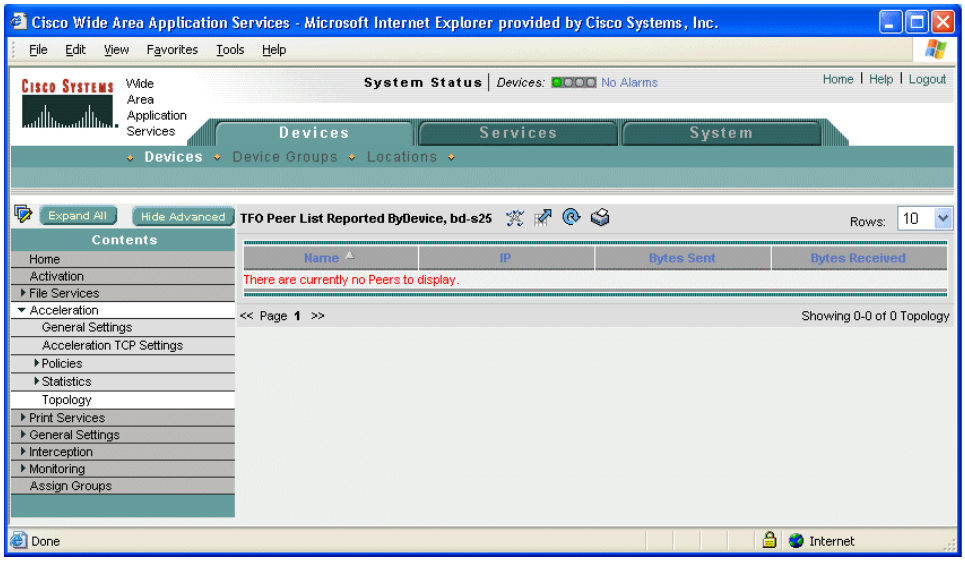
Step 2 Click the **Edit** icon next to the device for which you want to view its TFO peers. The Device Home window appears.

Step 3 From the Contents pane, choose **Acceleration > Topology**. The TFO List Reported by Device window appears. (See Figure 12-10.)

This window displays information about each peer device involved in optimized connections with this WAE.

If a peer device is not registered with the WAAS Central Manager, the MAC address for the peer device name is shown and "unknown" is displayed for the IP address.

Figure 12-10 TFO Peer List Window

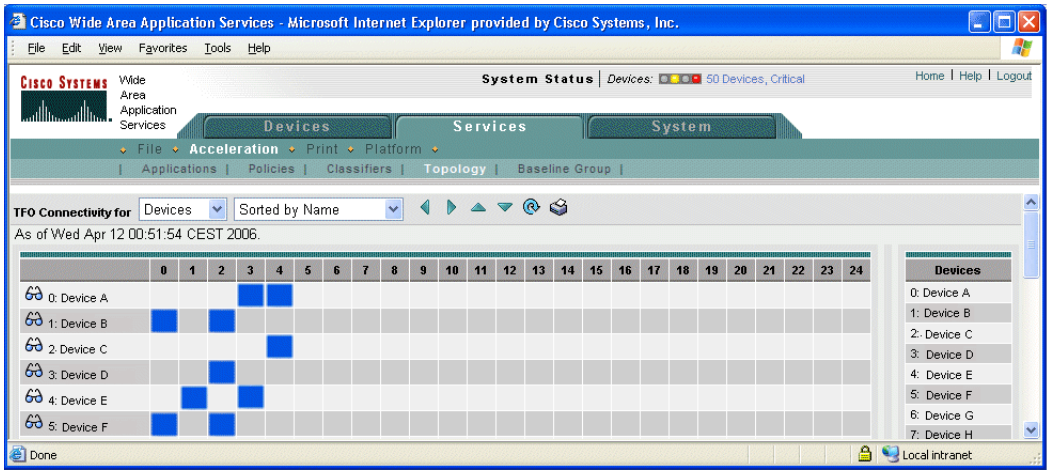


Step 4 View a topology map that displays a grid of all the connections between your WAE devices, by doing one of the following steps:

- From the TFO List Reported by Device window, click the **View Topology** icon in the taskbar.
- From the Services tab, choose **Acceleration > Topology**.

The topology map appears. (See Figure 12-11.)

Figure 12-11 Topology Map



The topology map uses blue squares to show connections between devices. Use the legend to the right of the grid to associate the device name with the number that appears at the top of the grid. For example, in Figure 12-11 Device A is connected to Device D and Device E because a blue square appears in slots 3 and 4 in the grid.

Step 5 Use the drop-down lists at the top of the window to perform the following tasks:

- Display connections between your various locations instead of between devices.
- Sort the grid by the number of connections instead of by device name.

Step 6 Click the **View** icon next to the WAE to view a list of peer devices for a specific WAE. The TFO Peer List window appears. (See Figure 12-10 on page 12-15.)

Modifying the Position of an Application Policy

Each application policy has an assigned position that determines the order in which a WAAS device refers to the policy in an attempt to classify traffic. For example, when a WAAS device intercepts traffic, it refers to the first policy in the list to try to match the traffic to an application. If the first policy does not provide a match, the WAAS device moves on to the next policy in the list.

For information on how to assign a position to a new policy, see the "Creating an Application Policy" section on page 12-5.

You should consider the position of policies that pass through traffic unoptimized because placing these policies at the top of the list can cancel out optimization policies that appear farther down the list. For example, if you have two application policies that match traffic going to IP address 10.10.10.2, and one policy optimizes this traffic and a second policy in a higher position passes through this traffic, then all traffic going to 10.10.10.2 will go through the WAAS system unoptimized. For this reason, you should make sure that your policies do not have overlapping matching conditions, and you should monitor the applications you create to make sure that WAAS is handling the traffic as expected. For more information on monitoring applications, see Chapter 15, "Monitoring and Troubleshooting Your WAAS Network."

To modify the position of an application policy, follow these steps:

Step 1 From the WAAS Central Manager GUI, choose **Devices > Devices** or **Devices > Device Groups**.

Step 2 Click the **Edit** icon next to the device or group that contains the application policy to modify.

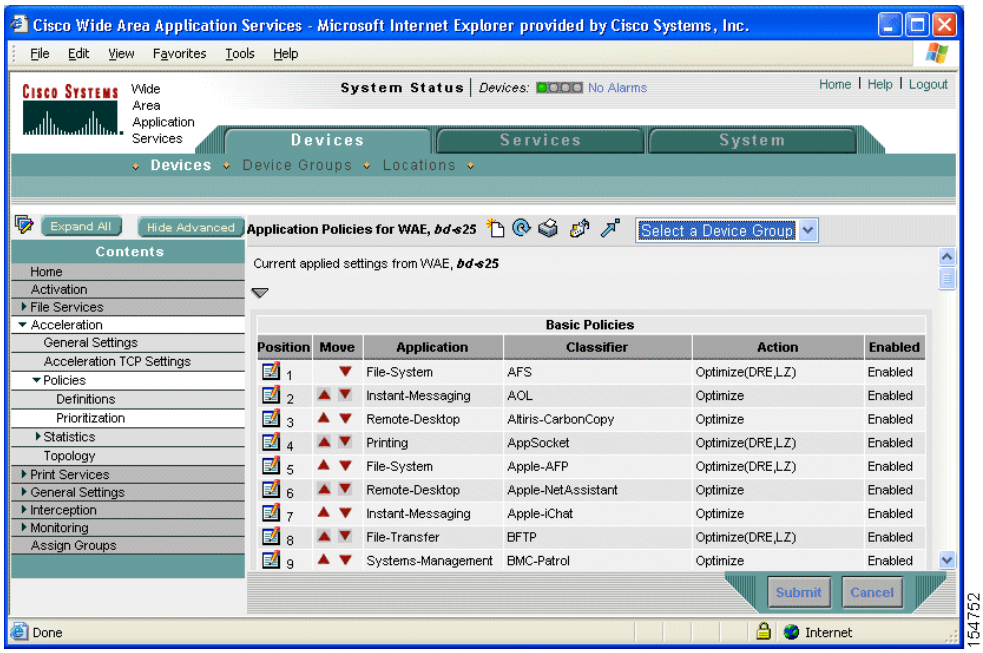
Step 3 From the Contents pane, choose **Acceleration > Policies > Prioritization**.

Step 4 The Application Policies window appears. This window categorizes policies into four categories: WAFS Accept, WAFS Transport, Port Mapper, and Basic.

Step 5 Click the arrow next to the appropriate category to display the list of applications for that category. (See Figure 12-12.)

In most cases, the application you want to change the position for will be located under the Basic Policies category because that category contains a majority of the default applications that shipped with the WAAS system. For a list of these default policies, see Appendix A, "Default Application Policies."

Figure 12-12 Modifying the Position of Application Policies



Step 6 Click the arrow next to the policy category to view the list of applications for that category.

Step 7 Use the up and down arrows (▲ ▼) next to a policy to move that policy higher or lower in the list.

Step 8 If you determine that a policy is not needed, follow these steps to delete the policy:

a. Click the **Edit** icon next to the policy you want to delete.

The Modifying Application Policy window appears.

b. Click the **Delete** icon in the taskbar.

Modifying the Acceleration TCP Settings

In most cases, you do not need to modify the acceleration TCP settings because your WAAS system automatically configures the acceleration TCP settings based on the hardware platform of the WAE device. WAAS automatically configures the settings only under the following circumstances:

- When you first install the WAE device in your network.
- When you enter the **restore factory-default** command on the device. For more information about this command, see the *Cisco Wide Area Application Services Command Reference*.

If your network has high BDP links, you may need to adjust the default buffer settings automatically configured for your WAE device. For more information, see the "Calculating the TCP Buffers for High BDP Links" section on page 12-19.

To modify the acceleration TCP settings, follow these steps:

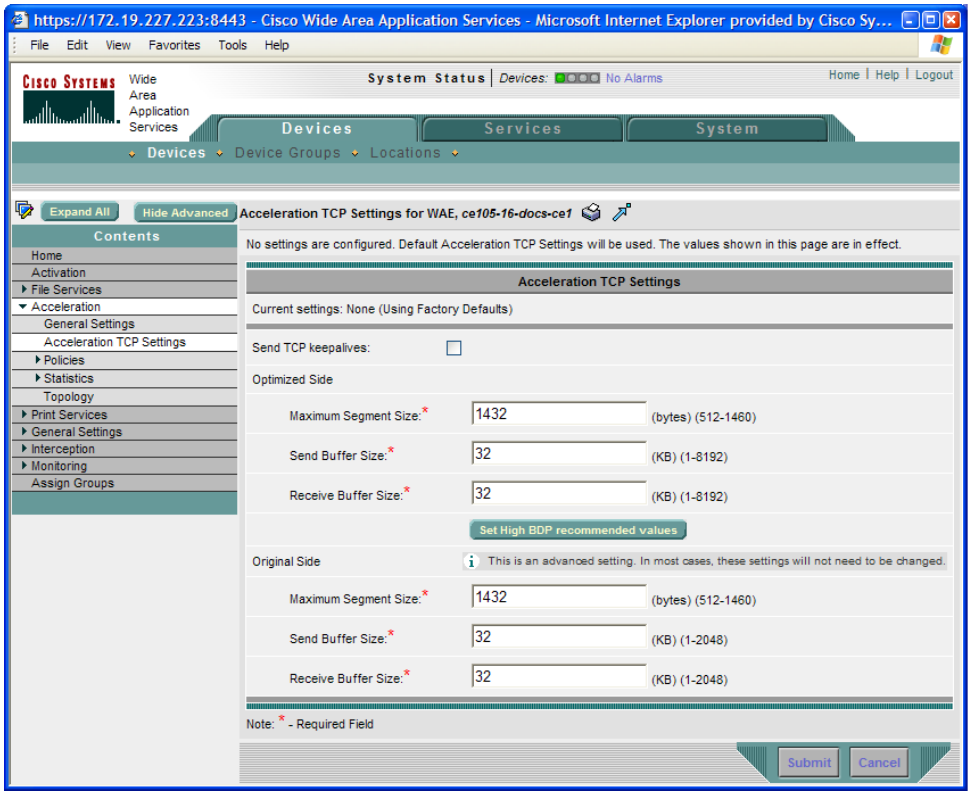
Step 1 From the WAAS Central Manager GUI, choose **Devices > Devices** or **Devices > Device Groups**.

Step 2 Click the **Edit** icon next to the device or device group for which you want to change the acceleration TCP settings.

Step 3 Click **Show Advanced** to display all menu items in the Contents pane. The Acceleration TCP Settings window is an advanced configuration page and does not appear in the basic view.

Step 4 From the Contents pane, choose **Acceleration > Acceleration TCP Settings**. The Acceleration TCP Settings window appears. (See Figure 12-13.)

Figure 12-13 Acceleration TCP Settings Window



Step 5 Keep the **Send TCP Keepalive** check box checked.

Note Enabling TCP keepalives between the Edge and Core WAEs impacts the WAAS system's ability to accommodate network disruptions.

Checking the **Send TCP Keepalive** check box allows this WAE device or group to disconnect the TCP connection to its peer device if no response is received from the TCP keepalive exchange. In this case, the two peer WAE devices will exchange TCP keepalives on a TCP connection and if no response is received for the keepalives for a specific period, the TCP connection will be torn down. When the keepalive option is enabled, any short network disruption in the WAN will cause the TCP connection between peer WAE devices to be disconnected.

If the Send TCP Keepalive check box is not checked, TCP keepalives will not be sent and connections will be maintained unless they are explicitly disconnected. By default, this setting is enabled.

Step 6 Modify the TCP acceleration settings as needed. See Table 12-4 for a description of these settings.

For information on how to calculate these settings for high BDP links, see the "Calculating the TCP Buffers for High BDP Links" section on page 12-19.

Table 12-4 TCP Settings

TCP Setting	Description
Optimized Side	
Maximum Segment Size	Maximum packet size allowed between this WAAS device and other WAAS devices participating in the optimized connection. The default is 1432 bytes.
Send Buffer Size	Allowed TCP sending buffer size (in kilobytes) for TCP packets sent from this WAAS device to other WAAS devices participating in the optimized connection. The default is 32 KB.
Receive Buffer Size	Allowed TCP receiving buffer size (in kilobytes) for incoming TCP packets from other WAAS devices participating in the optimized connection. The default is 32 KB.
Original Side	
Maximum Segment Size	Maximum packet size allowed between the origin client or server and this WAAS device. The default is 1432 bytes.
Send Buffer Size	Allowed TCP sending buffers size (in kilobytes) for TCP packets sent from this WAAS device to the origin client or server. The default is 32 KB.
Receive Buffer Size	Allowed TCP receiving buffer size (in kilobytes) for incoming TCP packets from the origin client or server. The default is 32 KB.

Step 7 If you are deploying the WAE across a high Bandwidth-Delay-Product (BDP) link, you can set recommended values for the send and receive buffer sizes by clicking the **Set High BDP recommended values** button. For more information about calculating TCP buffers for high BDP links, see the "Calculating the TCP Buffers for High BDP Links" section on page 12-19.

Step 8 Click **Submit**.

Calculating the TCP Buffers for High BDP Links

Cisco WAAS can be deployed in different network environments, involving multiple link characteristics such as bandwidth, latency, and packet loss. All WAAS devices are configured to accommodate networks with maximum Bandwidth-Delay-Product (BDP) of up to the values listed below:

- WAE-511/512—Default BDP is 32 KB
- WAE-611/612—Default BDP is 512 KB
- WAE-7326 —Default BDP is 2048 KB

If your network provides higher bandwidth or higher latencies are involved, use the following formula to calculate the actual link BDP:

BDP [Kbytes] = (link BW [Kbytes/sec] * Round-trip latency [Sec])

When multiple links 1..N are the links for which the WAE is optimizing traffic, the maximum BDP should be calculated as follows:

MaxBDP = Max (BDP(link 1),..,BDP(link N))

If the calculated MaxBDP is greater than the DefaultBDP for your WAE model, the Acceleration TCP settings should be modified to accommodate that calculated BDP.

Once you calculate the size of the Max BDP, enter that value in the Send Buffer Size and Receive Buffer Size for the optimized and original side on the Acceleration TCP Settings window.

Enabling and Disabling the Global Optimization Settings

The global optimization settings determine if TFO Optimization, Data Redundancy Elimination, Compression, and the EPM adapter are enabled on a device or device group. By default, all of these options are enabled. If you choose to disable one of these options, the device will be unable to apply the full WAAS optimization techniques to the traffic that it intercepts.

To enable or disable a global optimization option, follow these steps:

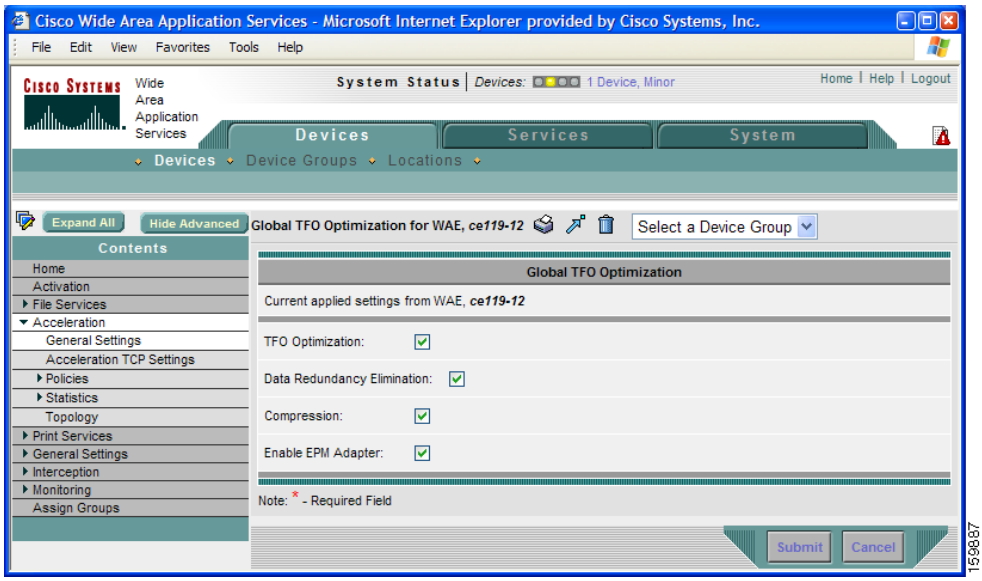
Step 1 From the WAAS Central Manager GUI, choose **Devices > Devices** or **Devices > Device Groups**.

Step 2 Click the **Edit** icon next to the device or device group for which you want to change the global optimization settings.

Step 3 From the Contents pane, choose **Acceleration > General Settings**.

The Global TFO Optimization window appears. (See Figure 12-14.)

Figure 12-14 Modifying the Global Optimization Settings



Step 4 Place a check next to the optimization options you want to enable, and uncheck the options that you want to disable.

For a description of each of the first three options, see Chapter 1, "Introduction to Cisco WAAS." For a description of the EPM service that the EPM adapter provides, see Table 12-2 on page 12-7.

Step 5 If you are configuring a device whose settings are governed by a device group and you want to apply the global optimization settings from a different device group to the device that you are configuring, follow these steps:

a. From the Select a Device Group drop-down list at the top of the window, choose the device group whose settings that you want to apply to the current device. (This drop-down list does not appear if you are configuring a device group.)

b. Click **Submit** to save the settings.

The changes are saved to the device. You can skip the next step.

Step 6 Click **Submit**.

The changes are saved to the device or device group.