



CHAPTER 4

Configuring Virtual Servers

Date: 2/17/11

This section provides an overview of server load balancing and procedures for configuring virtual servers for load balancing on an ACE.

Topics include:

- [Load Balancing Overview, page 4-1](#)
- [Configuring Virtual Servers, page 4-2](#)
- [Managing Virtual Servers, page 4-55](#)

Load Balancing Overview

Server load balancing (SLB) is the process of deciding to which server a load balancer should send a client request for service. For example, a client request can consist of an HTTP GET for a Web page or an FTP GET to download a file. The job of the load balancer is to select the server that can successfully fulfill the client request and do so in the shortest amount of time without overloading either the server or the server farm as a whole.

Depending on the load-balancing algorithm or predictor that you configure, the ACE performs a series of checks and calculations to determine the server that can best service each client request. The ACE bases server selection on several factors, including the server with the fewest connections with respect to load, source or destination address, cookies, URLs, or HTTP headers.

The ANM allows you to configure load balancing using:

- Virtual servers—See [Configuring Virtual Servers, page 4-2](#).
- Real servers—See [Configuring Real Servers, page 5-4](#).
- Server farms—See [Configuring Server Farms, page 5-12](#).
- Sticky groups—See [Configuring Sticky Groups, page 6-7](#).
- Parameter maps—See [Configuring Parameter Maps, page 7-1](#).

For information about SLB as configured and performed by the ACE, see:

- [Configuring Virtual Servers, page 4-2](#)
- [Load-Balancing Predictors, page 5-2](#)
- [Real Servers, page 5-3](#)
- [Server Farms, page 5-4](#)

- [Health Monitoring, page 5-26](#)
- [TCL Scripts, page 5-27](#)
- [Configuring Stickiness, page 6-1](#)

Configuring Virtual Servers

In a load-balancing environment, a virtual server is a construct that allows multiple physical servers to appear as one for load-balancing purposes. A virtual server is bound to physical services running on real servers in a server farm and uses IP address and port information to distribute incoming client requests to the servers in the server farm according to a specified load-balancing algorithm.

You use class maps to configure a virtual server address and definition. The load-balancing predictor algorithms (for example, roundrobin, least connections, and so on) determine the servers to which the ACE sends connection requests.

For more information about virtual servers and ANM, see:

- [Understanding Virtual Server Configuration and ANM, page 4-2](#)
- [Using ANM to Configure Virtual Servers, page 4-4](#)
- [Virtual Server Configuration Procedure, page 4-5](#)

Understanding Virtual Server Configuration and ANM

The ANM Virtual Server configuration interface, an abstraction of the Modular Policy CLI, simplifies, reorders, and makes more atomic the configuration and deployment of a functional load-balancing environment. With simplification or abstraction, some constraints or limitations are necessarily introduced. This section identifies the constraints and framework used by the ANM for virtual server configuration.

In the ANM, a viable virtual server has the following attributes:

- A single Layer 3/Layer 4 match condition
This means that you can specify only a single IP address (or single IP address range if a netmask is used), with only a single port (or port range). Having a single match condition greatly simplifies and aids virtual server configuration.
- A default Layer 7 action
- A Layer 7 policy map
- A Layer 3/Layer 4 class map
- A single multi-match policy map, a class-map match, and an action

In addition:

- The virtual server multi-match policy map is associated with an interface or is global.
- The name of the virtual server is derived from the name of the Layer 3/Layer 4 class map.

Example 4-1 shows the minimum configuration statements required for a virtual server.

Example 4-1 Minimum Configuration Required for a Virtual Server

```
class-map match-all Example_VIP
  2 match virtual-address 10.10.10.10 tcp eq www
policy-map type loadbalance first-match Example_VIP-l7slb
  class class-default
    forward
policy-map multi-match int10
  class Example_VIP
    loadbalance policy Example_VIP-l7slb

interface vlan 10
  ip address 192.168.65.37 255.255.255.0
  service-policy input int10
  no shutdown
```

Note also the following items regarding the ANM and virtual servers:

- **Additional configuration options**

The Virtual Server configuration screen allows you to configure additional items for a functional VIP. These items include server farms, sticky groups, real servers, probes, parameter maps, inspection, class maps, and inline match conditions. Because too many items on a screen can be overwhelming, not all configuration options appear on Virtual Server configuration screen, such as sticky statics or backup real servers. These options are available elsewhere in the ANM interface instead of on the Virtual Server configuration screen.

- **Configuration options and roles**

To support and maintain the separation of roles, some objects cannot be configured using the Virtual Server configuration screen. These objects include SSL certificates, SSL keys, NAT pools, interface IP addresses, and ACLs. Providing these options as separate configuration options in the ANM interface ensures that a user who can view or modify virtual servers or aspects of virtual servers cannot create or delete virtual servers.

- **Changes to virtual servers using the CLI or Expert options can prevent further modifications in the Virtual Server configuration screen**

If you create a virtual server using the Virtual Server configuration screen, modify it using the CLI or Expert options (**Config > Devices > Expert**), and then attempt to modify it again using the Virtual Server configuration screen, error messages will be displayed and you will not be able to modify the virtual server.

Related Topics

- [Configuring Virtual Servers, page 4-2](#)
- [Using ANM to Configure Virtual Servers, page 4-4](#)
- [Virtual Server Configuration Procedure, page 4-5](#)

Using ANM to Configure Virtual Servers

It is important to understand the following concepts when using the ANM to configure virtual servers:

- **Virtual server configuration screens**

The ANM Virtual Server configuration screens are designed to aid you in configuring virtual servers by presenting configuration options that are relevant to your choices. For example, the protocols that you select in the Properties configuration subset determine the other configuration subsets that appear.

- **Use the virtual server configuration method that suits you**

The ANM Virtual Server configuration screens simplify the process of creating, modifying, and deploying virtual servers by displaying those options that you are most likely to use. In addition, as you specify attributes for a virtual server, such as protocols, the interface refreshes with related configuration options, such as Protocol Inspection or Application Acceleration and Optimization, thereby speeding virtual server configuration and deployment.

While Virtual Server configuration screens remove some configuration complexities, they have a few constraints that the Expert configuration options do not. If you are comfortable using the CLI, you can use the Expert options (such as **Config > Devices > context > Expert > Class Maps or Policy** or **Config > Devices > context > Load Balancing > Parameter Maps** to configure more complex attributes of virtual servers, traffic policies, and parameter maps.

- **Synchronizing virtual server configurations**

If you configure a virtual server using the CLI and then use the Sync option (**Config > Devices > ACE > Sync**) to synchronize configurations, the configuration that appears in ANM for the virtual server might not display all configuration options for that virtual server. The configuration that appears in the ANM depends on a number of items, such as the protocols configured in class maps or the rules defined for policy maps.

For example, if you configure a virtual server on the CLI that includes a class map that can match any protocol, you will not see the virtual server Application Acceleration and Optimization configuration subset in the ANM.

- **Modifying shared objects**

Modifying an object that is used by multiple virtual servers, such as a server farm, real server, or parameter map, could impact the other virtual servers. See [Shared Objects and Virtual Servers, page 4-6](#) for more information about modifying objects used by multiple virtual servers.

Related Topics

- [Configuring Virtual Servers, page 4-2](#)
- [Understanding Virtual Server Configuration and ANM, page 4-2](#)
- [Virtual Server Configuration Procedure, page 4-5](#)

Virtual Server Configuration Procedure

Use this procedure to add virtual servers to the ANM for load-balancing purposes.

Assumptions

- Depending on the protocol to be used for the virtual server, parameter maps need to be defined.
- For SSL service, SSL certificates, keys, chain groups, and parameter maps must be configured.

Procedure

- Step 1** Select **Config > Devices > context > Load Balancing > Virtual Servers**. The Virtual Servers table appears.
- Step 2** Click **Add** to add a new virtual server, or select an existing virtual server, then click **Edit** to modify it. The Virtual Server configuration screen appears with a number of configuration subsets. The subsets that you see depend on whether you use the Basic View or the Advanced View and entries you make in the Properties subset. Change views by using the View object selector at the top of the configuration pane.

[Table 4-1](#) identifies and describes virtual server configuration subsets with links to related topics for configuration information.



Note The protocols that are available depend on the ACE device that you are configuring. For a list of the protocols available for each ACE device type, see [Table 4-2](#).

Table 4-1 Virtual Server Configuration Subsets

Configuration Subset	Description	Related Topics
Properties	This subset allows you to specify basic virtual server characteristics, such as the virtual server name, IP address, protocol, port, and VLANs.	Configuring Virtual Server Properties, page 4-8
SSL Termination	This subset appears when TCP is the selected protocol and Other or HTTPS is the application protocol. This subset allows you to configure the virtual server to act as an SSL proxy server and terminate SSL sessions between it and its clients.	Configuring Virtual Server SSL Termination, page 4-13
Protocol Inspection	This subset appears in the Advanced View for: <ul style="list-style-type: none"> • TCP with FTP, HTTP, HTTPS, RTSP, or SIP • UDP with DNS or SIP This subset appears in the Basic view for TCP with FTP. This subset allows you to configure the virtual server so that it can verify protocol behavior and identify unwanted or malicious traffic passing through the ACE on selected application protocols.	Configuring Virtual Server Protocol Inspection, page 4-14

Table 4-1 Virtual Server Configuration Subsets (continued)

Configuration Subset	Description	Related Topics
Application Acceleration And Optimization	This subset appears only for ACE appliances. It appears in the Advanced View when HTTP or HTTPS is the selected application protocol. This subset allows you to configure application acceleration and optimization options for HTTP or HTTPS traffic.	Configuring Application Acceleration and Optimization, page 4-44
L7 Load-Balancing	This subset appears only in the Advanced View for: <ul style="list-style-type: none"> TCP with Generic, HTTP, HTTPS, RTSP, or SIP UDP with Generic, RADIUS, or SIP This subset allows you to configure Layer 7 load-balancing options, including SSL initiation.	Configuring Virtual Server Layer 7 Load Balancing, page 4-26
Default L7 Load-Balancing Action	This subset allows you to establish the default Layer 7 load-balancing actions for all network traffic that does not meet previously specified match conditions including the SSL initiation configuration.	Configuring Virtual Server Default Layer 7 Load Balancing, page 4-41
NAT	This subset appears in the Advanced View only. This subset allows you to set up Name Address Translation (NAT) for the virtual server.	Configuring Virtual Server NAT, page 4-54

- Step 3** When you finish configuring virtual server properties, click:
- **Deploy Now** to deploy the configuration on the ACE.
 - **Cancel** to exit the procedure without saving your entries and to return to the Virtual Servers table.
 - **Deploy Later** to save your entries and apply them at a later time.

Related Topics

- [Configuring Virtual Servers, page 4-2](#)
- [Understanding Virtual Server Configuration and ANM, page 4-2](#)
- [Using ANM to Configure Virtual Servers, page 4-4](#)
- [Shared Objects and Virtual Servers, page 4-6](#)
- [Understanding Roles, page 15-6](#)

Shared Objects and Virtual Servers

A shared object is one that is used by multiple virtual servers. Examples of shared objects are:

- Action lists
- Class maps
- Parameter maps
- Real servers

- Server farms
- SSL services
- Sticky groups

Because these objects are shared, modifying an object's configuration in one virtual server can impact other virtual servers that use the same object.

Configuring Shared Objects

ANM offers the following options for shared objects in virtual server configuration screens (**Config > Devices > context > Load Balancing > Virtual Servers**):

- **View**—Click **View** to review the object's configuration. The screen refreshes with read-only fields and the following three buttons.
- **Cancel**—Click **Cancel** to close the read-only view and to return to the previous screen.
- **Edit**—Click **Edit** to modify the selected object's configuration. The screen refreshes with fields that can be modified, except for the Name field which remains read-only.



Note Before changing a shared object's configuration, make sure you understand the effect of the changes on other virtual servers using the same object. As an alternative, consider using the Duplicate option instead.

- **Duplicate**—Click **Duplicate** to create a new object with the same configuration as the selected object. The screen refreshes with configurable fields. In the Name field, enter a unique name for the new object, then modify the configuration as desired. This option allows you to create a new object without impacting other virtual servers using the same object.

Deleting Virtual Servers with Shared Objects

If you create a virtual server and include shared objects in its configuration, deleting the virtual server does not delete the associated shared objects. This ensures that other virtual servers using the same shared objects are not impacted.

Related Topics

- [Managing Virtual Servers, page 4-55](#)
- [Virtual Server Protocols by Device Type, page 4-8](#)
- [Configuring Virtual Server Properties, page 4-8](#)
- [Configuring Virtual Server SSL Termination, page 4-13](#)
- [Configuring Virtual Server Protocol Inspection, page 4-14](#)
- [Configuring Virtual Server Layer 7 Load Balancing, page 4-26](#)
- [Configuring Virtual Server Default Layer 7 Load Balancing, page 4-41](#)
- [Configuring Application Acceleration and Optimization, page 4-44](#)

Virtual Server Protocols by Device Type

The protocols that are available for a virtual server depend on the ACE device you are configuring. [Table 4-2](#) lists the protocols available for each device type.

Table 4-2 Virtual Server Protocols for ACE Modules and Devices

Protocol	ACE 1.0 Modules	ACE 2.0 Modules	ACE 4710 Appliance Running Image A1(8)	ACE 4710 Appliance Running Image A3(1.0)
Any	X	X	X	X
TCP				
FTP	X	X	X	X
Generic		X		X
HTTP	X	X	X	X
HTTPS	X	X	X	X
Other	X	X	X	X
RTSP		X		X
RDP		X		X
SIP		X		X
UDP				
DNS	X	X	X	X
Generic		X		
Other	X	X	X	X
RADIUS		X		X
SIP		X		

Related Topics

- [Configuring Virtual Servers, page 4-2](#)
- [Configuring Virtual Server Properties, page 4-8](#)

Configuring Virtual Server Properties

Use this procedure to configure virtual server properties.

Procedure

-
- Step 1** Select **Config > Devices > context > Load Balancing > Virtual Servers**. The Virtual Servers table appears.
- Step 2** Click **Add** to add a new virtual server, or select an existing virtual server, then click **Edit** to modify it. The Virtual Server configuration screen appears. The Properties configuration subset is open by default.

The fields that you see in the Properties configuration subset depend on whether you are using Advanced View or Basic View:

- To configure Advanced View properties, continue with [Step 3](#).
- To configure Basic View properties, continue with [Step 4](#).

Step 3 To configure virtual server properties in the Advanced View, enter the information in [Table 4-3](#).

Table 4-3 Virtual Server Properties – Advanced View

Field	Description
Virtual Server Name	Enter the name for the virtual server.
Virtual IP Address	Enter the IP address for the virtual server.
Virtual IP Mask	Select the subnet mask to apply to the virtual server IP address.
Transport Protocol	Select the protocol the virtual server supports: <ul style="list-style-type: none"> • Any—The virtual server is to accept connections using any IP protocol. • TCP—The virtual server is to accept connections that use TCP. • UDP—The virtual server is to accept connections that use UDP.
Application Protocol	This field appears if TCP or UDP is selected. The application protocols that are available depend on the type of ACE being configured. Select the application protocol to be supported by the virtual server. Table 4-2 identifies the available protocols for each ACE device type. Note This field is read-only if you are editing an existing virtual server. ANM does not allow changes between protocols that require a change to the Layer 7 server load-balancing policy map. You need to delete the virtual server and create a new one with the desired application protocol.
Port	This field appears for any TCP or UDP protocol. Enter the port to be used for the specified protocol. Valid entries are integers from 0 to 65535 or a range of integers, such as 10-20 . Enter 0 (zero) to indicate all ports. For a complete list of protocols and ports, see the Internet Assigned Numbers Authority available at www.iana.org/numbers/ .
All VLANs	Check the check box to support incoming traffic from all VLANs. Clear the check box to support incoming traffic from specific VLANs only.
VLAN	This field appears if the All VLANs check box is cleared. In the Available Items list, select the VLANs to use for incoming traffic, then click Add . The items appear in the Selected Items list. To remove VLANs, select them in the Selected Items lists, then click Remove . The items appear in the Available Items list. Note You cannot change the VLAN for a virtual server once it is specified. Instead, delete the virtual server and create a new one with the desired VLAN.

Table 4-3 Virtual Server Properties – Advanced View (continued)

Field	Description
Connection Parameter Maps	<p>This field appears if TCP is the selected protocol.</p> <p>Select an existing connection parameter map or click *New* to create a new one:</p> <ul style="list-style-type: none"> If you select an existing parameter map, you can view, modify, or duplicate the existing configuration. See Shared Objects and Virtual Servers, page 4-6 for more information about modifying shared objects. If you click *New*, the Connection Parameter Maps configuration pane appears. Configure the connection parameter map as described in Table 7-2. <p>Note Click More Settings to access the additional Connection Parameter Maps configuration attributes. By default, ANM hides the default Connection Parameter Maps configuration attributes and the attributes which are not commonly used.</p>
DNS Parameter Maps	<p>This field appears if DNS is the selected protocol over UDP.</p> <p>Select an existing DNS parameter map or click *New* to create a new one:</p> <ul style="list-style-type: none"> If you select an existing parameter map, you can view, modify, or duplicate the existing configuration. See Shared Objects and Virtual Servers, page 4-6 for more information about modifying shared objects. If you click *New*, the DNS Parameter Maps configuration pane appears. Configure the DNS parameter map as described in Table 7-11.
Generic Parameter Maps	<p>This field appears if Generic is the selected application protocol over TCP or UDP.</p> <p>Select an existing Generic parameter map or click *New* to create a new one:</p> <ul style="list-style-type: none"> If you select an existing parameter map, you can view, modify, or duplicate the existing configuration. See Shared Objects and Virtual Servers, page 4-6 for more information about modifying shared objects. If you click *New*, the Generic Parameter Maps configuration pane appears. Configure the Generic parameter map as described in Table 7-4.
HTTP Parameter Maps	<p>This field appears if HTTP or HTTPS is the selected application protocol.</p> <p>Select an existing HTTP parameter map or click *New* to create a new one:</p> <ul style="list-style-type: none"> If you select an existing parameter map, you can view, modify, or duplicate the existing configuration. See Shared Objects and Virtual Servers, page 4-6 for more information about modifying shared objects. If you click *New*, the HTTP Parameter Maps configuration pane appears. Configure the HTTP parameter map as described in Table 7-5.
RTSP Parameter Maps	<p>This field appears if RTSP is the selected application protocol over TCP.</p> <p>Select an existing RTSP parameter map or click *New* to create a new one:</p> <ul style="list-style-type: none"> If you select an existing parameter map, you can view, modify, or duplicate the existing configuration. See Shared Objects and Virtual Servers, page 4-6 for more information about modifying shared objects. If you click *New*, the RTSP Parameter Maps configuration pane appears. Configure the RTSP parameter map as described in Table 7-8.

Table 4-3 Virtual Server Properties – Advanced View (continued)

Field	Description
ICMP Reply	<p>Indicate how the virtual server is to respond to ICMP ECHO requests:</p> <ul style="list-style-type: none"> • None—The virtual server is not to send ICMP ECHO-REPLY responses to ICMP requests. • Active—The virtual server is to send ICMP ECHO-REPLY responses only if the configured VIP is active. • Always—The virtual server is always to send ICMP ECHO-REPLY responses to ICMP requests. • Primary Inservice—The virtual server is to reply to an ICMP ping only if the primary server farm state is UP, regardless of the state of the backup server farm. If this option is selected and the primary server farm state is DOWN, the ACE discards the ICMP request and the request times out.
VIP Advertise	<p>This field appears for ACE 1.0 and 2.0 modules only.</p> <p>This option allows the ACE to advertise the IP address of the virtual server as the host route. Select the desired VIP advertise option:</p> <ul style="list-style-type: none"> • None—The ACE is not to advertise the IP address of the virtual server as the host route. • Active—The ACE is to advertise the IP address of the virtual server as the host route only if there is at least one active real server in the server farm. • Always—The ACE is always to advertise the IP address of the virtual server as the host route. • Active-Metric—The ACE is to advertise the IP address of the virtual server as the host route if: <ul style="list-style-type: none"> • There is at least one active real server in the server farm. • A distance metric is specified for the route in the Distance field. • Always-Metric—The ACE is to advertise the IP address of the virtual server as the host route, using the distance metric in the Distance field.
Distance	<p>This field appears for ACE 1.0 and 2.0 modules only.</p> <p>This field appears if you select Active-Metric or Always-Metric in the VIP Advertise field. Enter the administrative distance to be included in the routing table. Valid entries are integers from 1 to 254.</p>
Status	<p>Indicate whether the virtual server is to be in service or out of service:</p> <ul style="list-style-type: none"> • In Service—Enables the virtual server for load-balancing operations. • Out Of Service—Disables the virtual server for load-balancing operations.

Step 4 To configure virtual server properties in the Basic View, enter the information in [Table 4-4](#).

Table 4-4 Virtual Server Properties – Basic View

Field	Description
Virtual Server Name	Enter the name for the virtual server.
Virtual IP Address	Enter the IP address for the virtual server.

Table 4-4 Virtual Server Properties – Basic View (continued)

Field	Description
Transport Protocol	<p>Select the protocol that the virtual server supports:</p> <ul style="list-style-type: none"> Any—The virtual server is to accept connections using any IP protocol. TCP—The virtual server is to accept connections that use TCP. UDP—The virtual server is to accept connections that use UDP.
Application Protocol	<p>This field appears if TCP or UDP is selected. The application protocols that are available depend on the type of ACE being configured.</p> <p>Select the application protocol to be supported by the virtual server. Table 4-2 identifies the available protocols for each ACE device type.</p> <p>Note This field is read-only if you are editing an existing virtual server. ANM does not allow changes between protocols that require a change to the Layer 7 server load-balancing policy map. You need to delete the virtual server and create a new one with the desired application protocol.</p>
Port	<p>This field appears for any specific TCP or UDP protocol.</p> <p>Enter the port to be used for the specified protocol. Valid entries are integers from 0 to 65535 or a range of integers, such as 10-20. Enter 0 (zero) to indicate all ports.</p> <p>For a complete list of all protocols and ports, see the Internet Assigned Numbers Authority available at www.iana.org/numbers/.</p>
All VLANs	<p>Check the check box to support incoming traffic from all VLANs. Clear the check box to support incoming traffic from specific VLANs only.</p>
VLAN	<p>This field appears if the All VLANs check box is cleared.</p> <p>In the Available Items list, select the VLANs to use for incoming traffic, then click Add. The items appear in the Selected Items list.</p> <p>To remove VLANs, select them in the Selected Items lists, then click Remove. The items appear in the Available Items list.</p> <p>Note You cannot change the VLAN for a virtual server once it is specified. Instead, delete the virtual server and create a new one with the desired VLAN.</p>

- Step 5** When you finish configuring virtual server properties, click:
- Deploy Now** to deploy the configuration on the ACE.
 - Cancel** to exit the procedure without saving your entries.
 - Deploy Later** to save your entries and apply them at a later time.

Related Topics

- [Configuring Virtual Servers, page 4-2](#)
- [Configuring Virtual Server SSL Termination, page 4-13](#)

Configuring Virtual Server SSL Termination

SSL termination service allows the virtual server to act as an SSL proxy server and terminate SSL sessions between it and its clients.

Use this procedure to configure virtual server SSL termination service.

Assumption

A virtual server has been configured for HTTPS over TCP or Other over TCP in the Properties configuration subset. For more information, see [Configuring Virtual Server Properties, page 4-8](#).

Procedure

-
- Step 1** Select **Config > Devices > context > Load Balancing > Virtual Servers**. The Virtual Servers table appears.
- Step 2** Select the virtual server you want to configure for SSL termination, then click **Edit**. The Virtual Server configuration screen appears.
- Step 3** Click **SSL Termination**. The Proxy Service Name field appears.
- Step 4** In the Proxy Service Name field, select an existing SSL termination service, or select ***New*** to create a new SSL proxy service:
- If you select an existing SSL service, the screen refreshes and allows you to view, modify, or duplicate the existing configuration. See [Shared Objects and Virtual Servers, page 4-6](#) for more information about modifying shared objects.
 - If you select ***New***, the Proxy Service configuration subset appears.
- Step 5** Configure the SSL service using the in [Table 4-5](#).
For more information about SSL, see [Configuring SSL, page 8-1](#).

Table 4-5 Virtual Server SSL Attributes


Field	Description
Name	Enter a name for this SSL proxy service. Valid entries are alphanumeric strings with a maximum of 26 characters.
Keys	Select the SSL key pair to use during the SSL handshake for data encryption.
Certificates	Select the SSL certificate to use during the SSL handshake.
Chain Groups	Select the chain group to use during the SSL handshake.
Auth Groups	Select the SSL authentication group to associate with this proxy server service.
	 <p>Note This option appears for ACE 2.0 modules and the ACE 4710 A3(1.0) release only.</p>

Table 4-5 Virtual Server SSL Attributes

Field	Description
CRL Best-Effort	This option appears if you select an authentication group in the Auth Groups field. Check the check box to allow the ANM to search client certificates for the service to determine if it contains a CRL in the extension and retrieve the value, if it exists. Clear the check box to disable this feature.
CRL Name	This option appears if the CRL Best-Effort check box is clear. Select the Certificate Revocation List the ANM is to use for this proxy service.
Parameter Maps	Select the SSL parameter map to associate with this proxy server service.

- Step 6** When you finish configuring virtual server properties, click:
- **Deploy Now** to deploy this configuration on the ACE.
 - **Cancel** to exit this procedure without saving your entries.
 - **Deploy Later** to save your entries and apply them at a later time.

Related Topics

- [Configuring Virtual Servers, page 4-2](#)
- [Configuring Virtual Server Properties, page 4-8](#)

Configuring Virtual Server Protocol Inspection

Configuring protocol inspection allows the virtual server to verify protocol behavior and identify unwanted or malicious traffic passing through the ACE.

In the Advanced View, protocol inspection configuration is available for the following virtual server protocol configurations:

- TCP with FTP, HTTP, HTTPS, RTSP, or SIP
- UDP with DNS or SIP

In the Basic View, protocol inspection configuration is available for TCP with FTP.

See [Table 4-2](#) for a list of protocols by ACE device type.

Use this procedure to configure protocol inspection on a virtual server.

Assumption

A virtual server has been configured to use one of the protocols that supports protocol inspection in the Properties configuration subset. See [Configuring Virtual Server Properties, page 4-8](#) for information on configuring these protocols.

Procedure

- Step 1** Select the item to configure:
- To configure a virtual server, select **Config > Devices > context > Load Balancing > Virtual Servers**.
 - To configure a configuration building block, select **Config > Global > All Building Blocks > building_block > Load Balancing > Virtual Servers**.
- The Virtual Servers table appears.
- Step 2** Select the virtual server that you want to configure for protocol inspection, then click **Edit**. The Virtual Server configuration screen appears.
- Step 3** Click **Protocol Inspection**. The Enable Inspect check box appears.
- Step 4** Check the Enable Inspect check box to enable inspection on the specified traffic. Clear this check box to disable inspection on this traffic. By default, the ACE allows all request methods.
- Step 5** If you checked the Enable Inspect check box, configure additional inspection options using the information in [Table 4-6](#).

Table 4-6 Protocol Inspection Configuration Options

Protocol	Description
DNS	In the Length field enter the maximum length of the DNS packet in bytes. If you do not enter a value in this field, the DNS packet size is not checked.
FTP	<ol style="list-style-type: none"> Check the Use Strict check box to indicate that the virtual server is to perform enhanced inspection of FTP traffic and enforce compliance with RFC standards. Clear this check box to indicate that the virtual server is not to perform enhanced FTP inspection. If you checked the Use Strict check box, in the Blocked FTP Commands field, identify the commands that are to be denied by the virtual server. See Table 11-9 for more information about the FTP commands. <ul style="list-style-type: none"> Select the commands that are to be blocked by the virtual server in the Available Items list, then click Add. The commands appear in the Selected Items list. To remove commands that you do not want to be blocked, select them in the Selected Items list, then click Remove. The commands appear in the Available Items list.

Table 4-6 Protocol Inspection Configuration Options (continued)

Protocol	Description
HTTP or HTTPS	<ol style="list-style-type: none"> <li data-bbox="391 317 1466 443">1. Check the Logging Enabled check box to enable monitoring of Layer 3 and Layer 4 traffic. When enabled, this feature logs every URL request that is sent in the specified class of traffic, including the source or destination IP address and the URL that is accessed. Clear this check box to disable monitoring of Layer 3 and Layer 4 traffic. <li data-bbox="391 457 1466 548">2. In the Policy subset, click Add to add a new match condition and action, or select an existing match condition and action, then click Edit to modify it. The Policy configuration pane appears. <li data-bbox="391 562 1466 737">3. In the Matches field, select an existing class map or *New* or *Inline Match* to configure new match criteria for protocol inspection. If you select an existing class map, the screen refreshes and allows you to view, modify, or duplicate the selected class map. See Shared Objects and Virtual Servers, page 4-6 for more information about modifying shared objects. <li data-bbox="391 751 1317 779">4. Configure match criteria and related actions using the information in Table 4-7. <li data-bbox="391 793 1317 919">5. Click: <ul style="list-style-type: none"> <li data-bbox="444 842 1317 869">• OK to save your entries. The Conditions table refreshes with the new entry. <li data-bbox="444 884 1149 911">• Cancel to exit the Policy subset without saving your entries. <li data-bbox="391 934 1466 1083">6. In the Default Action field, select the default action that the virtual server is to take when specified match conditions for protocol inspection are not met: <ul style="list-style-type: none"> <li data-bbox="444 1010 1304 1037">• Permit—The specified HTTP traffic is to be received by the virtual server. <li data-bbox="444 1052 1271 1079">• Reset—The specified HTTP traffic is to be denied by the virtual server.

Table 4-6 Protocol Inspection Configuration Options (continued)

Protocol	Description
SIP	<ol style="list-style-type: none"> <li data-bbox="430 317 1502 411">1. In the Actions subset, click Add to add a new match condition and action, or select an existing match condition and action, then click Edit to modify it. The Actions configuration pane appears. <li data-bbox="430 422 1502 594">2. In the Matches field, select an existing class map or *New* or *Inline Match* to configure new match criteria for protocol inspection. If you select an existing class map, the screen refreshes and allows you to view, modify, or duplicate the selected class map. See Shared Objects and Virtual Servers, page 4-6 for more information about modifying shared objects. <li data-bbox="430 604 1356 636">3. Configure match criteria and related actions using the information in Table 4-9. <li data-bbox="430 646 1502 846">4. In the Action field, select the action that the virtual server is to take when the specified match conditions are met: <ul style="list-style-type: none"> <li data-bbox="479 730 1307 762">• Drop—The specified SIP traffic is to be discarded by the virtual server. <li data-bbox="479 772 1307 804">• Permit—The specified SIP traffic is to be received by the virtual server. <li data-bbox="479 814 1291 846">• Reset—The specified SIP traffic is to be denied by the virtual server. <li data-bbox="430 856 1461 1014">5. Click: <ul style="list-style-type: none"> <li data-bbox="479 909 1356 940">• OK to save your entries. The Conditions table refreshes with the new entry. <li data-bbox="479 951 1453 1014">• Cancel to exit the Conditions subset without saving your entries and to return to the Conditions table. <li data-bbox="430 1024 1421 1203">6. In the SIP Parameter Maps field, select an existing parameter map or select *New* to configure a new one. If you select an existing parameter map, the screen refreshes and allows you to view, modify, or delete the selected parameter map. See Shared Objects and Virtual Servers, page 4-6 for more information about modifying shared objects. <li data-bbox="430 1213 1291 1245">7. Configure SIP parameter map options using the information in Table 7-9. <li data-bbox="430 1255 1502 1434">8. In the Secondary Connection Parameter Map field, select an existing parameter map or select *New* to configure a new one. If you select an existing parameter map, the screen refreshes and allows you to view, modify, or delete the selected parameter map. See Shared Objects and Virtual Servers, page 4-6 for more information about modifying shared objects. <li data-bbox="430 1444 1485 1476">9. Configure secondary connection parameter map options using the information in Table 7-2. <li data-bbox="430 1486 1502 1686">10. In the Default Action field, select the default action that the virtual server is to take when specified match conditions for SIP protocol inspection are not met: <ul style="list-style-type: none"> <li data-bbox="479 1570 1307 1602">• Drop—The specified SIP traffic is to be discarded by the virtual server. <li data-bbox="479 1612 1307 1644">• Permit—The specified SIP traffic is to be received by the virtual server. <li data-bbox="479 1654 1291 1686">• Reset—The specified SIP traffic is to be denied by the virtual server. <li data-bbox="430 1696 1502 1833">11. Check the Logging Enabled check box to enable monitoring of Layer 3 and Layer 4 traffic. When enabled, this feature logs every URL request that is sent in the specified class of traffic, including the source or destination IP address and the URL that is accessed. Clear this check box to disable monitoring of Layer 3 and Layer 4 traffic.
RTSP	There are no protocol-specific inspection options for RTSP.

Table 4-7 HTTP and HTTPS Protocol Inspection Match Criteria Configuration

Selection	Action
Existing class map	<ol style="list-style-type: none"> 1. Click View to review the match condition information for the selected class map. 2. Click: <ul style="list-style-type: none"> • Cancel to continue without making changes and to return to the previous screen. • Edit to modify the existing configuration. • Duplicate to create a new class map with the same attributes without affecting other virtual servers using the same classmap. <p>See Shared Objects and Virtual Servers, page 4-6 for information about modifying shared objects.</p> 3. In the Action field, indicate the action that the virtual server is to perform on the traffic if it matches the specified match criteria: <ul style="list-style-type: none"> • Permit—The specified traffic is to be received by the virtual server if it meets the specified deep inspection match criteria. • Reset—The specified traffic is to be denied by the virtual server, which then sends a TCP reset message to the client or server to close the connection.
New	<ol style="list-style-type: none"> 1. In the Name field, specify a unique name for this class map. 2. In the Match field, select the method to be used to evaluate multiple match statements when multiple match conditions exist: <ul style="list-style-type: none"> • Any—A match exists if at least one of the match conditions is satisfied. • All—A match exists only if all match conditions are satisfied. 3. In the Conditions table, click Add to add a new set of conditions, or select an existing entry, then click Edit to modify it. The Type field appears. 4. In the Type field, select the type of condition that is to be met for protocol inspection. 5. Provide condition-specific criteria using the information in Table 4-8. 6. In the Action field, indicate the action that the virtual server is to perform on the traffic if it matches the specified match criteria: <ul style="list-style-type: none"> • Permit—The specified traffic is to be received by the virtual server if it meets the specified deep inspection match criteria. • Reset—The specified traffic is to be denied by the virtual server, which then sends a TCP reset message to the client or server to close the connection.
Inline Match	<ol style="list-style-type: none"> 1. In the Conditions Type field, select the type of inline match condition that is to be met for protocol inspection. 2. Provide condition-specific criteria using the information in Table 4-8. 3. In the Action field, indicate the action that the virtual server is to perform on the traffic if it matches the specified match criteria: <ul style="list-style-type: none"> • Permit—The specified traffic is to be received by the virtual server if it meets the specified deep inspection match criteria. • Reset—The specified traffic is to be denied by the virtual server, which then sends a TCP reset message to the client or server to close the connection.

Table 4-8 HTTP and HTTPS Protocol Inspection Conditions and Options

Condition	Description
Content	<p>Specific content contained within the HTTP entity-body is to be used for application inspection decisions.</p> <ol style="list-style-type: none"> In the Content Expression field, enter the content that is to be matched. Valid entries are alphanumeric strings from 1 to 255 characters. In the Content Offset field, enter the number of bytes to be ignored starting with the first byte of the Message body, after the empty line (CR,LF,CR,LF) between the headers and the body of the message. Valid entries are from 1 to 255 bytes.
Content Length	<p>The content parse length is used for application inspection decisions.</p> <ol style="list-style-type: none"> In the Content Length Operator field, select the operand to use to compare content length: <ul style="list-style-type: none"> Equal To—The content length must equal the number in the Content Length Value field. Greater Than—The content length must be greater than the number in the Content Length Value field. Less Than—The content length must be less than the number in the Content Length Value field. Range—The content length must be within the range specified in the Content Length Lower Value field and the Content Length Higher Value field. Enter values to apply for content length comparison: <ul style="list-style-type: none"> If you select Equal To, Greater Than, or Less Than in the Content Length Operator field, the Content Length Value field appears. In the Content Length Value field, enter the number of bytes for comparison. Valid entries are integers from 0 to 4294967295. If you select Range in the Content Length Operator field, the Content Length Lower Value and the Content Length Higher Value fields appear: <ol style="list-style-type: none"> In the Content Length Lower Value field, enter the lowest number of bytes to be used for this match condition. Valid entries are integers from 0 to 4294967295. The number in this field must be less than the number entered in the Content Length Higher Value field. In the Content Length Higher Value field, enter the highest number of bytes to be used for this match condition. Valid entries are integers from 0 to 4294967295. The number in this field must be greater than the number entered in the Content Length Lower Value field.
Content Type Verification	<p>Verification of MIME-type messages with the header MIME-type is to be used for application inspection decisions. This option verifies that the header MIME-type value is in the internal list of supported MIME-types and that the header MIME-type matches the content in the data or body portion of the message.</p>

Table 4-8 HTTP and HTTPS Protocol Inspection Conditions and Options (continued)

Condition	Description
Header	<p>The name and value in an HTTP header are used for application inspection decisions.</p> <ol style="list-style-type: none"> In the Header field, select one of the predefined HTTP headers to match, or select HTTP Header to specify a different HTTP header. If you select HTTP Header, in the Header Name field, enter the name of the HTTP header to match. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters. In the Header Value field, enter the header-value expression string to compare against the value in the specified field in the HTTP header. Valid entries are text strings with a maximum of 255 alphanumeric characters. The ACE supports regular expressions for matching. Header expressions allow spaces, provided that the spaces are escaped or quoted. All headers in the header map must be matched. See Table 11-35 for a list of the supported characters that you can use in regular expressions.
Header Length	<p>The length of the header in the HTTP message is used for application inspection decisions.</p> <ol style="list-style-type: none"> In the Header Length Type field, specify whether HTTP header request or response messages are to be used for application inspection decisions: <ul style="list-style-type: none"> Request—HTTP header request messages are to be checked for header length. Response—HTTP header response messages are to be checked for header length. In the Header Length Operator field, select the operand to be used to compare header length: <ul style="list-style-type: none"> Equal To—The header length must equal the number in the Header Length Value field. Greater Than—The header length must be greater than the number in the Header Length Value field. Less Than—The header length must be less than the number in the Header Length Value field. Range—The header length must be within the range specified in the Header Length Lower Value field and the Header Length Higher Value field. Enter values to apply for header length comparison: <ul style="list-style-type: none"> If you select Equal To, Greater Than, or Less Than in the Header Length Operator field, the Header Length Value field appears. In the Header Length Value field, enter the number of bytes for comparison. Valid entries are integers from 0 to 255. If you select Range in the Header Length Operator field, the Header Length Lower Value and the Header Length Higher Value fields appear: <ol style="list-style-type: none"> In the Header Length Lower Value field, enter the lowest number of bytes to be used for this match condition. Valid entries are integers from 0 to 255. The number in this field must be less than the number entered in the Header Length Higher Value field. In the Header Length Higher Value field, enter the highest number of bytes to be used for this match condition. Valid entries are integers from 1 to 255. The number in this field must be greater than the number entered in the Header Length Lower Value field.
Header MIME Type	<p>Multipurpose Internet Mail Extension (MIME) message types are used for application inspection decisions.</p> <p>In the Header MIME Type field, select the MIME message type to use for this match condition.</p>

Table 4-8 HTTP and HTTPS Protocol Inspection Conditions and Options (continued)

Condition	Description
Port Misuse	<p>The misuse of port 80 (or any other port running HTTP) is to be used for application inspection decisions.</p> <p>Indicate the application category to use for this match condition:</p> <ul style="list-style-type: none"> • IM—Instant messaging applications are to be checked. • P2P—Peer-to-peer applications are to be checked. • Tunneling—Tunneling applications are to be checked.
Request Method	<p>A request method is to be used for application inspection decisions.</p> <ol style="list-style-type: none"> 1. Select the type of request method to use for this match condition: <ul style="list-style-type: none"> • Ext—An HTTP extension method is to be used. • RFC—The request method defined in RFC 2616 is to be used. 2. In the Request Method field, select the request method that is to be inspected.
Strict HTTP	<p>Compliance with HTTP RFC 2616 is to be used for application inspection decisions.</p>
Transfer Encoding	<p>An HTTP transfer-encoding type is to be used for application inspection decisions. The transfer-encoding general-header field indicates the type of transformation, if any, that has been applied to the HTTP message body to safely transfer it between the sender and the recipient.</p> <p>In the Transfer Encoding field, select the type of encoding that is to be checked:</p> <ul style="list-style-type: none"> • Chunked—The message body is transferred as a series of chunks. • Compress—The encoding format that is produced by the UNIX file compression program <i>compress</i>. • Deflate—The .zlib format that is defined in RFC 1950 in combination with the DEFLATE compression mechanism described in RFC 1951. • Gzip—The encoding format that is produced by the file compression program GZIP (GNU zip) as described in RFC 1952. • Identity—The default (identity) encoding which does not require the use of transformation.

Table 4-8 HTTP and HTTPS Protocol Inspection Conditions and Options (continued)

Condition	Description
URL	<p>URL names are to be used for application inspection decisions.</p> <p>In the URL field, enter a URL or a portion of a URL to match. Valid entries are URL strings from 1 to 255 alphanumeric characters and include only the portion of the URL following <code>www.hostname.domain</code>. For example, in the URL <code>www.anydomain.com/latest/whatsnew.html</code>, include only <code>/latest/whatsnew.html</code>.</p>
URL Length	<p>URL length is to be used for application inspection decisions.</p> <ol style="list-style-type: none"> In the URL Length Operator field, select the operand to use to compare URL length: <ul style="list-style-type: none"> Equal To—The URL length must equal the number in the URL Length Value field. Greater Than—The URL length must be greater than the number in the URL Length Value field. Less Than—The URL length must be less than the number in the URL Length Value field. Range—The URL length must be within the range specified in the URL Length Lower Value field and the URL Length Higher Value field. Enter values to apply for URL length comparison: <ul style="list-style-type: none"> If you select Equal To, Greater Than, or Less Than in the URL Length Operator field, the URL Length Value field appears. In the URL Length Value field, enter the value for comparison. Valid entries are from 1 to 65535 bytes. If you select Range in the URL Length Operator field, the URL Length Lower Value and the URL Length Higher Value fields appear: <ol style="list-style-type: none"> In the URL Length Lower Value field, enter the lowest number of bytes to be used for this match condition. Valid entries are integers from 1 to 65535. The number in this field must be less than the number entered in the URL Length Higher Value field. In the URL Length Higher Value field, enter the highest number of bytes to be used for this match condition. Valid entries are integers from 1 to 65535. The number in this field must be greater than the number entered in the URL Length Lower Value field.

Table 4-9 SIP Protocol Inspection Match Criteria Configuration

Selection	Action
Existing class map	<ol style="list-style-type: none"> 1. Click View to review the match condition information for the selected class map. 2. Click: <ul style="list-style-type: none"> • Cancel to continue without making changes and to return to the previous screen. • Edit to modify the existing configuration. • Duplicate to create a new class map with the same attributes without affecting other virtual servers using the same classmap. <p>See Shared Objects and Virtual Servers, page 4-6 for more information about modifying shared objects.</p> 3. In the Action field, indicate the action that the virtual server is to perform on the traffic if it matches the specified match criteria: <ul style="list-style-type: none"> • Drop—The specified traffic is to be dropped by the virtual server. • Permit—The specified traffic is to be received by the virtual server. • Reset—The specified traffic is to be denied by the virtual server, which then sends a TCP reset message to the client or server to close the connection.
New	<ol style="list-style-type: none"> 1. In the Name field, specify a unique name for this class map. 2. In the Conditions table, click Add to add a new set of conditions, or select an existing entry, then click Edit to modify it. The Type field appears. 3. In the Type field, select the type of condition that is to be met for protocol inspection. 4. Provide condition-specific criteria using the information in Table 4-10. 5. In the Action field, indicate the action that the virtual server is to perform on the traffic if it matches the specified match criteria: <ul style="list-style-type: none"> • Drop—The specified traffic is to be dropped by the virtual server. • Permit—The specified traffic is to be received by the virtual server. • Reset—The specified traffic is to be denied by the virtual server, which then sends a TCP reset message to the client or server to close the connection.
Inline Match	<ol style="list-style-type: none"> 1. In the Conditions Type field, select the type of inline match condition that is to be met for protocol inspection. Table 4-10 describes the types of conditions and their related configuration options. 2. Provide condition-specific criteria using the information in Table 4-10. 3. In the Action field, indicate the action that the virtual server is to perform on the traffic if it matches the specified match criteria: <ul style="list-style-type: none"> • Drop—The specified traffic is to be dropped by the virtual server. • Permit—The specified traffic is to be received by the virtual server. • Reset—The specified traffic is to be denied by the virtual server, which then sends a TCP reset message to the client or server to close the connection.

Table 4-10 SIP Protocol Inspection Conditions and Options

Condition	Description
Called Party	<p>The destination or called party specified in the URI of the SIP To header is used for SIP protocol inspection decisions.</p> <p>In the Called Party field, enter a regular expression that identifies the called party in the URI of the SIP To header for this match condition. Valid entries are unquoted text strings with no spaces and a maximum of 255 alphanumeric characters. The ACE supports regular expressions for matching string expressions. Table 11-35 lists the supported characters that you can use for matching string expressions.</p>
Calling Party	<p>The source or caller specified in the URI of the SIP From header is used for SIP protocol inspection decisions.</p> <p>In the Calling Party field, enter a regular expression that identifies the calling party in the URI of the SIP From header for this match condition. Valid entries are unquoted text strings with no spaces and a maximum of 255 alphanumeric characters. The ACE supports regular expressions for matching string expressions. Table 11-35 lists the supported characters that you can use for matching string expressions.</p>
IM Subscriber	<p>An IM (instant messaging) subscriber is used for application inspection decisions.</p> <p>In the IP Subscriber field, enter a regular expression that identifies the IM subscriber for this match condition. Valid entries are unquoted text strings with no spaces and a maximum of 255 alphanumeric characters. The ACE supports regular expressions for matching string expressions. Table 11-35 lists the supported characters that you can use for matching string expressions.</p>
Message Path	<p>SIP inspection allows you to filter messages coming from or transiting through certain SIP proxy servers. The ACE maintains a list of the unauthorized SIP proxy IP addresses or URLs in the form of regular expressions and checks this list against the VIA header field in each SIP packet.</p> <p>In the Message Path field, enter a regular expression that identifies the SIP proxy server for this match condition. Valid entries are unquoted text strings with no spaces and a maximum of 255 alphanumeric characters. The ACE supports regular expressions for matching string expressions. Table 11-35 lists the supported characters that you can use for matching string expressions.</p>
SIP Content Length	<p>The SIP message body content length is used for SIP protocol inspection decisions.</p> <p>To specify SIP traffic based on SIP message body length:</p> <ol style="list-style-type: none"> 1. In the Content Operator field, confirm that Greater Than is selected. 2. In the Content Length field, enter the maximum size of a SIP message body in bytes that the ACE is to allow without performing SIP protocol inspection. If a SIP message exceeds the specified value, the ACE performs SIP protocol inspection as defined in an associated policy map. Valid entries are integers from 0 to 65534 bytes.
SIP Content Type	<p>The content type in the SIP message body is used for SIP protocol inspection decisions.</p> <p>In the Content Type field, enter a regular expression that identifies the content type in the SIP message body to use for this match condition. Valid entries are unquoted text strings with no spaces and a maximum of 255 alphanumeric characters. The ACE supports regular expressions for matching string expressions. Table 11-35 lists the supported characters that you can use for matching string expressions.</p>

Table 4-10 SIP Protocol Inspection Conditions and Options (continued)

Condition	Description
SIP Request Method	A SIP request method is used for application inspection decisions. In the Request Method field, select the request method that is to be inspected.
Third Party	SIP allows users to register other users on their behalf by sending REGISTER messages with different values in the From and To header fields. This process can pose a security threat if the REGISTER message is actually a Deregister message. A malicious user could cause a DoS (denial-of-service) attack by deregistering all users on their behalf. To prevent this security threat, you can specify a list of privileged users who can register or unregister someone else on their behalf. The ACE maintains the list as a regex table. If you configure this policy, the ACE drops REGISTER messages with mismatched From and To headers and a From header value that does not match any of the privileged user IDs. In the Third Party Registration Entities field, enter a regular expression that identifies a privileged user who is authorized for third-party registrations. Valid entries are unquoted text strings with no spaces and a maximum of 255 alphanumeric characters. The ACE supports regular expressions for matching string expressions. Table 11-35 lists the supported characters that you can use for matching string expressions.
URI Length	The ACE can validate the length of SIP URIs or Tel URIs. A SIP URI is a user identifier that a calling party (source) uses to contact the called party (destination). A Tel URI is a telephone number that identifies the endpoint of a SIP connection. For more information about SIP URIs and Tel URIs, see RFC 2534 and RFC 3966, respectively. To filter SIP traffic based on URIs: <ol style="list-style-type: none"> In the URI Type field, indicate the type of URI to be used: <ul style="list-style-type: none"> SIP URI—The calling party URI is to be used for this match condition. Tel URI—A telephone number is to be used for this match condition. In the URI Operator field, confirm that Greater Than is selected. In the URI Length field, enter the maximum length of the SIP URI or Tel URI in bytes. Valid entries are integers from 0 to 254 bytes.

- Step 6** When you finish configuring virtual server properties, click:
- **Deploy Now** to deploy this configuration on the ACE.
 - **Cancel** to exit this procedure without saving your entries.
 - **Deploy Later** to save your entries and deploy the configuration at a later time.

Related Topics

- [Configuring Virtual Server Properties, page 4-8](#)
- [Configuring Virtual Server SSL Termination, page 4-13](#)
- [Configuring Virtual Server Layer 7 Load Balancing, page 4-26](#)

Configuring Virtual Server Layer 7 Load Balancing

In the Advanced View, Layer 7 load balancing is available for virtual servers configured with one of the following protocol combinations:

- TCP with Generic, HTTP, HTTPS, RTSP, or SIP
- UDP with Generic, RADIUS, or SIP

See [Configuring Virtual Server Properties, page 4-8](#) for information on configuring these protocols.

[Table 4-2](#) identifies the protocols that are available for each type of ACE device.

Use this procedure to configure Layer 7 load balancing on a virtual server.

Assumption

A virtual server has been configured with one of the following protocol combinations:

- TCP with Generic, HTTP, HTTPS, RTSP, or SIP
- UDP with Generic, RADIUS, or SIP

Procedure

-
- Step 1** Select **Config > Devices > context > Load Balancing > Virtual Servers**. The Virtual Servers table appears.
 - Step 2** Select the virtual server you want to configure for Layer 7 load balancing, then click **Edit**. The Virtual Server configuration screen appears.
 - Step 3** Click **L7 Load-Balancing**. The Layer 7 Load-Balancing Rule Match table appears.
 - Step 4** In the Rule Match table, click **Add** to add a new match condition and action, or select an existing match condition and action, then click **Edit** to modify it. The Rule Match configuration pane appears.
 - Step 5** In the Rule Match field, select an existing class map or ***New*** or ***Inline Match*** to configure new match criteria for Layer 7 load balancing:
 - If you select an existing class map, click **View** to review, modify, or duplicate the existing configuration. See [Shared Objects and Virtual Servers, page 4-6](#) for more information about modifying shared objects.
 - If you click ***New*** or ***Inline Match***, the Rule Match configuration pane appears.

Step 6 Configure match criteria using the information in [Table 4-11](#).

Table 4-11 Layer 7 Load-Balancing Match Criteria Configuration

Selection	Action
Existing class map	<ol style="list-style-type: none"> 1. Click View to review the match condition information for the selected class map. 2. Click: <ul style="list-style-type: none"> • Cancel to continue without making changes and to return to the previous screen. • Edit to modify the existing configuration. • Duplicate to create a new class map with the same attributes without affecting other virtual servers using the same classmap. <p>See Shared Objects and Virtual Servers, page 4-6 for more information about modifying shared objects.</p>
New	<ol style="list-style-type: none"> 1. In the Name field, enter a unique name for this class map. 2. In the Match field, select the method to be used to evaluate multiple match statements when multiple match conditions exist: <ul style="list-style-type: none"> • match-any—A match exists if at least one of the match conditions is satisfied. • match-all—A match exists only if all match conditions are satisfied. 3. In the Conditions table, click Add to add a new set of conditions or select an existing entry, then click Edit to modify it. 4. In the Type field, select the match condition and configure any protocol-specific options: <ul style="list-style-type: none"> • For Generic protocol options, see Table 11-10. • For HTTP and HTTPS protocol options, see Table 4-12. • For RADIUS protocol options, see Table 11-11. • For RTSP protocol options, see Table 11-12. • For SIP protocol options, see Table 11-13. 5. Click: <ul style="list-style-type: none"> • OK to accept your entries and to return to the Conditions table. • Cancel to exit this procedure without saving your entries and to return to the Conditions table.
Inline Match	<p>In the Conditions Type field, select the type of inline match condition and configure any protocol-specific options:</p> <ul style="list-style-type: none"> • For Generic protocol options, see Table 11-10. • For HTTP and HTTPS protocol options, see Table 4-12. • For RADIUS protocol options, see Table 11-11. • For RTSP protocol options, see Table 11-12. • For SIP protocol options, see Table 11-13.

Table 4-12 Layer 7 HTTP/HTTPS Load-Balancing Conditions and Options


Match Condition	Description
Class Map	<p>An existing class map is used for the match condition.</p> <p>In the Class Map field, select the class map to be used.</p>
HTTP Content	<p> Note This option appears for ACE 2.0 modules and the ACE 4710 A3(1.0) release only.</p> <p>Specific content contained within the HTTP entity-body is used to establish a match condition.</p> <ol style="list-style-type: none"> In the Content Expression field, enter the content that is to be matched. Valid entries are alphanumeric strings from 1 to 255 characters. In the Content Offset field, enter the number of bytes to be ignored starting with the first byte of the Message body, after the empty line (CR,LF,CR,LF) between the headers and the body of the message. Valid entries are integers from 1 to 255.
HTTP Cookie	<p>HTTP cookies are used for the match condition.</p> <ol style="list-style-type: none"> In the Cookie Name field, enter a unique cookie name. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters. In the Cookie Value field, enter a unique cookie value expression. Valid entries are unquoted text strings with no spaces and a maximum of 255 alphanumeric characters. The ACE supports regular expressions for matching string expressions. Table 11-35 lists the supported characters that you can use for matching string expressions. Check the Secondary Cookie Matching check box to indicate that the ACE is to use both the cookie name and the cookie value to satisfy this match condition. Clear this check box to indicate that the ACE is to use either the cookie name or the cookie value to satisfy this match condition.
HTTP Header	<p>An HTTP header and corresponding value are used to establish match conditions.</p> <ol style="list-style-type: none"> In the Header Name field, specify the header in one of the following ways: <ul style="list-style-type: none"> To specify an HTTP header that is not one of the standard HTTP headers, select the first radio button and enter the HTTP header name in the Header Name field. Enter an unquoted text string with no spaces and a maximum of 64 characters. To specify one of the standard HTTP headers, select the second radio button and select the desired HTTP header from the list. In the Header Value field, enter the header-value expression string to compare against the value in the specified field in the HTTP header. Valid entries are text strings with a maximum of 255 alphanumeric characters. The ACE supports regular expressions for matching. Header expressions allow spaces, provided that the spaces are escaped or quoted. All headers in the header map must be matched. Table 11-35 lists the supported characters that you can use in regular expressions.

Table 4-12 Layer 7 HTTP/HTTPS Load-Balancing Conditions and Options (continued)

Match Condition	Description
HTTP URL	<p>The ACE performs regular expression matching against the received packet data from a particular connection based on the HTTP URL string.</p> <ol style="list-style-type: none"> 1. In the URL Expression field, enter a URL, or portion of a URL, to match. Valid entries are URL strings from 1 to 255 alphanumeric characters. Include only the portion of the URL following www.hostname.domain in the match statement. For example, in the URL www.anydomain.com/latest/whatsnew.html, include only /latest/whatsnew.html. To match the www.anydomain.com portion, the URL string can take the form of a URL regular expression. The ACE supports regular expressions for matching URL strings. Table 11-35 lists the supported characters that you can use in regular expressions. 2. In the Method Expression field, enter the HTTP method to match. Valid entries are unquoted text strings with no spaces and a maximum of 15 alphanumeric characters. The method can either be one of the standard HTTP 1.1 method names (OPTIONS, GET, HEAD, POST, PUT, DELETE, TRACE, or CONNECT) or a text string that must be matched exactly (for example, CORVETTE).
Source Address	<p>A client source IP address is used for the match condition.</p> <ol style="list-style-type: none"> 1. In the Source Address field, enter the source IP address of the client. Enter the IP address in dotted-decimal notation (for example, 192.168.11.2). 2. In the Source Netmask field, select the subnet mask to apply to the source IP address.

- Step 7** In the Primary Action field, indicate the action that the virtual server is to perform on the traffic if it matches the specified match criteria:
- Drop—Client requests for content are to be discarded when match conditions are met. Continue with [Step 11](#).
 - Forward—Client requests for content are to be forwarded without performing load balancing on the requests when match conditions are met. Continue with [Step 11](#).
 - Loadbalance—Client requests for content are to be directed to a server farm when match conditions are met. Continue with [Step 8](#).
 - Sticky—Client requests for content are to be handled by a sticky group when match conditions are met. Continue with [Step 9](#).

- Step 8** If you select Loadbalance as the primary action:
- a. In the Server Farm field, select the primary server farm to use for load balancing, or select ***New*** to configure a new server farm (see [Table 4-13](#)).
 - b. In the Backup Server Farm field, select the server farm to act as the backup server farm for load balancing if the primary server farm is unavailable, or select ***New*** to configure a new backup server farm (see [Table 4-13](#)).



Note If you select an existing object in either of these fields, you can view, modify, or duplicate the selected object's existing configuration. See [Shared Objects and Virtual Servers, page 4-6](#) for more information about modifying shared objects in virtual servers.

Table 4-13 New Server Farm Attributes

Field	Description
Name	Enter a unique name for the server farm. Valid entries are unquoted text strings with no spaces and a maximum of 64 characters.
Type	<p>Select the type of server farm:</p> <ul style="list-style-type: none"> • Host—A typical server farm that consists of real servers that provide content and services to clients. By default, if you configure a backup server farm and all real servers in the primary server farm go down, the primary server farm fails over to the backup server farm. Use the following options to specify thresholds for failover and returning to service. <ul style="list-style-type: none"> a. In the Partial-Threshold Percentage field, enter the minimum percentage of real servers in the primary server farm that must remain active for the server farm to stay up. If the percentage of active real servers falls below this threshold, the ACE takes the server farm out of service. Valid entries are integers from 0 to 99. b. In the Back Inservice field, enter the percentage of real servers in the primary server farm that must be active again for the ACE to place the server farm back into service. Valid entries are integers from 0 to 99. The value in this field should be larger than the value in the Partial Threshold Percentage field. • Redirect—A server farm that consists only of real servers that redirect client requests to alternate locations specified in the real server configuration.
Fail Action	<p>Select the action the ACE is to take if any real server in the server farm fails:</p> <ul style="list-style-type: none"> • N/A—Indicates that the ACE is to take no action if any server in the server farm fails. • Purge—Indicates that the ACE is to remove connections to a real server if that real server in the server farm fails. The ACE sends a reset command to both the client and the server that failed. • Reassign—Indicates that the ACE reassign the existing server connections to the backup real server (if configured) if the real server fails after you enter this command. If a backup real server has not been configured for the failing server, this selection leaves the existing connections untouched in the failing real server.
Transparent	<p>This field appears only for real servers identified as host servers.</p> <p>Specify whether network address translation from the VIP address to the server IP is to occur:</p> <ul style="list-style-type: none"> • N/A—Indicates that the default value is to be used; the default value is False. • False—Indicates that network address translation from the VIP address to the server IP address is not to occur. • True—Indicates that network address translation from the VIP address to the server IP address is to occur.

Table 4-13 ***New Server Farm Attributes (continued)***

Field	Description
Fail-On-All	<p>This field appears only for host server farms.</p> <p>By default, real servers that you configure in a server farm inherit the probes that you configure directly on that server farm. When you configure multiple probes on a server farm, the real servers in the server farm use an OR logic with respect to the probes, which means that if one of the probes configured on the server farm fails, all the real servers in that server farm fail and enter the PROBE-FAILED state.</p> <p>With AND logic, if one server farm probe fails, the real servers in the server farm remain in the OPERATIONAL state. If all the probes associated with the server farm fail, then all the real servers in that server farm fail and enter the PROBE-FAILED state. You can also configure AND logic for probes that you configure directly on real servers in a server farm. For more information, see the command in server farm host real server configuration mode.</p> <p>Check this checkbox to configure the real servers in a server farm to use AND logic with respect to multiple server farm probes.</p> <p>The Fail On All function is applicable to all probe types.</p>
Predictor	<p>Specify the method for selecting the next server in the server farm to respond to client requests. Round Robin is the default predictor method for a server farm.</p> <p>See Table 4-14 for the supported predictor methods and configurable attributes for each predictor method.</p>

Table 4-13 New Server Farm Attributes (continued)

Field	Description
Probes	<p>Specify the health monitoring probes to use:</p> <ul style="list-style-type: none"> To include a probe that you want to use for health monitoring, select it in the Available list, then click Add. The probe appears in the Selected list. To remove a probe that you do not want to use for health monitoring, select it in the Selected list, then click Remove. The probe appears in the Available list. To specify a sequence for probe use, select probes in the Selected list, then click Up or Down until you have the desired sequence. To view the configuration for an existing probe, select a probe in the list on the right, then click View to review its configuration. <p>To add a new probe, click Create. See Configuring Health Monitoring for Real Servers, page 5-28 for details on adding a new health monitoring probe and defining attributes for the specific probe type. In addition to the probe attributes that you set as described in the Configuring Health Monitoring for Real Servers section, set the following probe configuration parameters in the Probes section under Server Farm as described below:</p> <ul style="list-style-type: none"> Expect Addresses—To configure expect addresses for a DNS probe, in the Expect Addresses field enter the IP address that the ACE appliance is to expect as a server response to a DNS request. Valid entries are unique IP addresses in dotted-decimal notation, such as 192.168.11.1. Probe Headers—To configure probe headers for either an HTTP or HTTPS probe, in the Probe Headers field enter the name of the HTTP header and the value to be matched using the format <i>header_name=header_value</i> where: <ul style="list-style-type: none"> <i>header_name</i> represents the HTTP header name the probe is to use. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters. You can specify predefined header or any custom header name provided that it does not exceed the maximum length limit. <i>header_value</i> represents the string to assign to the header field. Valid entries are text strings with a maximum of 255 characters. If the string includes spaces, enclose the string with quotes. Probe Expect Status—To configure probe expect status for an FTP, HTTP, HTTPS, RTSP, SIP-TCP, SIP-UDP, or SMTP probe, in the Probe Expect Status field enter the following information: <ul style="list-style-type: none"> To configure a single expect status code, enter the minimum expect status code for this probe followed by the same expect status code that you entered as the minimum. Valid entries are integers from 0 to 999. To configure a range of expect status codes, enter the lower limit of the range of status codes followed by the upper limit of the range of status codes. The maximum expect status code must be greater than or equal to the value specified for the minimum expect status code. Valid entries are integers from 0 to 999. SNMP OID Table—To configure the SNMP OID for an SNMP probe, see Configuring an OID for SNMP Probes, page 5-51. <p>After you add a probe, you can modify the attributes for a health probe from the Health Monitoring table (Config > Virtual Contexts > context > Load Balancing > Health Monitoring) as described in Configuring Health Monitoring for Real Servers, page 5-28. You can also delete an existing health probe from the Health Monitoring table.</p>

Table 4-13 New Server Farm Attributes (continued)

Field	Description
Real Servers	<p>The Real Servers table allows you to add, modify, remove, or change the order of real servers.</p> <ol style="list-style-type: none"> 1. Select an existing server, or click Add to add a server to the server farm: <ul style="list-style-type: none"> • If you select an existing server, you can view, modify, or duplicate the server's existing configuration. See Shared Objects and Virtual Servers, page 4-6 for more information about modifying shared objects. • If you click Add, the screen refreshes so you can enter server information. 2. In the Name field, specify the name of the real server in one of the following ways: <ul style="list-style-type: none"> • To identify a new real server, select the first radio button, then enter the name of the real server in the adjoining field. • To specify an existing real server, select the second radio button, then select one of the real servers listed. 3. In the IP Address field, enter the IP address of the real server in dotted-decimal format. 4. In the Port field, enter the port number to be used for server port address translation (PAT). Valid entries are integers from 1 to 65535. 5. In the Weight field, enter the weight to assign to this server in the server farm. Valid entries are integers from 1 to 100, and the default is 8. 6. In the Redirection Code field, select the appropriate redirection code. This field appears only for real servers identified as redirect servers. <ul style="list-style-type: none"> • N/A—Indicates that the webhost redirection code is not defined. • 301—Indicates that the requested resource has been moved permanently. For future references to this resource, the client should use one of the returned URIs. • 302—Indicates that the requested resource has been found, but has been moved temporarily to another location. For future references to this resource, the client should use the request URI because the resource may be moved to other locations from time to time. 7. In the Web Host Redirection field, enter the URL string used to redirect requests to another server. This field appears only for real servers identified as redirect servers. Enter the URL and port used to redirect requests to another server. Valid entries are in the form <code>http://host.com:port</code> where host is the name of the server and port is the port to be used. Valid host entries are unquoted text strings with no spaces and a maximum of 255 characters. Valid port numbers are from 1 to 65535. <p>The relocation string supports the following special characters:</p> <ul style="list-style-type: none"> • %h—Inserts the hostname from the request Host header • %p—Inserts the URL path string from the request 8. In the Rate Bandwidth field, enter the real server bandwidth limit in bytes per second. Valid entries are integers from 1 to 300000000 bytes. 9. In the Rate Connection field, enter the limit for connections per second. Valid entries are integers from 1 to 350000. <ul style="list-style-type: none"> • OK to accept your entries and add this real server to the server farm. The table refreshes with updated information. • Cancel to exit this procedure without saving your entries and to return to the Real Servers table.

Table 4-13 *New Server Farm Attributes (continued)*

Field	Description
	<p>10. In the State field, select the administrative state of this server:</p> <ul style="list-style-type: none"> • In Service—The server is to be placed in use as a destination for server load balancing • In Service Standby—The server is a backup server and remains inactive unless the primary server fails. If the primary server fails, the backup server becomes active and starts accepting connections. • Out Of Service—The server is not to be placed in use by a server load balancer as a destination for client connections. <p>11. In the Fail-On-All field, check this checkbox to configure a real server to remain in the OPERATIONAL state unless all probes associated with it fail (AND logic). The Fail-On-All function is applicable to all probe types. Fail-On-All is applicable only for host real servers.</p> <p>12. Click:</p> <ul style="list-style-type: none"> • OK to accept your entries and add this real server to the server farm. The table refreshes with updated information. • Cancel to exit this procedure without saving your entries and to return to the Real Servers table.

Table 4-14 *Predictor Methods and Attributes*

Predictor Method	Description / Action
Hash Address	<p>Indicates that the ACE is to select the server using a hash value based on the source or destination IP address.</p> <p>To configure the hash address predictor method:</p> <ol style="list-style-type: none"> 1. In the Mask Type field, indicate whether server selection is based on the source IP address or the destination IP address: <ul style="list-style-type: none"> • N/A—Indicates that this option is not defined. • Source—Indicates that the server is selected based on the source IP address. • Destination—Indicates that the server is selected based on the destination IP address. 2. In the IP Netmask field, select the subnet mask to apply to the address. If none is specified, the default is 255.255.255.255.

Table 4-14 Predictor Methods and Attributes (continued)

Hash Content	<p>The ACE selects the server by using a hash value based on the specified content string of the HTTP packet body.</p> <ol style="list-style-type: none"> In the Begin Pattern field, enter the beginning pattern of the content string and the pattern string to match before hashing. If you do not specify a beginning pattern, the ACE starts parsing the HTTP body immediate following the offset byte. You cannot configure different beginning and ending patterns for different server farms that are part of the same traffic classification. Valid entries are unquoted text strings with no spaces and a maximum of 255 alphanumeric characters. The ACE supports regular expressions for matching string expressions. Table 11-35 lists the supported characters that you can use for matching string expressions. In the End Pattern field, enter the pattern that marks the end of hashing. If you do not specify either a length or an end pattern, the ACE continues to parse the data until it reaches the end of the field or the end of the packet, or until it reaches the maximum body parse length. You cannot configure different beginning and ending patterns for different server farms that are part of the same traffic classification. Valid entries are unquoted text strings with no spaces and a maximum of 255 alphanumeric characters. The ACE supports regular expressions for matching string expressions. Table 11-35 lists the supported characters that you can use for matching string expressions. In the Length field, enter the length in bytes of the portion of the content (starting with the byte after the offset value) that the ACE uses for sticking the client to the server. Valid entries are integers from 1 to 1000 bytes. The offset and length can vary from 0 to 1000 bytes. If the payload is longer than the offset but shorter than the offset plus the length of the payload, the ACE sticks the connection based on that portion of the payload starting with the byte after the offset value and ending with the byte specified by the offset plus the length. The total of the offset and the length cannot exceed 1000. <p>Note You cannot specify both the length and the end-pattern options for a Hash Content predictor.</p> <ol style="list-style-type: none"> In the HTTP Content Offset field, enter the portion of the content that the ACE uses to stick the client on a particular server by indicating the bytes to ignore starting with the first byte of the payload. Valid entries are integers from 0 to 999 bytes. The default is 0, which indicates that the ACE does not exclude any portion of the content.
Hash Cookie	<p>Indicates that the ACE is to select the server by using a hash value based on the cookie name.</p> <p>In the Cookie Name field, enter a cookie name in the form of an unquoted text string with no spaces and a maximum of 64 characters.</p>
Hash Header	<p>Indicates that the ACE is to select the server by using a hash value based on the header name.</p> <p>In the Header Name field, select the HTTP header to be used for server selection:</p> <ul style="list-style-type: none"> To specify an HTTP header that is not one of the standard HTTP headers, select the first radio button and enter the HTTP header name in the Header Name field. Valid entries are unquoted text strings with no spaces and a maximum of 64 characters. To specify one of the standard HTTP headers, select the second radio button, then select one of the HTTP headers from the list.

Table 4-14 Predictor Methods and Attributes (continued)

Hash Layer 4	<p>The ACE selects the server by using a Layer 4 generic protocol load-balancing method. Use this predictor to load balance packets from protocols that are not explicitly supported by the ACE.</p> <ol style="list-style-type: none"> In the Begin Pattern field, enter the beginning pattern of the Layer 4 payload and the pattern string to match before hashing. If you do not specify a beginning pattern, the ACE starts parsing the HTTP body immediate following the offset byte. You cannot configure different beginning and ending patterns for different server farms that are part of the same traffic classification. <p>Valid entries are unquoted text strings with no spaces and a maximum of 255 alphanumeric characters. The ACE supports regular expressions for matching string expressions. Table 11-35 lists the supported characters that you can use for matching string expressions.</p> <ol style="list-style-type: none"> In the End Pattern field, enter the pattern that marks the end of hashing. If you do not specify either a length or an end pattern, the ACE continues to parse the data until it reaches the end of the field or the end of the packet, or until it reaches the maximum body parse length. You cannot configure different beginning and ending patterns for different server farms that are part of the same traffic classification. <p>Valid entries are unquoted text strings with no spaces and a maximum of 255 alphanumeric characters. The ACE supports regular expressions for matching string expressions. Table 11-35 lists the supported characters that you can use for matching string expressions.</p> <ol style="list-style-type: none"> In the Length field, enter the length in bytes of the portion of the payload (starting with the byte after the offset value) that the ACE uses for sticking the client to the server. Valid entries are integers from 1 to 1000 bytes. <p>The offset and length can vary from 0 to 1000 bytes. If the payload is longer than the offset but shorter than the offset plus the length of the payload, the ACE sticks the connection based on that portion of the payload starting with the byte after the offset value and ending with the byte specified by the offset plus the length. The total of the offset and the length cannot exceed 1000.</p> <p>Note You cannot specify both the length and end-pattern options for a Hash Layer 4 predictor.</p> <ol style="list-style-type: none"> In the HTTP Content Offset field, enter the portion of the content that the ACE uses to stick the client on a particular server by indicating the bytes to ignore starting with the first byte of the payload. Valid entries are integers from 0 to 999 bytes. The default is 0, which indicates that the ACE does not exclude any portion of the content.
Hash URL	<p>Indicates that the ACE is to select the server using a hash value based on the URL. Use this method to load balance firewalls.</p> <p>Enter values in one or both of the pattern fields:</p> <ul style="list-style-type: none"> In the URL Begin Pattern field, enter the beginning pattern of the URL and the pattern string to parse. In the URL End Pattern field, enter the ending pattern of the URL and the pattern string to parse. <p>Valid entries for these fields are unquoted text strings with no spaces and a maximum of 255 alphanumeric characters for each pattern you configure.</p>

Table 4-14 *Predictor Methods and Attributes (continued)*

Least Bandwidth	<p>The ACE selects the server with the least amount of network traffic over a specified sampling period.</p> <ol style="list-style-type: none"> 1. In the Assess Time field, enter the number of seconds for which the ACE is to collect traffic information. Valid entries are integers from 1 to 10 seconds. 2. In the Least Bandwidth Samples field, enter the number of samples over which you want to weight and average the results of the probe query to calculate the final load value. Valid entries are 1, 2, 4, 8, and 16 (integers from 1 to 16 that are also a power of 2).
Least Connections	<p>Indicates that the ACE is to select the server with the fewest number of connections.</p> <p>In the Slowstart Duration field, enter the slow-start value to be applied to this predictor method. Valid entries are integers from 1 to 65535, where 1 is the slowest ramp-up value.</p> <p>The slow-start mechanism is used to avoid sending a high rate of new connections to servers that you have just put into service.</p>
Least Loaded	<p>The ACE selects the server with the lowest load based on information from SNMP probes.</p> <ol style="list-style-type: none"> 1. In the SNMP Probe Name field, select the name of the SNMP probe to use. 2. In the Auto Adjust field, configure the autoadjust feature to assign a maximum load value of 16000 to that server to prevent it from being flooded with new incoming connections. The ACE periodically adjusts this load value based on feedback from the server's SNMP probe and other configured options. Options include: <ul style="list-style-type: none"> • N/A—Indicates that this option is not defined. • Average—Instructs the ACE to apply the average load of the server farm to a real server whose load reaches zero. The average load is the running average of the load values across all real servers in the server farm. • Off—Overrides the default behavior of the ACE of setting the load value for a server with a load of zero to 16000. When you configure this parameter, the ACE sends all new connections to the server that has a load of zero until the next load update arrives from the SNMP probe for this server. There may be times when you want the ACE to send all new connections to a real server whose load is zero. 3. In the Weight Connection field, check the check box to instruct the ACE to use the current connection count in the final load calculation for a real server. When you configure this option, the ACE includes the current connection count in the total load calculation for each real server in a server farm. Clear the check box to reset the behavior of the ACE to the default of excluding the current connection count from the load calculation.

Table 4-14 Predictor Methods and Attributes (continued)

Response	<p>The ACE selects the server with the lowest response time for a requested response-time measurement.</p> <ol style="list-style-type: none"> 1. In the Response Type field, select the type of measurement to use: <ul style="list-style-type: none"> • App-Req-To-Resp—The response time from when the ACE sends an HTTP request to a server to the time that the ACE receives a response from the server for that request. • Syn-To-Close—The response time from when the ACE sends a TCP SYN to a server to the time that the ACE receives a CLOSE from the server. • Syn-To-Synack—The response time from when the ACE sends a TCP SYN to a server to the time that the ACE receives a SYN-ACK from the server. 2. In the Response Samples field, enter the number of samples over which you want to average the results of the response-time measurement. Valid entries are 1, 2, 4, 8, and 16 (integers from 1 to 16 that are also a power of 2). 3. In the Weight Connection field, check the check box to instruct the ACE to use the current connection count in the final load calculation for a real server. When you configure this option, the ACE includes the current connection count in the total load calculation for each real server in a server farm. Clear the check box to reset the behavior of the ACE to the default of excluding the current connection count from the load calculation.
Round Robin	<p>Indicates that the ACE is to select the next server in the list of servers based on server weight. This is the default predictor method.</p>

Step 9 If you select Sticky as the primary action, in the Sticky Group field, select an existing sticky group or click ***New*** to add a new sticky group (see [Table 4-15](#)).



Note If you select an existing sticky group, you can view, modify, or duplicate the selected object's existing configuration. See [Shared Objects and Virtual Servers, page 4-6](#) for more information about modifying shared objects in virtual servers.

Table 4-15 Sticky Group Attributes

Field	Description
Group Name	Enter a unique identifier for the sticky group. You can either accept the automatically incremented entry given or you can enter your own. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters.
Type	<p>Select the method to be used when establishing sticky connections and configure any type-specific attributes:</p> <ul style="list-style-type: none"> • HTTP Content—The virtual server is to stick client connections to the same real server based on a string in the data portion of the HTTP packet. See Table 6-2 for additional configuration options. • HTTP Cookie—The virtual server is either to learn a cookie from the HTTP header of a client request or to insert a cookie in the Set-Cookie header of the response from the server to the client, and then use the learned cookie to provide stickiness between the client and server for the duration of the transaction. See Table 6-3 for additional configuration options. • HTTP Header—The virtual server is to stick client connections to the same real server based on HTTP headers. See Table 6-4 for additional configuration options. • IP Netmask—The virtual server is to stick a client to the same server for multiple subsequent connections as needed to complete a transaction using the client source IP address, the destination IP address, or both. See Table 6-5 for additional configuration options. <p>Note If an organization uses a megaproxy to load balance client requests across multiple proxy servers when a client connects to the Internet, the source IP address is no longer a reliable indicator of the true source of the request. In this situation, you can use cookies or another sticky method to ensure session persistence.</p> <ul style="list-style-type: none"> • Layer 4 Payload—The virtual server is to stick client connections to the same real server based on a string in the payload portion of the Layer 4 protocol packet. See Table 6-6 for additional configuration options. • RADIUS—The virtual server is to stick client connections to the same real server based on a RADIUS attribute. • RTSP Header—The virtual server is to stick client connections to the same real server based on the RTSP Session header field. Table 6-8 for additional configuration options. • SIP Header—The virtual server is to stick client connections to the same real server based on the SIP Call-ID header field.
Sticky Server Farm	Select an existing server farm to act as the primary server farm for this sticky group, or select *New* to create a new server farm. If you select *New* , configure the server farm using the information in Table 4-13 .
Backup Server Farm	Select an existing server farm to act as the backup server farm this sticky group, or select *New* to create a new server farm. If you select *New* , configure the server farm using the information in Table 4-13 .
Aggregate State	<p>Check the check box to indicate that the state of the primary server farm is to be tied to the state of all real servers in the server farm and in the backup server farm, if configured. The ACE declares the primary server farm down if all real servers in the primary server farm and all real servers in the backup server farm are down.</p> <p>Clear the check box if the state of the primary server farm is not to be tied to all real servers in the server farm and in the backup server farm.</p>

Table 4-15 Sticky Group Attributes (continued)

Field	Description
Sticky Enabled On Backup Server Farm	Check the check box to indicate that the backup server farm is sticky. Clear the check box if the backup server farm is not sticky.
Replicate On HA Peer	Check the check box to indicate that the virtual server is to replicate sticky table entries on the backup server farm. If a failover occurs and this option is selected, the new active server farm can maintain the existing sticky connections. Clear the check box to indicate that the virtual server is not to replicate sticky table entries on the backup server farm.
Timeout (Minutes)	Enter the number of minutes that the virtual server keeps the sticky information for a client connection in the sticky table after the latest client connection terminates. Valid entries are integers from 1 to 65535; the default is 1440 minutes (24 hours).
Timeout Active Connections	Check the check box to specify that the virtual server is to time out sticky table entries even if active connections exist after the sticky timer expires. Clear the check box to specify that the virtual is not to time out sticky table entries even if active connections exist after the sticky timer expires. This is the default behavior.

- Step 10** In the Compression Method field, select the HTTP compression method to indicate how the ACE appliance is to compress packets when a client request indicates that the client browser is capable of packet compression. By default, HTTP compression is disabled in the ACE. When you configure HTTP compression using the ACE, the appliance compresses data in the HTTP GET responses from the real servers. The ACE does not compress HTTP requests from clients or the HTTP headers in the server responses.



Note By default, the ACE supports HTTP compression at rates of 100 megabits per second (Mbps). Installing an optional HTTP compression license allows you to increase this value to a maximum of 2 Gbps. See the *Cisco 4700 Series Application Control Engine Appliance Administration Guide* for information on ACE licensing options.

Options include:

- Gzip—Specifies the gzip compression format as the method to use when the client browser supports both the deflate and gzip compression methods. Gzip is the file format for compression described in RFC1952.
- Deflate—Specifies the deflate compression format as the method to use when the client browser supports both the deflate and gzip compression methods. Deflate is the data format for compression described in RFC1951.
- N/A—HTTP compression is disabled.

When you enable HTTP compression, the ACE compresses the packets using the following default compression parameter values:

- Mime type—All text formats (text/*).
- Minimum size—512 bytes.
- User agent—None.

- Step 11** In the SSL Initiation field, select an existing service, or select ***New*** to create a new service:
- If you select an existing SSL service, you can view, modify, or duplicate the existing configuration. See [Shared Objects and Virtual Servers, page 4-6](#) for more information about modifying shared objects.
 - If you select ***New***, configure the service using the information in [Table 4-5](#). For more information about SSL, see [Configuring SSL, page 8-1](#).
- Step 12** In the Insert HTTP Headers field, enter the name of the HTTP header and the value to be matched using the format *header_name=header_value* where:
- *header_name* represents the name of the HTTP header to insert in the client HTTP request. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters. You can specify predefined header or any custom header name provided that it does not exceed the maximum length limit.
 - *header_value* represents the expression string to compare against the value in the specified field in the HTTP header. Valid entries are text strings with a maximum of 255 alphanumeric characters. The ACE supports regular expressions for matching. Header expressions allow spaces, provided that the spaces are escaped or quoted. All headers in the header map must be matched. [Table 11-35](#) lists the supported characters that you can use in regular expressions.
- For example, you might enter `Host=www.cisco.com`.
- Step 13** Click:
- **OK** to save your entries and to return to the Rule Match table.
 - **Cancel** to exit this procedure without saving your entries and to return to the Rule Match table.
- Step 14** When you finish configuring virtual server properties, click:
- **Deploy Now** to deploy this configuration on the ACE.
 - **Cancel** to exit this procedure without saving your entries.
 - **Deploy Later** to save your entries and apply them at a later time.
-

Related Topics

- [Configuring Virtual Servers, page 4-2](#)
- [Configuring Virtual Server Properties, page 4-8](#)
- [Configuring Virtual Server SSL Termination, page 4-13](#)
- [Configuring Virtual Server Protocol Inspection, page 4-14](#)



Configuring Virtual Server Default Layer 7 Load Balancing

Use this procedure configure default Layer 7 load-balancing actions for all network traffic that does not meet previously specified match conditions.

Assumption

A virtual server has been configured. See [Configuring Virtual Servers, page 4-2](#) for information on configuring a virtual server.

Procedure

-
- Step 1** Select **Config > Devices > context > Load Balancing > Virtual Servers**. The Virtual Servers table appears.
- Step 2** Select the virtual server you want to configure for default Layer 7 load balancing, then click **Edit**. The Virtual Server configuration screen appears.
- Step 3** Click **Default L7 Load-Balancing Action**. The Default L7 Load-Balancing Action configuration pane appears.
- Step 4** In the Primary Action field, indicate the default action the virtual server is to take in response to client requests for content when specified match conditions are not met:
- Drop—Client requests that do not meet specified match conditions are to be discarded. Continue with [Step 8](#).
 - Forward—Client requests that do not meet specified match conditions are to be forwarded without performing load balancing on the requests. Continue with [Step 8](#).
 - Loadbalance—Client requests for content are to be directed to a server farm. Continue with [Step 5](#).
 - Sticky—Client requests for content are to be handled by a sticky group when match conditions are met. Continue with [Step 6](#).
- Step 5** If you select Loadbalance as the primary action:
- a. In the Server Farm field, select the primary server farm to use for load balancing, or select ***New*** to configure a new server farm (see [Table 4-13](#)).
 - b. In the Backup Server Farm field, select the server farm to act as the backup server farm for load balancing if the primary server farm is unavailable, or select ***New*** to configure a new backup server farm (see [Table 4-13](#)).
-  **Note** If you select an existing object in either field, you can view, modify, or duplicate the selected object's existing configuration. See [Shared Objects and Virtual Servers, page 4-6](#) for more information about modifying shared objects in virtual servers.
-
- Step 6** If you select Sticky as the primary action, in the Sticky Group field, select an existing sticky group or click ***New*** to add a new sticky group (see [Table 4-15](#)).
-  **Note** If you select an existing sticky group, you can view, modify, or duplicate the selected object's existing configuration. See [Shared Objects and Virtual Servers, page 4-6](#) for more information about modifying shared objects in virtual servers.
-
- Step 7** In the Compression Method field, select the HTTP compression method to indicate how the ACE appliance is to compress packets when a client request indicates that the client browser is capable of packet compression. By default, HTTP compression is disabled in the ACE. When you configure HTTP compression using the ACE, the appliance compresses data in the HTTP GET responses from the real servers. The ACE does not compress HTTP requests from clients or the HTTP headers in the server responses.



Note By default, the ACE supports HTTP compression at rates of 100 megabits per second (Mbps). Installing an optional HTTP compression license allows you to increase this value to a maximum of 2 Gbps. See the *Cisco 4700 Series Application Control Engine Appliance Administration Guide* for information on ACE licensing options.

Options include:

- Deflate—Specifies the deflate compression format as the method to use when the client browser supports both the deflate and gzip compression methods. deflate, the data format for compression described in RFC1951.
- Gzip—Specifies the gzip compression format as the method to use when the client browser supports both the deflate and gzip compression methods. Gzip is the file format for compression described in RFC1952.
- N/A—HTTP compression is disabled.

When you enable HTTP compression, the ACE compresses the packets using the following default compression parameter values:

- Mime type—All text formats (text/*).
- Minimum size—512 bytes.
- User agent—None.

- Step 8** In the SSL Initiation field, select an existing service, or select ***New*** to create a new service:
- If you select an existing SSL service, you can view, modify, or duplicate the existing configuration. See [Shared Objects and Virtual Servers, page 4-6](#) for more information about modifying shared objects.
 - If you select ***New***, configure the service using the information in [Table 4-5](#). For more information about SSL, see [Configuring SSL, page 8-1](#).
- Step 9** In the Insert HTTP Headers field, enter the name of the HTTP header and the value to be matched using the format *header_name=header_value* where:
- *header_name* represents the name of the HTTP header to insert in the client HTTP request. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters. You can specify predefined header or any custom header name provided that it does not exceed the maximum length limit.
 - *header_value* represents the expression string to compare against the value in the specified field in the HTTP header. Valid entries are text strings with a maximum of 255 alphanumeric characters. The ACE supports regular expressions for matching. Header expressions allow spaces, provided that the spaces are escaped or quoted. All headers in the header map must be matched. [Table 11-35](#) lists the supported characters that you can use in regular expressions.
- For example, you might enter `Host=www.cisco.com`.
- Step 10** When you finish configuring virtual server properties, click:
- **Deploy Now** to deploy this configuration on the ACE.
 - **Cancel** to exit this procedure without saving your entries and to return to the Virtual Servers table.
 - **Deploy Later** to save your entries and apply the configuration at a later time.

Related Topics

- [Configuring Virtual Server Properties](#), page 4-8
- [Configuring Virtual Server SSL Termination](#), page 4-13
- [Configuring Virtual Server Protocol Inspection](#), page 4-14
- [Configuring Virtual Server Layer 7 Load Balancing](#), page 4-26

Configuring Application Acceleration and Optimization

The ACE appliance includes configuration options that allow you to accelerate enterprise applications, resulting in increased employee productivity, enhanced customer retention, and increased online revenues. The application acceleration functions of the ACE appliance apply several optimization technologies to accelerate Web application performance. This application acceleration functionality enables enterprises to optimize network performance and improve access to critical business information. It also accelerates the performance of Web applications, including customer relationship management (CRM), portals, and online collaboration by up to 10 times.

Refer to [Configuring Application Acceleration and Optimization](#), page 12-1 or the *Cisco 4700 Series Application Control Engine Appliance Application Acceleration and Optimization Configuration Guide* for more information about application acceleration and optimization.

Use this procedure to configure acceleration and optimization on virtual servers that are configured on ACE appliances.

This option is available only for ACE appliances and only in the Advanced View.

Assumption

A virtual server has been configured on an ACE appliance with HTTP or HTTPS as the application protocol. See [Configuring Virtual Servers](#), page 4-2 for information on configuring a virtual server.

Procedure

-
- Step 1** Select **Config > Devices > context > Load Balancing > Virtual Servers**. The Virtual Servers table appears.
- Step 2** Select the virtual server you want to configure for optimization, then click **Edit**. The Virtual Server configuration screen appears.
- Step 3** Click **Application Acceleration And Optimization**. The Application Acceleration And Optimization configuration pane appears.
- Step 4** In the Configuration field, indicate the method you want to use to configure application acceleration and optimization:
- EZ—Use standard acceleration and optimization options. Continue with [Step 5](#).
 - Custom—Associate specific match criteria, actions, and parameter maps for application acceleration and optimization for the virtual server. If you choose this option, continue with [Step 6](#) through [Step 14](#).
- Step 5** If you select EZ, the Latency Optimization (FlashForward) and Bandwidth Optimization (Delta) fields appear.
- a. Check the Latency Optimization (FlashForward) check box to indicate that the ACE appliance is to use bandwidth reduction and download acceleration techniques to objects embedded within HTML pages. Clear the check box to indicate that the ACE appliance is not to employ these techniques to

objects embedded within HTML pages. Latency optimization corresponds to FlashForward functionality. For more information about FlashForward functionality, see [Optimization Overview, page 12-2](#).

- b. Check the Bandwidth Optimization (Delta) check box to indicate that the ACE appliance is to dynamically update client browser caches with content differences, or deltas. Clear the check box to indicate that the ACE appliance is not to dynamically update client browser caches. Bandwidth optimization corresponds to action list Delta optimization. For more information about configuring Delta optimization, see [Optimization Overview, page 12-2](#) and [Configuring an HTTP Optimization Action List, page 12-3](#).
- c. Continue with [Step 14](#).

Step 6 If you select Custom, the Actions configuration pane appears with a table listing match criteria and actions. Click **Add** to add an entry to this table, or select an existing entry, then click **Edit** to modify it. The configuration pane refreshes with the available configuration options.

Step 7 In the Apply Building Block field, select one of the configuration building blocks for the type of optimization you want to configure, or leave blank to configure optimization without a building block:

- Bandwidth Optimization—Maximizes bandwidth for Web-based traffic.
- Latency Optimization for Embedded Objects—Reduces the latency associated with embedded objects in Web-based traffic.
- Latency Optimization for Embedded Images—Reduces the latency associated with embedded images in Web-based traffic.
- Latency Optimization for Containers—Reduces the latency associated with Web containers.

If you select one of the building blocks, the Rule Match configuration subset displays the configuration options with selections based on the building block chosen. You can accept the entries as they are or modify them.

If you do not select a building block, additional configuration options appear depending on the features you enable.

- Step 8** In the Rule Match field, select an existing class map or click ***New*** to specify new match criteria:
- If you select an existing class map, you can view, modify, or duplicate the existing configuration. See [Shared Objects and Virtual Servers, page 4-6](#) for more information about modifying shared objects.
 - If you click ***New***, the screen refreshes so that you can enter new match criteria.

Step 9 Configure match criteria using the information in [Table 4-16](#).

Table 4-16 Optimization Match Criteria Configuration

Field	Description
Name	Enter a unique name for this match criteria rule.

Table 4-16 Optimization Match Criteria Configuration (continued)

Field	Description
Match	Select the method to be used to evaluate multiple match statements when multiple match conditions exist: <ul style="list-style-type: none"> match-any—A match exists if at least one of the match conditions is satisfied. match-all—A match exists only if all match conditions are satisfied.
Conditions	Click Add to add a new set of conditions or select an existing entry, then click Edit to modify it: <ol style="list-style-type: none"> In the Type field, select the match condition to be used, then configure any condition-specific options using the information in Table 4-12. Click OK to save your entries, or Cancel to exit this procedure without saving your entries.

Step 10 In the Actions field, select an existing action list to use for optimization or click ***New*** to create a new action list:

- If you select an existing action list, you can view, modify, or duplicate the existing configuration. See [Shared Objects and Virtual Servers, page 4-6](#) for more information about modifying shared objects.
- If you click ***New***, the screen refreshes so you can configure an action list.

Step 11 Configure the action list using the information in [Table 4-17](#).

Table 4-17 Optimization Action List Configuration Options

Field	Description
Action List Name	Enter a unique name for the action list. Valid entries are unquoted text strings with a maximum of 64 alphanumeric characters.
Enable Delta	Delta optimization dynamically updates client browser caches directly with content differences, or deltas, resulting in faster page downloads. Check this check box to enable delta optimization for the specified URLs. Clear this check box to disable this feature. If you are configuring optimization without a building block, additional options appear. Configure these options using the information in Table 4-18 .
Enable AppScope	AppScope runs on the Management Console of the optional Cisco AVS 3180A Management Station and measures end-to-end application performance. Check this check box to enable AppScope performance monitoring for use with the ACE appliance. Clear this check box to disable this feature. If you are configuring optimization without a building block, additional options appear. Configure these options using the information in Table 4-18 .

Table 4-17 Optimization Action List Configuration Options (continued)

Field	Description
Flash Forward	<p>The FlashForward feature reduces bandwidth usage and accelerates embedded object downloading by combining local object storage with dynamic renaming of embedded objects, thereby enforcing object freshness within the parent HTML page.</p> <p>Specify how the ACE appliance is to implement FlashForward:</p> <ul style="list-style-type: none"> • N/A—This feature is not enabled. • Flash Forward—FlashForward is to be enabled for the specified URLs and embedded objects are to be transformed. • Flash Forward Object—FlashForward static caching is to be enabled for the objects that the corresponding URLs refer to, such as Cascading Style Sheets (CSS), JPEG, and GIF files. <p>If you are configuring without a building block and select either FlashForward or FlashForward Object, an addition option appears. Configure this option using the information in Table 4-18.</p>
Cache Dynamic	<p>Check this check box to enable Adaptive Dynamic Caching for the specified URLs even if the expiration settings in the response indicate that the content is dynamic. The expiration of cache objects is controlled by the cache expiration settings based on time or server load.</p> <p>Clear this check box to disable this feature.</p>
Cache Forward	<p>Specify how the ACE appliance is to implement cache forwarding:</p> <ul style="list-style-type: none"> • N/A—This feature is not enabled. • With Wait—Cache forwarding is enabled with the wait option for the specified URLs. If the object has expired but the maximum cache TTL time period has not yet expired, the ACE appliance sends a request to the origin server for the object. Users requesting this page continue to receive content from the cache during this time but must wait for the object to be updated before their request is satisfied. When the fresh object is returned, it is sent to the requesting user and the cache is updated. • Without Wait—Cache forwarding is enabled without the wait option.
Dynamic Dynamic Entity Tag	<p>This feature enables the acceleration of embedded objects not able to be cached, which results in improved application response time. When enabled, this feature eliminates the need for users to download objects not able to be cached on each request.</p> <p>Check this check box to indicate that the ACE appliance is to implement just-in-time object acceleration for embedded objects not able to be cached.</p> <p>Clear this check box to disable this feature.</p>

Step 12 If you are configuring optimization without a building block, additional options appear when you enable specific features. Configure the additional options using the information in [Table 4-18](#).

Table 4-18 Application Acceleration and Optimization Additional Configuration Options

Field	Description
Response Codes To Ignore (Comma Separated)	Enter a comma-separated list of HTTP response codes for which the response body must not be read. For example, an entry of 302 indicates that the ACE is to ignore the response body of a 302 (redirect) response from the origin server. Valid entries are unquoted text strings with a maximum of 64 alphanumeric characters.
Set Browse Freshness Period	Select the method that the ACE is to use to determine the freshness of objects in the client's browser: <ul style="list-style-type: none"> • N/A—This option is not configured. • Disable Browser Object Freshness Control—Browser freshness control is not to be used. • Set Freshness Similar To Flash Forward Objects—The ACE is to set freshness similar to that used for FlashForwarded objects and to use the values specified in the <i>Maximum Time for Cache Time-To-Live</i> and <i>Minimum Time For Cache Time-To-Live</i> fields.
Duration For Browser Freshness (Seconds)	This field appears if the Set Browse Freshness Period option is not configured. Enter the number of seconds that objects in the client's browser are considered fresh. Valid entries are 0 to 2147483647 seconds.
Enable Delta Options	
Max. For Post Data To Scan For Logging (kBytes)	Enter the maximum number of kilobytes of POST data the ACE is to scan for parameters for the purpose of logging transaction parameters in the statistics log. Valid entries are 0 to 1000 KB.
Base File Anonymous Level	Information that is common to a large set of users is generally not confidential or user-specific. Conversely, information that is unique to a specific user or a small set of users is generally confidential or user-specific. The anonymous base file feature enables the ACE to create and deliver condensed base files that contain only information that is common to a large set of users. No information unique to a particular user, or across a very small subset of users, is included in anonymous base files. Enter the value for base file anonymity for the all-user condensation method. Valid entries are integers from 0 to 50; the default value of 0 disables the base file anonymity feature.
Cache-Key Modifier Expression	A cache object key is a unique identifier that is used to identify a cached object to be served to a client, replacing a trip to the origin server. The cache key modifier feature allows you to modify the canonical form of a URL; that is, the portion before “?” in a URL. For example, the canonical URL of “http://www.xyz.com/somepage.asp?action=browse&level=2” is “http://www.xyz.com/somepage.asp”. Enter a regular expression containing embedded variables as described in Table 4-19 . The ACE transforms URLs specified in class maps for this virtual server with the expression and variable entered here. Valid entries are unquoted text strings with no spaces and a maximum of 255 alphanumeric characters. If the string includes spaces, enclose the string with quotation marks (“”).

Table 4-18 Application Acceleration and Optimization Additional Configuration Options (continued)

Field	Description
Min. Time For Cache Time-To-Live (Seconds)	Enter the minimum number of seconds that an object without an explicit expiration time should be considered fresh in the ACE cache. This value specifies the minimum time that content can be cached. If the ACE is configured for FlashForward optimization, this value should normally be 0. If the ACE is configured for dynamic caching, this value should indicate how long the ACE should cache the page. (See Table 4-17 for information about these configuration options.) Valid entries are 0 to 2147483647 seconds.
Max. Time For Cache Time-To-Live (Seconds)	Enter the maximum number of seconds that an object without an explicit expiration time should be considered fresh in the ACE cache. Valid entries are 0 to 2147483647 seconds.
Cache Time-To-Live Duration (%)	Enter the percent of an object's age at which an embedded object without an explicit expiration time is considered fresh. Valid entries are 0 to 100 percent.
Expression To Modify Cache Key Query Parameter	The cache parameter feature allows you to modify the query parameter of a URL; that is, the portion after "?" in a URL. For example, the query parameter portion of "http://www.xyz.com/somepage.asp?action=browse&level=2" is "action=browse&level=2". Enter a regular expression containing embedded variables as described in Table 4-19 . The ACE transforms URLs specified in class maps for this virtual server with the expression and variable entered here. If no string is specified, the query parameter portion of the URL is used as the default value for this portion of the cache key. Valid entries are unquoted text strings with no spaces and a maximum of 255 alphanumeric characters.
Canonical URL Expressions	The ACE uses the canonical URL feature to eliminate the "?" and any characters that follow to identify the general part of the URL. This general URL is then used to create the base file. In this way, the ACE maps multiple URLs to a single canonical URL. Enter a comma-separated list of parameter expander functions as defined in Table 4-19 to identify the URLs to associate with this parameter map. Valid entries are unquoted text strings with a maximum of 255 alphanumeric characters.
Enable Cacheable Content Optimization	This feature allows the ACE to detect content that can be cached and perform delta optimization on it. Check the check box to enable delta optimization of content that can be cached. Clear the check box to disable this feature.
Enable Delta Optimization On First Visit To Web Page	Check the check box to enable condensation on the first visit to a Web page. Clear the check box to disable this feature.
Min. Page Size For Delta Optimization (Bytes)	Enter the minimum page size, in bytes, that can be condensed. Valid entries are integers from 1 to 250000 bytes.
Max. Page Size For Delta Optimization (Bytes)	Enter the maximum page size, in bytes, that can be condensed. Valid entries are integers from 1 to 250000 bytes.

Table 4-18 Application Acceleration and Optimization Additional Configuration Options (continued)

Field	Description
Set Default Client Script	Indicate the scripting language that the ACE is to recognize on condensed content pages: <ul style="list-style-type: none"> • N/A—Indicates that this option is not configured. • Javascript—Indicates that the default scripting language is JavaScript. • Visual Basic Script—Indicates that the default scripting language is Visual Basic.
Exclude Iframes From Delta Optimization	Check the check box to indicate that delta optimization is not to be applied to IFrames (inline frames). Clear the check box to indicate that delta optimization is to be applied to IFrames.
Exclude Non-ASCII Data From Delta Optimization	Check the check box to indicate that delta optimization is not to be applied to non-ASCII data. Clear the check box to indicate that delta optimization is to be applied to non-ASCII data.
Exclude JavaScripts From Delta Optimization	Check the check box to indicate that delta optimization is not to be applied to JavaScript. Clear the check box to indicate that delta optimization is to be applied to JavaScript.
MIME Types To Exclude From Delta Optimization	<ol style="list-style-type: none"> 1. In the first field, enter a comma-separated list of the MIME (Multipurpose Internet Mail Extension) type messages that are not to have delta optimization applied, such as image/Jpeg, text/html, application/msword, or audio/mpeg. See Supported MIME Types, page 7-23 for a list of supported MIME types. 2. Click Add to add the entry to the list box on the right. You can position the entries in the list box by using the Up and Down buttons.
Remove HTML META Elements From Documents	Check the check box to indicate that HTML META elements are to be removed from documents to prevent them from being condensed. Clear the check box to indicate that HTML META elements are not to be removed from documents.
Rebase Delta Optimization Threshold (%)	Enter the delta threshold, expressed as a percent, when rebasing is to be triggered. This entry represents the size of a page delta relative to total page size, expressed as a percent. This entry triggers rebasing when the delta response size exceeds the threshold as a percentage of base file size. Valid entries are 0 to 10000 percent.
Rebase Flash Forward Threshold (%)	Enter the threshold, expressed as a percent, when rebasing is to be triggered based on the percent of FlashForwarded URLs in the response. This entry triggers rebasing when the difference between the percentages of FlashForwarded URLs in the delta response and the base file exceeds the threshold. Valid entries are 0 to 10000 percent.
Rebase History Size (Pages)	Enter the number of pages to be stored before the ACE resets all rebase control parameters to zero and starts over. This option prevents the base file from becoming too rigid. Valid entries are 10 to 2147483647.
Rebase Modify Cool-Off Period (Seconds)	Enter the number of seconds after the last modification before performing a rebase. Valid entries are 1 to 14400 seconds (4 hours).
Rebase Reset Period (Seconds)	Enter the period of time, in seconds, for performing a meta data refresh. Valid entries are 1 to 900 seconds (15 minutes).

Table 4-18 Application Acceleration and Optimization Additional Configuration Options (continued)

Field	Description
UTF-8 Character Set Threshold	<p>The UTF-8 (8-bit Unicode Transformation Format) character set is an international standard that allows Web pages to display non-ASCII or non-English multibyte characters. It can represent any universal character in the Unicode standard and is backwards compatible with ASCII.</p> <p>Enter the number of UTF-8 characters that need to appear on a page to constitute a UTF-8 character set page. Valid entries are integers from 1 to 1,000,000.</p>
Server Load Threshold Trigger (%)	<p>The server load threshold trigger indicates that the time-to-live (TTL) period for cached objects is to be based dynamically on server load. With this method, TTL periods increase if the current response time from the origin sever is greater than the average response time and decrease if the current response time from the origin server is less than the average response time when the difference in response times exceeds a specified threshold amount.</p> <p>Enter the threshold, expressed as a percent, at which the TTL for cached objects is to be changed. Valid entries are from 0 to 100 percent.</p>
Server Load Time-To-Live Change (%)	<p>This option specifies the percentage by which the cache TTL is increased or decreased in response to a change in server load. For example, if this value is set to 20 and the current TTL for a response is 300 seconds, and if the current server response times exceeds the trigger threshold, the cache TTL for the response is raised to 360 seconds.</p> <p>Enter the percent by which the cache TTL is to be increased or decreased when the server load threshold trigger is met. Valid entries are from 0 to 100 percent.</p>
Delta Optimization Mode	<p>Select the method by which delta optimization is to be implemented:</p> <ul style="list-style-type: none"> • N/A—Indicates that a delta optimization mode is not configured. • Enable The All-User Mode For Delta Optimization—Indicates that the ACE is to generate the delta against a single base file that is shared by all users of the URL. This option is usable in most cases if the structure of a page is common across all users, and the disk space overhead is minimal. • Enable The Per-User Mode For Delta Optimization—Indicates that the ACE is to generate the delta against a base file that is created specifically for that user. This option is useful when page contents, including layout elements, are different for each user, and delivers the highest level of condensation. However, this increases disk space requirements because a copy of the base page that is delivered to each user is cached. This option is useful when privacy is required because base pages are not shared among users.
Enable Appscope Options	
Appscope Optimize Rate (%)	<p>Enter the percentage of all requests or sessions to be sampled for performance with acceleration (or optimization) applied. All applicable optimizations for the class will be performed. Valid entries are from 0 to 100 percent, with a default of 10 percent. The sum of this value and the value entered in the Passthru Rate Percent field must not exceed 100.</p>
Appscope Passthrough Rate (%)	<p>Enter the percentage of all requests or sessions to be sampled for performance without optimization. No optimizations for the class will be performed. Valid entries are from 0 to 100, with a default of 10 percent. The sum of this value and the value entered in the Optimize Rate Percent field must not exceed 100.</p>

Table 4-18 Application Acceleration and Optimization Additional Configuration Options (continued)

Field	Description
Max Number For Parameter Summary Log (Bytes)	Enter the maximum number of bytes that are to be logged for each parameter value in the parameter summary of a transaction log entry in the statistics log. If a parameter value exceeds this limit, it is truncated at the specified limit. Valid entries are 0 to 10,000 bytes.
Specify String For Grouping Requests	<p>Enter the string the ACE is to use to sort requests for AppScope reporting. The string can contain a URL regular expression that defines a set of URLs in which URLs that differ only by their query parameters are to be treated as separate URLs in AppScope reports.</p> <p>For example, to define a string that is used to identify the URLs <code>http://server/catalog.asp?region=asia</code> and <code>http://server/catalog.asp?region=america</code> as two separate reporting categories, you would enter <code>http_query_param(region)</code>.</p> <p>Valid entries contain 1 to 255 characters and can contain the parameter expander functions listed in Table 4-19.</p>

[Table 4-19](#) lists the parameter expander functions that you can use.

Table 4-19 Parameter Expander Functions

Variable	Description
<code>\$(number)</code>	<p>Expands to the corresponding matching subexpression (by <i>number</i>) in the URL pattern. Subexpressions are marked in a URL pattern using parentheses (). The numbering of the subexpressions begins with 1 and is the number of the left-parenthesis “(“ counting from the left. You can specify any positive integer for the number. <code>\$(0)</code> matches the entire URL. For example, if the URL pattern is <code>((http://server/.*)/(.*)/a.jsp)</code>, and the URL that matches it is <code>http://server/main/sub/a.jsp?category=shoes&session=99999</code>, then the following are correct:</p> <p><code>\$(0)</code> = <code>http://server/main/sub/a.jsp</code> <code>\$(1)</code> = <code>http://server/main/sub/</code> <code>\$(2)</code> = <code>http://server/main</code> <code>\$(3)</code> = <code>sub</code></p> <p>If the specified subexpression does not exist in the URL pattern, then the variable expands to the empty string.</p>
<code>\$http_query_string()</code>	<p>Expands to the value of the whole query string in the URL. For example, if the URL is <code>http://myhost/dothis?param1=value1&param2=value2</code>, then the following is correct:</p> <p><code>\$http_query_string()</code> = <code>param1=value1&param2=value2</code></p> <p>This function applies to both GET and POST requests.</p>

Table 4-19 Parameter Expander Functions (continued)

Variable	Description
<p><code>\$http_query_param(query-param-name)</code></p> <p>The obsolete syntax is also supported: <code>\$param(query-param-name)</code></p>	<p>Expands to the value of the named query parameter (case-sensitive). For example, if the URL is <code>http://server/main/sub/a.jsp?category=shoes&session=99999</code>, then the following are correct:</p> <pre>\$http_query_param(category) = shoes \$http_query_param(session) = 99999</pre> <p>If the specified parameter does not exist in the query, then the variable expands to the empty string. This function applies to both GET and POST requests.</p>
<code>\$http_cookie(cookie-name)</code>	Evaluates to the value of the named cookie. For example, <code>\$http_cookie(cookiexyz)</code> . The cookie name is case-sensitive.
<code>\$http_header(request-header-name)</code>	Evaluates to the value of the specified HTTP request header. In the case of multivalued headers, it is the single representation as specified in the HTTP specification. For example, <code>\$http_header(user-agent)</code> . The HTTP header name is not case-sensitive.
<code>\$http_method()</code>	Evaluates to the HTTP method used for the request, such as GET or POST.
<p>Boolean Functions:</p> <p><code>\$http_query_param_present(query-param-name)</code> <code>\$http_query_param_notpresent(query-param-name)</code> <code>\$http_cookie_present(cookie-name)</code> <code>\$http_cookie_notpresent(cookie-name)</code> <code>\$http_header_present(request-header-name)</code> <code>\$http_header_notpresent(request-header-name)</code> <code>\$http_method_present(method-name)</code> <code>\$http_method_notpresent(method-name)</code></p>	<p>Evaluates to a Boolean value: True or False, depending on the presence or absence of the element in the request. The elements are a specific query parameter (<i>query-param-name</i>), a specific cookie (<i>cookie-name</i>), a specific request header (<i>request-header-name</i>), or a specific HTTP method (<i>method-name</i>). All identifiers are case-sensitive except for the HTTP request header name.</p>
<code>\$regex_match(param1, param2)</code>	<p>Evaluates to a Boolean value: True if the two parameters match and False if they do not match. The two parameters can be any two expressions, including regular expressions, that evaluate to two strings. For example, this function:</p> <pre>\$regex_match(\$http_query_param(URL), .*Store\.asp.*)</pre> <p>compares the query URL with the regular expression string <code>.*Store\.asp.*</code>.</p> <p>If the URL matches this regular expression, this function evaluates to True.</p>

- Step 13** When you finish configuring match criteria and actions, click:
- **OK** to save your entries and to return to the Rule Match and Actions table.
 - **Cancel** to exit this procedure without saving your entries and to return to the Rule Match and Actions table.
- Step 14** When you finish configuring virtual server properties, click:
- **Deploy Now** to save your entries. The ACE appliance validates the action list configuration and deploys it.
 - **Cancel** to exit this procedure without saving your entries and to return to the Virtual Servers table.
 - **Deploy Later** to save your entries and apply the configuration at a later time.
-

Related Topics

- [Optimization Traffic Policies and Typical Configuration Flow, page 12-2](#)
- [Configuring Traffic Policies for HTTP Optimization, page 12-7](#)
- [Configuring Virtual Server Protocol Inspection, page 4-14](#)
- [Configuring Virtual Server Layer 7 Load Balancing, page 4-26](#)
- [Configuring Virtual Server Default Layer 7 Load Balancing, page 4-41](#)

Configuring Virtual Server NAT

Use this procedure to configure Name Address Translation (NAT) for virtual servers. The NAT configuration subset appears in the Advanced View only.

Assumptions

- A virtual server has been configured. See [Configuring Virtual Servers, page 4-2](#) for information on configuring a virtual server.
- A VLAN has been configured. See [Configuring VLAN Interfaces, page 9-2](#) for information on configuring a VLAN interface.
- At least one NAT pool has been configured on a VLAN interface. See [Configuring VLAN Interface NAT Pools, page 9-10](#) for information on configuring a NAT pool.

Procedure

-
- Step 1** Select **Config > Devices > context > Load Balancing > Virtual Servers**. The Virtual Servers table appears.
- Step 2** Select the virtual server you want to configure for NAT, then click **Edit**. The Virtual Server configuration screen appears.
- Step 3** Click **NAT**. The NAT table appears.
- Step 4** Click **Add** to add an entry, or select an existing entry, then click **Edit** to modify it.
- Step 5** In the VLAN field, select the VLAN you want to use NAT. For more information about NAT, see [Configuring VLAN Interface NAT Pools, page 9-10](#).
- Step 6** In the NAT Pool ID field, select the NAT pool that you want to associate with the selected VLAN.

- Step 7** Click:
- **OK** to save your entries and to return to the NAT table. The NAT table refreshes with the new entry.
 - **Cancel** to exit the procedure without saving your entries and to return to the NAT table.
- Step 8** When you finish configuring virtual server properties, click:
- **Deploy Now** to deploy this configuration on the ACE.
 - **Cancel** to exit this procedure without saving your entries and to return to the Virtual Servers table.
 - **Deploy Later** to save your entries and apply the configuration at a later time.
-

Related Topics

- [Configuring Virtual Servers, page 4-2](#)
- [Configuring Virtual Server Properties, page 4-8](#)
- [Configuring Virtual Server SSL Termination, page 4-13](#)
- [Configuring Virtual Server Protocol Inspection, page 4-14](#)
- [Configuring Virtual Server Layer 7 Load Balancing, page 4-26](#)
- [Configuring Virtual Server Default Layer 7 Load Balancing, page 4-41](#)

Managing Virtual Servers

The Virtual Servers table (**Config > Operations > Virtual Servers**) provides the following information by default for each virtual server:

- Server name, sorted by virtual context
- Admin state
- Operational state



Note This column is populated for ACE 4710 appliances running image A3(1.0) and later. Clicking on the value in this column (irrespective of ACE version) will display detailed information about the Virtual Server in a popup.

- Number of active connections



Note This column is populated for ACE 4710 appliances running image A3(1.0) and later. For ACE devices, the Active Connections column will display N/A for older versions of the ACE appliance and module.

- VIP address
- Configured port
- VLANs
- Associated server farms
- Device

- High availability

You can activate or suspend virtual servers from this table and obtain additional information about the state of the virtual server.

The following options are available from the Virtual Servers table:

- [Deploying Virtual Servers, page 4-56](#)
- [Viewing All Staged Virtual Servers, page 4-57](#)
- [Modifying Deployed Virtual Servers, page 4-57](#)
- [Modifying Staged Virtual Servers, page 4-58](#)
- [Viewing Virtual Servers by Context, page 4-58](#)
- [Activating Virtual Servers, page 4-59](#)
- [Suspending Virtual Servers, page 4-59](#)
- [Managing GSS VIP Answers, page 4-60](#)
- [Activating and Suspending DNS Rules Governing GSS Load Balancing, page 4-62](#)
- [Viewing Detailed Virtual Server Information, page 4-63](#)
- [Viewing Virtual Servers, page 4-63](#)
- [Understanding CLI Commands Sent from Virtual Server Table, page 4-64](#)

Deploying Virtual Servers

You can deploy virtual servers on your network at times that are convenient and appropriate for your environment. For example, if your site prefers to make changes to the network during a specific time each night, you can modify and save virtual server configurations during the day and then deploy them when appropriate.

Use this procedure to deploy staged virtual servers on your network.

Procedure

-
- | | |
|---------------|---|
| Step 1 | Select Config > Deploy . The Staged Objects table appears. |
| Step 2 | Select the virtual server you want to deploy on your network, then click Deploy . The virtual server is deployed and the table refreshes with updated information. |
-

Related Topics

- [Configuring Virtual Servers, page 4-2](#)
- [Viewing All Staged Virtual Servers, page 4-57](#)
- [Modifying Staged Virtual Servers, page 4-58](#)

Viewing All Staged Virtual Servers

The ANM allows you to deploy configured virtual servers when it is appropriate for your environment. To view all objects that have been configured but have not yet been deployed on your network, select **Config > Deploy**. The Staged Objects table appears listing the:

- Virtual server name
- Device ID and virtual context
- Time the virtual server was created
- User who last modified the object
- Time the object was last updated

Deployment status is also available in the Virtual Servers table (**Config > Devices > context > Load Balancing > Virtual Servers**). Virtual servers with configurations that have not been deployed appear with the status Not Deployed in the Configured State column.

Related Topics

- [Configuring Virtual Servers, page 4-2](#)
- [Deploying Virtual Servers, page 4-56](#)
- [Modifying Staged Virtual Servers, page 4-58](#)
- [Modifying Deployed Virtual Servers, page 4-57](#)

Modifying Deployed Virtual Servers

Use this procedure to modify the configuration of a deployed virtual server.

Procedure

-
- Step 1** Select **Config > Devices > context > Load Balancing > Virtual Servers**. The Virtual Servers table appears.
 - Step 2** Select the virtual server you want to modify, then click **Edit**. The Virtual Server configuration screen appears.
 - Step 3** Modify the virtual server's configuration as desired. See [Table 4-1](#) for virtual server configuration options.
 - Step 4** When you are done modifying the configuration, click:
 - **Deploy Now** to immediately deploy this configuration.
 - **Cancel** to exit this procedure without saving your entries and to return to the Virtual Servers table.
-

Related Topics

- [Managing Virtual Servers, page 4-55](#)
- [Viewing All Staged Virtual Servers, page 4-57](#)
- [Activating Virtual Servers, page 4-59](#)
- [Suspending Virtual Servers, page 4-59](#)

Modifying Staged Virtual Servers

Use this procedure to modify the configuration of a staged virtual server.

Procedure

- Step 1** Select **Config > Deploy**. The Staged Objects table appears, listing those virtual servers that have not yet been deployed in the network.
- Step 2** Select the virtual server you want to modify, then click **Edit**. The virtual server configuration screen appears.
- Step 3** Modify the virtual server's configuration as desired. See [Table 4-1](#) for virtual server configuration options.
- Step 4** When you are done modifying the configuration, click:
- **Deploy Now** to immediately deploy this configuration.
 - **Cancel** to exit this procedure without saving your entries and to return to the Virtual Servers table.
 - **Deploy Later** to save your entries and apply this configuration at a later time.
-

Related Topics

- [Deploying Virtual Servers, page 4-56](#)
- [Viewing All Staged Virtual Servers, page 4-57](#)
- [Viewing Virtual Servers by Context, page 4-58](#)

Viewing Virtual Servers by Context

Use this procedure to view all virtual servers associated with a virtual context.

Procedure

- Step 1** Select **Config > Devices**. The device tree appears.
- Step 2** Select the context associated with the virtual servers you want to view, then select **Load Balancing > Virtual Servers**. The Virtual Servers table appears with the following information:
- Virtual server name
 - Configured state, such as Inservice or Out of service
 - Virtual IP address
 - Port
 - Associated VLANs
 - Associated server farms
 - The owner, and context in which the virtual server was created
-

Related Topics

- [Configuring Virtual Servers, page 4-2](#)
- [Managing Virtual Servers, page 4-55](#)

Activating Virtual Servers

Use this procedure to activate a virtual server.

**Note**

A missing operation or Admin state on a CSM or CSS device most likely means that the community string was not enabled on those devices. If the community string is not enabled on a CSM or CSS device, and any kind of operation is performed on those devices, it will not succeed, and ANM will not provide any kind of indication.

- For CSM devices, you must enable the community string of the Catalyst 6K chassis.
- For CSS devices, you must enable the community string of the CSS device itself.

Procedure

-
- Step 1** Select **Config > Operations > Virtual Servers**. The Virtual Servers table appears.
- Step 2** Select the virtual server that you want to activate, then click **Activate**. The server is activated and the screen refreshes with updated information in the Configured State column.
-

Related Topics

- [Managing Virtual Servers, page 4-55](#)
- [Viewing Virtual Servers, page 4-63](#)
- [Suspending Virtual Servers, page 4-59](#)

Suspending Virtual Servers

Use this procedure to suspend a virtual server.

**Note**

A missing operation or Admin state on a CSM or CSS device most likely means that the community string was not enabled on those devices. If the community string is not enabled on a CSM or CSS device, and any kind of operation is performed on those devices, it will not succeed, and ANM will not provide any kind of indication.

- For CSM devices, you must enable the community string of the Catalyst 6K chassis.
- For CSS devices, you must enable the community string of the CSS device itself.

Procedure

-
- Step 1** Select **Config > Operations > Virtual Servers**. The Virtual Servers table appears.
- Step 2** Select the virtual server that you want to suspend, then click **Suspend**. The Suspend Virtual Server screen appears.

- Step 3** In the Reason field, enter the reason for this action. You might enter a trouble ticket, an order ticket, or a user message. **Do not enter a password in this field.**
-

Related Topics

- [Managing Virtual Servers, page 4-55](#)
- [Viewing Virtual Servers, page 4-63](#)
- [Activating Virtual Servers, page 4-59](#)

Managing GSS VIP Answers

In a GSS network, the term answers refers to resources that respond to content queries. When you create an answer using the primary Global Site Selector Manager (PGSSM), you are simply identifying a resource on your GSS network to which queries can be directed and that can provide your user's D-proxy with the address of a valid host to serve their request.

Virtual IP (VIP) addresses associated with an SLB such as the Cisco CSS, Cisco CSM, Cisco IOS-compliant SLB, LocalDirector, or a Web server are types of answers that are specified in the ANM UI in the GSS VIP Answers table found in ANM under **Configuration > Operations**. Use this procedure to poll, activate, or suspend GSS VIP answers.

Assumption

You have established GSS VIP answers using the PGSSM.

Procedure

- Step 1** Select **Config > Operations > GSS VIP Answers**. The GSS Answers table appears. For a list of fields available, see [Table 4-20](#).

Table 4-20 GSS Answer Table

Field	Description
Multiple Row Selection Checkbox	Check to select all entries at the same time, or check line items individually.
IP Address	VIP answer IP address.
Name	VIP answer name.
Config State	VIP answer configured status.
PGSSM Oper State	Operational status as shown on the primary GSS manager (PGSSM).
Answer Group	Answer group names to which the VIP answer belong.
Location	Logical groupings for GSS resources that correspond to geographical entities such as a city, data center, or content site.
Device	Primary GSS device name on ANM.
PGSSM Time	Last operational status update time on the primary GSS.

- Step 2** Click the checkbox(es) to the left of the servers you want to poll, activate or suspend.

Step 3 Click:

- **Active/Suspended** hyperlink to view the VIP answer details across the GSS node(s). A popup window appears listing all nodes associated with the VIP, operational state, hit count, and timestamp for each node.
- **Poll Now** to query the chosen resource to verify it is still active.

**Note**

If you click **Poll Now** immediately after you click **Activate** or **Suspend**, you might not get the VIP answer operational status on the PGSSM that reflects your most recent configuration. It might be necessary to click Poll Now 2 or 3 times in succession to get an accurate result.

Apart from this, the ability of ANM to update the VIP answer operational status and statistics accurately in detailed GSS statistics window might depend on the polling interval that has been configured on the GSS. The polling interval can be configured directly on the GSS device. (The default is 5 minutes.) Therefore, it can take 5 minutes or more, depending on the interval, for the ANM server to show an accurate result.

- **Activate** to reactivate a GSS answer.
- **Suspend** to temporarily stop the GSS from using an associated answer.

If you clicked **Activate** or **Suspend**, a dialog box prompts for a Reason. Acceptable text consists of any characters or nothing at all.

Step 4 Click:

- **Deploy Now** to complete Activation or Suspension.
- **Cancel** to cancel the Activation or Suspension operation.

Related Topics

- [Load Balancing Overview, page 4-1](#)
- [Activating and Suspending DNS Rules Governing GSS Load Balancing, page 4-62](#)

Activating and Suspending DNS Rules Governing GSS Load Balancing

The DNS rules table in **Configuration > Operations** navigation tree specifies actions for the GSS to take when it receives a request from a known source (a member of a source address list) for a known hosted domain (a member of a domain list).

The DNS rule specifies which response (answer) is given to the requesting user's local DNS host (D-proxy) and how that answer is chosen. One of a variety of balance methods is used to determine the best response to the request, based on the status and load of the GSS host devices.

Use this procedure to activate or suspend DNS rules associated with your GSS VIP answers table.

Assumption

You have established GSS VIP answers and DNS rules using the PGSSM.

Procedure

- Step 1** Select **Config > Operations > DNS Rules**. The DNS Rules table appears. For a list of fields available, see [Table 4-21](#).

Table 4-21 DNS Rules Table

Field	Description
Multiple Row Selection Checkbox	Check to select all entries at the same time, or check line items individually.
Name	Name of the DNS rule.
Source Address	Collection of IP addresses or address blocks for known client DNS proxies (or D-proxies).
Domains	Domain list name containing one or more domain names that point to content for which the GSS is acting as the authoritative DNS server and for which you wish to use the GSS technology to balance traffic and user requests.
Config State	DNS rules configured status, either Active or Suspended.
Answer Group	Lists of GSS resources that are candidates to respond to DNS queries received from a user for a hosted domain.
Owner	Owner names, providing a simple way to organize and identify groups of related GSS resources.
Device	Primary GSS device name on ANM.
PGSSM Time	Last operational status update time on the GSS.

- Step 2** Click the checkbox(es) to the left of the servers you want to activate or suspend.
- Step 3** Click the **Activate** or **Suspend** button. A dialog box prompts for a Reason. Acceptable text consists of any characters or none at all.
- Step 4** Click:
- **Deploy Now** to complete Activation or Suspension.
 - **Cancel** to cancel the Activation or Suspension operation.

Related Topics

- [Load Balancing Overview, page 4-1](#)
- [Managing GSS VIP Answers, page 4-60](#)

Viewing Detailed Virtual Server Information

Use this procedure to view detailed information about the state of a virtual server.

Procedure

-
- Step 1** Select **Config > Operations > Virtual Servers**. The Virtual Servers table appears.
- Step 2** Select the virtual server whose configuration details you want to view. Click the hyperlinked entry for that virtual server that appears in the Operational State column. The Details window appears with the following information:
- Current operational status
 - Description, if one was entered
 - Configured interfaces, such as VLANs
 - Configured service policies including:
 - Configured class maps, detailed by type (such as load balancing or inspection)
 - States of configured options, indicated by word (**ACTIVE**, **DISABLED**, **OUTOFSERVICE**) and color (green, orange/yellow, and red)
 - Associated policy maps with details on their type and action (L7 loadbalance, serverfarm)
 - Statistics regarding connections and counts
-

Related Topics

- [Configuring Virtual Servers, page 4-2](#)
- [Managing Virtual Servers, page 4-55](#)

Viewing Virtual Servers

To view all virtual servers, select **Config > Operations > Virtual Servers**. The Virtual Servers table appears with the following information for each server:

- Server name, sorted by virtual context
- Admin state
- Operational state



Note This column is populated for ACE 4710 appliances running image A3(1.0) and later. Clicking on the value in this column (irrespective of ACE version) will display detailed information about the Virtual Server in a popup.

- Number of active connections



Note This column is populated for ACE 4710 appliances running image A3(1.0) and later. For ACE devices, the Active Connections column will display N/A for older versions of the ACE appliance and module.

- VIP address
- Configured port
- VLANs
- Associated server farms
- Device
- High availability

You can activate or suspend virtual servers from this table and obtain additional information about the state of the virtual server.

Related Topics

- [Activating Virtual Servers, page 4-59](#)
- [Suspending Virtual Servers, page 4-59](#)
- [Viewing Detailed Virtual Server Information, page 4-63](#)

Understanding CLI Commands Sent from Virtual Server Table

Table 4-22 displays the CLI commands dispatched to the device for a given Virtual Servers table option, and is sorted by device.

Table 4-22 CLI Commands Deployed from Real Servers Table

Command	Sample CLI Sent
ACE Modules and Appliances	
Virtual Server Activate	policy-map multi-match int25 class VIP3 loadbalance vip inservice
Virtual Server Suspend	policy-map multi-match int25 class VIP3 no loadbalance vip inservice
CSMs	
Virtual Server Activate	vserver APP1 inservice
Virtual Server Suspend	vserver APP1 no inservice

Table 4-22 *CLI Commands Deployed from Real Servers Table*

Command	Sample CLI Sent
CSS Devices	
Virtual Server Activate	owner hm content LB active
Virtual Server Suspend	owner hm content LB suspend

