CHAPTER 5

Configuring Virtual Servers

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

Note When you use the ACE CLI to configure named objects (such as a real server, virtual server, parameter map, class map, health probe, and so on), consider that the Device Manager (DM) supports object names with an alphanumeric string of 1 to 64 characters, which can include the following special characters: underscore (_), hyphen (-), dot (.), and asterisk (*). Spaces are not allowed.

If you use the ACE CLI to configure a named object with special characters that the DM does not support, you may not be able to configure the ACE using DM.

This chapter contains the following topics:

Load Balancing Overview

Server load balancing (SLB) is the process of deciding to which server a load-balancing device 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 appliance performs a series of checks and calculations to determine the server that can best service each client request. The ACE appliance 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 ACE Appliance Device Manager allows you to configure load balancing as described in the following topics:

- Virtual servers—See Configuring Virtual Servers, page 5-2.
- Real servers—See Configuring Real Servers, page 6-5.
- Server farms—See Configuring Server Farms, page 6-18.

- Sticky groups—See Configuring Sticky Groups, page 7-11.
- Parameter maps—See Configuring Parameter Maps, page 8-1.

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

- Configuring Virtual Servers, page 5-2
- Load-Balancing Predictors, page 6-2
- Real Servers, page 6-3
- Server Farms, page 6-5
- Configuring Health Monitoring, page 6-39
- TCL Scripts, page 6-40
- Configuring Sticky Groups, page 7-11

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, round-robin, least connections, and so on) determine the servers to which the ACE sends connection requests.

For more information about virtual servers and the ACE Appliance Device Manager, see the following topics:

- Understanding Virtual Server Configuration and ACE Appliance Device Manager, page 5-2
- Information About Using Device Manager to Configure Virtual Servers, page 5-5
- Virtual Server Configuration Procedure, page 5-7

Understanding Virtual Server Configuration and ACE Appliance Device Manager

The ACE Appliance Device Manager 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 ACE Appliance Device Manager for virtual server configuration.

In ACE Appliance Device Manager, 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 an IPv4 netmask or IPv6 prefix length 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 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 5-1 shows the minimum configuration statements required for a virtual server.

Example 5-1 Minimum Configuration Required for a Virtual Server

IPv4

```
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
```

IPv6

```
class-map match-all Example2_VIP
   2 match virtual-address 2001:DB8:10::5 tcp eq www
policy-map type loadbalance first-match Example2_VIP-l7slb
   class class-default
      forward
policy-map multi-match int11
   class Example2_VIP
      loadbalance policy Example2_VIP-l7slb

interface vlan 10
   ip address 2001:DB8:10::21/64
   service-policy input int11
   no shutdown
```

Note the following items regarding the ACE Appliance Device Manager 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 ACE Appliance Device Manager 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 ACE Appliance Device Manager interface ensures that a user who can view or modify virtual servers or aspects of virtual servers cannot create or delete virtual servers.

- RBAC role and domain requirements

  If you want to create, modify, or delete a virtual server, we recommend that you use the pre-defined Admin role (see Table 15-4).Only the Admin pre-defined role supports the ability to successfully deploy a functional virtual server from the ACE appliance Device Manager.

  If a user prefers to be assigned a custom role, and wants the ability to create, modify, or delete a virtual server, that user requires the proper role permissions to be defined by the administrator to allow them to perform those virtual server activities.

Note A user must be assigned with a default domain (default-domain) to be able to configure a virtual server. A domain is the namespace in which a user operates.

Included below are a list of RBAC permissions which are required for a user to create, modify, or delete a virtual server:

```
-------------------------------------------
 Rule    Type    Permission      Feature
 -----------------------------------------
  1.   Permit    Create               real
  2.   Permit    Create         serverfarm
  3.   Permit    Create                vip
  4.   Permit    Create              probe
  5.   Permit    Create        loadbalance
  6.   Permit    Create                nat
  7.   Permit    Create          interface
  8.   Permit    Create         connection
  9.   Permit    Create                ssl
 10.   Permit    Create                pki
 11.   Permit    Create             sticky
 12.   Permit    Create            inspect
```

Note that certain configured virtual servers may only cover a subset of the features and may not require all the permissions outlined above. In general, the above set of permissions are required for allowing users to configure all elements of a virtual server.

For background information, see the "Managing User Roles" section in Chapter 15, "Managing the ACE Appliance".

Related Topics

- Configuring Virtual Servers, page 5-2
- Information About Using Device Manager to Configure Virtual Servers, page 5-5
- Virtual Server Configuration Procedure, page 5-7

Information About Using Device Manager to Configure Virtual Servers

It is important to understand the following when using the ACE Appliance Device Manager to configure virtual servers:

- **Virtual server configuration screens**

  The ACE Appliance Device Manager 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 ACE Appliance Device Manager 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 > Virtual Contexts >** *context* **> Expert > Class Maps or Policy** or **Config > Virtual Contexts >** *context* **> Load Balancing > Parameter Map** to configure more complex attributes of virtual servers, traffic policies, and parameter maps.

- **Synchronizing virtual server configurations**

  When you use the CLI to change a virtual context's configuration on the ACE appliance, the ACE Appliance Device Manager periodically polls the CLI (approximately once every two minutes) for configuration changes. When it detects an out-of-band configuration change in a context, the changes are applied to the configuration maintained by ACE Appliance Device Manager. The status bar at the bottom of the ACE Appliance Device Manager indicates a summary count of the contexts in the various synchronization states

  If you configure a virtual server using the CLI and then use the CLI Sync option (**Config > Virtual** *Contexts* > CLI Sync) to manually synchronize configurations, the configuration that appears in the ACE Appliance Device Manager for the virtual server might not display all configuration options for that virtual server. The configuration that appears in the ACE Appliance Device Manager 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 ACE Appliance Device Manager.

- **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 5-9 for more information about modifying objects used by multiple virtual servers.

Related Topics

- Configuring Virtual Servers, page 5-2
- Understanding Virtual Server Configuration and ACE Appliance Device Manager, page 5-2
- Virtual Server Configuration Procedure, page 5-7

Virtual Server Usage Guidelines

The Virtual Server configuration window provides you with numerous configuration options. However, instead of setting every option in one pass, configure your virtual server in stages. The first stage should always be to establish basic “pass through” connectivity with simple load balancing and include minimal additional features. This level of setup should verify that ports, VLANs, interfaces, SSL termination (if applicable), and real servers have been set up properly, enabling basic connectivity.

After you establish this level of connectivity, additional virtual server features will be easier to configure and troubleshoot.

Common features to add to a working basic virtual server are as follows:

- Health monitoring probes
- Session persistence (sticky)
- Additional real servers to a server farm
- Application protocol inspection
- Application acceleration and optimization

Table 5-1 identifies and describes virtual server configuration subsets with links to related topics for configuration information.

Related Topics

- Configuring Virtual Servers, page 5-2
- Information About Using Device Manager to Configure Virtual Servers, page 5-5
- Virtual Server Testing and Troubleshooting, page 5-6
- Virtual Server Configuration Procedure, page 5-7

Virtual Server Testing and Troubleshooting

As outlined in the “Virtual Server Usage Guidelines” section on page 5-6, first set up a basic virtual server that only enables connectivity and simple load balancing, such as round-robin between two real servers. Next, use a client, such as a web browser, to send a request from the client network to the virtual server VIP address. If the request is successful, you can now make changes or add virtual server features.

If the request is not successful, begin virtual server troubleshooting as outlined in the following sequence:

1. Wait and retry your request after a minute or two, especially if the existing ACE configuration is large. It can take seconds or even minutes for configuration changes to affect how traffic is handled by ACE.
2. Click the **Details** button in the lower right of the Virtual Server page. The Details button displays the output of the **show service-policy** CLI command.
3. Verify that the VIP State in the **show service-policy** CLI command output is INSERVICE. If the VIP state is not INSERVICE, this may indicate the following:
   - The virtual server has been manually disabled in the configuration.
   - The real servers are all unreachable from ACE or manually disabled. If all of a virtual server's real servers are out of service due to one of those reasons, the virtual server itself will be marked Out Of Service.

4. Verify the Hit Count in the **show service-policy** CLI command output. Hit Count shows the number of requests received by ACE. This value should increase for each request attempted by your client. If the hit count does not increase with each request, this indicates that the request is not reaching your virtual server configuration.

   This could be a problem with one of the following:

   – A physical connection.

   – VLAN or VLAN interface configuration.

   – Missing or incorrect ACL applied to the client interface.

   – Incorrect IP address (that is, a VIP that is not valid on the selected VLANs for the virtual server, or a VIP that is not accessible to your client).

   If the Hit Count value increases but no response is received (Server Pkt Count does not increases), the problem is more likely to be in the connectivity between the ACE and the backend real servers. This issue is typically caused by one or more of the following problems:

   – You are working on a one-armed configuration (that is, do not plan to change routing for your real servers) and have not selected an appropriate NAT pool for your virtual server to use with source NAT.

   – A different routing problem (for example, server traffic does not know how to get back to the ACE).

   – Addressing problem (for example, you have an incorrect real server address, or the real server is not accessible to ACE due to network topology).

Note Hit count can increase by more than one, even if you make only a single request from your web browser, because retrieving a typical web page makes many requests from the client to the server.

Related Topics

- Configuring Virtual Servers, page 5-2
- Information About Using Device Manager to Configure Virtual Servers, page 5-5
- Virtual Server Usage Guidelines, page 5-6
- Virtual Server Configuration Procedure, page 5-7

Virtual Server Configuration Procedure

Use this procedure to add virtual servers to the ACE Appliance Device Manager 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 Choose **Config > Virtual Contexts >** *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, and 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 configuration entries you make in the Properties subset. Change views by using the View object selector at the top of the configuration pane.

Table 5-1 identifies and describes virtual server configuration subsets with links to related topics for configuration information.

Table 5-1 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 5-10
SSL Termination[1]	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 5-18
Protocol Inspection	This subset appears in the Advanced View for the following: • 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 appliance on selected application protocols.	Configuring Virtual Server Protocol Inspection, page 5-20
L7 Load-Balancing	This subset appears only in the Advanced View for the following: • 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[1].	Configuring Virtual Server Layer 7 Load Balancing, page 5-30
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. It also allows you to configure SSL initiation[1]. SSL initiation appears only in the Advanced View.	Configuring Virtual Server Default Layer 7 Load Balancing, page 5-55

Table 5-1 Virtual Server Configuration Subsets (continued)

Configuration Subset	Description	Related Topics
Application Acceleration And Optimization	This subset appears only in the Advanced View and 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 5-57
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 5-61

1. The SSL initiation and termination configuration options do not apply to the ACE NPE software version (see the "Information About the ACE No Payload Encryption Software Version" section on page 1-2).

Step 3 When you finish configuring virtual server properties, do the following:

- Click **Deploy Now** to deploy the configuration on the ACE appliance.
- Click **Cancel** to exit the procedure without saving your entries and to return to the Virtual Servers table.

Step 4 (Optional) To display statistics and status information for an existing virtual server, from the Virtual Servers table, choose a virtual server and click **Details**.

A pop-up window appears that displays the detailed virtual server information (see the "Displaying Virtual Server Statistics and Status Information" section on page 5-62 for details).

Note This feature requires ACE software Version A3(2.1) or later. An error displays with earlier software versions.

Related Topics

- Configuring Virtual Servers, page 5-2
- Understanding Virtual Server Configuration and ACE Appliance Device Manager, page 5-2
- Information About Using Device Manager to Configure Virtual Servers, page 5-5
- Shared Objects and Virtual Servers, page 5-9
- Role Mapping in ACE Appliance Device Manager, page 15-19

Shared Objects and Virtual Servers

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

- 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

ACE Appliance Device Manager offers the following options for shared objects in virtual server configuration screens (**Config** > **Virtual Contexts** > *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, and 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 5-63
- Configuring Virtual Server Properties, page 5-10
- Configuring Virtual Server SSL Termination, page 5-18
- Configuring Virtual Server Protocol Inspection, page 5-20
- Configuring Virtual Server Layer 7 Load Balancing, page 5-30
- Configuring Virtual Server Default Layer 7 Load Balancing, page 5-55
- Configuring Application Acceleration and Optimization, page 5-57

Configuring Virtual Server Properties

Use this procedure to configure virtual server properties.

Procedure

Step 1 Choose **Config > Virtual Contexts >** *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, and 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 5-2.

Table 5-2 Virtual Server Properties – Advanced View

Field	Description
Virtual Server Name	Enter the name for the virtual server.
IP Address Type	Select either IPv4 or IPv6 for the address type of the virtual server.
Virtual IP Address	Enter the IP address for the virtual server.
Virtual IP Mask	(IPv4 address type only) Select the subnet mask to apply to the virtual server IP address.
Virtual IP Prefix Length	(IPv6 address type only) Enter the prefix length to apply to the virtual server IP address. The default length for the prefix is 128.
Transport Protocol	Select the protocol the virtual server supports: • Any—Indicates the virtual server is to accept connections using any IP protocol. • TCP—Indicates that the virtual server is to accept connections that use TCP. • UDP—Indicates that the virtual server is to accept connections that use UDP. **Note** This field is read-only if you are editing an existing virtual server. The Device Manager 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 protocol.

Table 5-2 Virtual Server Properties – Advanced View (continued)

Field	Description
Application Protocol	This field appears if TCP or UDP is selected. Select the application protocol to be supported by the virtual server. **Note** This field is read-only if you are editing an existing virtual server. The Device Manager 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. For TCP, the options are as follows: • FTP—File Transfer Protocol • Generic—Generic protocol parsing • HTTP—Hyper Text Transfer Protocol • HTTPS—HTTP over SSL If you select HTTPS, the SSL Termination configuration subset appears. See the "Configuring Virtual Server SSL Termination" section on page 5-18. • Other—Any protocol other than those specified • RDP—Remote Desktop Protocol • RTSP—Real Time Streaming Protocol • SIP—Session Initiation Protocol • Unterminated HTTPS **Note** This option is not available if the ACE is using the NPE software version (see the "Information About the ACE No Payload Encryption Software Version" section on page 1-2). For UDP, the options are as follows: • DNS—Domain Name System • Generic—Generic protocol parsing • Other—Any protocol other than those specified • RADIUS—Remote Authentication Dial-In User Service • SIP—Session Initiation Protocol If you select any specific application protocol, the Protocol Inspection configuration subset appears. See the "Configuring Virtual Server Protocol Inspection" section on page 5-20.

Table 5-2 Virtual Server Properties – Advanced View (continued)

Field	Description
Port	By default, this field appears with the default port number for the specified protocol. To change the port number, 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.

Table 5-2 Virtual Server Properties – Advanced View (continued)

Field	Description
VLAN	This field appears if the All VLANs check box is cleared. In the Available list, select the VLANs to use for incoming traffic, and then click **Add to Selection**. The items appear in the Selected list. To remove VLANs, select them in the Selected lists and then click **Remove from Selection**. The items appear in the Available list. **Note** You cannot change the VLAN for a virtual server once it is specified. Instead, you need to delete the virtual server and create a new one with the desired VLAN.
HTTP Parameter Map	This field appears if HTTP or HTTPS is the selected application protocol. Select an existing HTTP parameter map or click ***New*** to create a new one: • If you select an existing parameter map, you can view, modify, or duplicate the existing configuration. See the "Shared Objects and Virtual Servers" section on page 5-9 for more information about modifying shared objects. • If you click ***New***, the HTTP Parameter Map configuration pane appears. Configure the HTTP parameter map as described in Table 8-2.
Connection Parameter Map	This field appears if TCP is the selected protocol. Select an existing connection parameter map or click ***New*** to create a new one: • If you select an existing parameter map, you can view, modify, or duplicate the existing configuration. See the "Shared Objects and Virtual Servers" section on page 5-9 for more information about modifying shared objects. • If you click ***New***, the Connection Parameter Map configuration pane appears. Configure the connection parameter map as described in Table 8-3. **Note** Click **More Settings** to access the additional Connection Parameter Maps configuration attributes. By default, Device Manager hides the default Connection Parameter Maps configuration attributes and the attributes which are not commonly used.

Table 5-2 Virtual Server Properties – Advanced View (continued)

Field	Description
KAL-AP-TAG Name	The KAL-AP-TAG feature allows the Cisco Global Site Selector (GSS) proprietary KAL-AP protocol to extract load and availability information from the ACE when a firewall is positioned between the GSS and the ACE. This feature allows you to configure a tag (name) per VIP for a maximum of 4,096 tags on an ACE. This feature does not replace the tag per domain feature. For more information about this feature, see the Configuring Health Monitoring chapter in the *Server Load-Balancing Guide, Cisco ACE Application Control Engine*. In the KAL-AP-TAG Name field, enter the name as an unquoted text string with no spaces and a maximum of 76 alphanumeric characters. The following scenarios are not supported and will result in an error: • You cannot configure a tag name for a VIP that already has a tag configuration as part of a different policy configuration. • You cannot associate the same tag name with more than one VIP. • You cannot associate the same tag name with a domain and a VIP. • You cannot assign two different tags to two different Layer 3 class maps that have the same VIP, but different port numbers. The KAL-AP protocol considers these class maps to have the same VIP and calculates the load for both Layer 3 rules together when the GSS queries the VIP.
Kal-AP Primary Out of Service	Check this box for the ACE to notify the Global Site Selector (GSS) that the primary server farm is down when the backup server farm is in use. By default, when you configure a redirect server farm as a backup server farm on the ACE and the primary server farm fails, the backup server farm redirects the client requests to another data center. However, the VIP remains in the INSERVICE state. When you configure the ACE to communicate with a GSS, it provides information for server availability. When a backup server is in use after the primary server farm is down and this feature is enabled, the ACE informs the GSS that the VIP for the primary server farm is out of service by returning a load value of 255. The GSS recognizes that the primary server farm is down and sends future DNS requests with the IP address of the other data center. Clear this check box to disable this feature.
DNS Parameter Map	This field appears if DNS is the selected protocol over UDP. Select an existing DNS parameter map or click ***New*** to create a new one: • If you select an existing parameter map, you can view, modify, or duplicate the existing configuration. See the "Shared Objects and Virtual Servers" section on page 5-9 for more information about modifying shared objects. • If you click ***New***, the DNS Parameter Map configuration pane appears. Configure the DNS parameter map as described in Table 8-11.

Table 5-2 Virtual Server Properties – Advanced View (continued)

Field	Description
Generic Parameter Map	This field appears if Generic is the selected application protocol over TCP or UDP. Select an existing Generic parameter map or click ***New*** to create a new one: • If you select an existing parameter map, you can view, modify, or duplicate the existing configuration. See the "Shared Objects and Virtual Servers" section on page 5-9 for more information about modifying shared objects. • If you click ***New***, the Generic Parameter Map configuration pane appears. Configure the Generic parameter map as described in Table 8-7.
RTSP Parameter Map	This field appears if RTSP is the selected application protocol over TCP. Select an existing RTSP parameter map or click ***New*** to create a new one: • If you select an existing parameter map, you can view, modify, or duplicate the existing configuration. See the "Shared Objects and Virtual Servers" section on page 5-9 for more information about modifying shared objects. • If you click ***New***, the RTSP Parameter Map configuration pane appears. Configure the RTSP parameter map as described in Table 8-8.
ICMP Reply	Indicate how the virtual server is to respond to ICMP ECHO requests: • None—Indicates that the virtual server is not to send ICMP ECHO-REPLY responses to ICMP requests. • Active—Indicates that the virtual server is to send ICMP ECHO-REPLY responses only if the configured VIP is active. • Always—Indicates that 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.
Status	Indicate whether the virtual server is to be in service or out of service: • 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 5-3.

Table 5-3 Virtual Server Properties – Basic View

Field	Description
Virtual Server Name	Enter the name for the virtual server.
IP Address Type	Select either IPv4 or IPv6 for the address type of the virtual server.
Virtual IP Address	Enter the IP address for the virtual server.
Transport Protocol	Select the protocol that the virtual server supports: • Any—Indicates that the virtual server is to accept connections using any IP protocol. • TCP—Indicates that the virtual server is to accept connections that use TCP. • UDP—Indicates that the virtual server is to accept connections that use UDP.
Application Protocol	Select the application protocol to be supported by the virtual server. For TCP, the options as follows: • FTP—File Transfer Protocol • HTTP—Hyper Text Transfer Protocol • HTTPS—HTTP over SSL If you select HTTPS, the SSL Termination configuration subset appears. See the "Configuring Virtual Server SSL Termination" section on page 5-18. **Note** This option is not available if the ACE is using the NPE software version (see the "Information About the ACE No Payload Encryption Software Version" section on page 1-2). • Generic—Generic protocol parsing • Other—Any protocol other than those specified. • RTSP—Real Time Streaming Protocol • RDP—Remote Desktop Protocol • SIP—Session Initiation Protocol For UDP, the options as follows: • DNS—Domain Name System • Generic—Generic protocol parsing • Other—Any protocol other than those specified. • RTSP—Real Time Streaming Protocol • RADIUS—Remote Authentication Dial-In User Service • SIP—Session Initiation Protocol

Table 5-3 Virtual Server Properties – Basic View (continued)

Field	Description
Port	By default, this field appears with the default port number for the specified protocol. To change the port number, 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 all 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 list, select the VLANs to use for incoming traffic, and then click **Add to Selection**. The items appear in the Selected list. To remove VLANs, select them in the Selected lists, and then click **Remove from Selection**. The items appear in the Available list. **Note** You cannot change the VLAN for a virtual server once it is specified. Instead, you need to delete the virtual server and create a new one with the desired VLAN.

Step 5 When you finish configuring virtual server properties, do the following:

- Click **Deploy Now** to deploy the configuration on the ACE appliance.
- Click **Cancel** to exit the procedure without saving your entries.

Related Topics

- Configuring Virtual Servers, page 5-2
- Configuring Virtual Server SSL Termination, page 5-18

Configuring Virtual Server SSL Termination

Note The information in this section does not apply to the ACE NPE software version (see the "Information About the ACE No Payload Encryption Software Version" section on page 1-2).

SSL termination service allows the virtual server to act as an SSL proxy server and terminate SSL sessions between it and its clients and then establishes a TCP connection to an HTTP server. When the ACE terminates the SSL connection, it decrypts the ciphertext from the client and transmits the data as clear text to an HTTP server.

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 the "Configuring Virtual Server Properties" section on page 5-10.

Procedure

Step 1 Choose **Config** > **Virtual Contexts** > *context* > **Load Balancing** > **Virtual Servers**. The Virtual Servers table appears.

Step 2 Select the virtual server you want to configure for SSL termination, and 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 the "Shared Objects and Virtual Servers" section on page 5-9 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 5-4.

Table 5-4 Virtual Server SSL Termination Attributes

Field	Description
Name	Enter a name for this SSL proxy service. Valid entries are alphanumeric strings with a maximum of 64 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.
CRL Best-Effort	This option appears if you select an authentication group in the Auth Group Name field. Check the check box to allow the ACE 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 if the ACE is to use for this proxy service.
Parameter Maps	Select the SSL parameter map to associate with this proxy server service.

For more information about SSL, see the "Configuring SSL" section on page 9-1.

Step 6 When you finish configuring virtual server properties, do the following:

- Click **Deploy Now** to deploy this configuration on the ACE appliance.

- Click **Cancel** to exit this procedure without saving your entries.

Related Topics

- Configuring Virtual Servers, page 5-2
- Configuring Virtual Server Properties, page 5-10

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 appliance.

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.

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 the "Configuring Virtual Server Properties" section on page 5-10 for information on configuring these protocols.

Procedure

Step 1 Select **Config** > **Virtual Contexts** > *context* > **Load Balancing** > **Virtual Servers**. The Virtual Servers table appears.

Step 2 Select the virtual server that you want to configure for protocol inspection, and 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, ACE appliances allow all request methods.

Step 5 If you checked the Enable Inspect check box, configure additional inspection options according to virtual server application protocol configuration:

- For DNS, in the Length field enter the maximum length of the DNS packet in bytes. Valid entries are from 512 to 65535 bytes. If you do not enter a value in this field, the DNS packet size is not checked.
- For FTP, continue with Step 6.
- For HTTP and HTTPS, continue with Step 7.
- For SIP, continue with Step 9.

Note There are no protocol-specific inspection options for RTSP.

Step 6 For FTP protocol inspection, do the following:

a. 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.

b. 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 12-13 for more information about the FTP commands.

- Select the commands that are to be blocked by the virtual server in the Available list, and then click **Add**. The commands appear in the Selected list.
- To remove commands that you do not want to be blocked, select them in the Selected list, and then click **Remove**. The commands appear in the Available list.

Step 7 For HTTP or HTTPS inspection, do the following:

a. 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.

b. In the Policy subset, click **Add** to add a new match condition and action, or select an existing match condition and action, and then click **Edit** to modify it. The Policy configuration pane appears.

c. 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 the "Shared Objects and Virtual Servers" section on page 5-9 for more information about modifying shared objects.

d. Configure match criteria and related actions by following the steps in Table 5-5.

Table 5-5 Protocol Inspection Match Criteria Configuration

Selection	Action
Existing class map	1. Click **View** to review the match condition information for the selected class map. 2. Do the following: – Click **Cancel** to continue without making changes and to return to the previous screen. – Click **Edit** to modify the existing configuration. – Click **Duplicate** to create a new class map with the same attributes without affecting other virtual servers using the same class map. See the "Shared Objects and Virtual Servers" section on page 5-9 for more information about modifying shared objects. 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: – Permit—Indicates that the specified traffic is to be received by the virtual server if it meets the specified deep inspection match criteria. – Reset—Indicates that 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 5-5 Protocol Inspection Match Criteria Configuration (continued)

Selection	Action
New	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: – All—Indicates that a match exists only if all match conditions are satisfied. – Any—Indicates that a match exists if at least one of the match conditions is satisfied. 3. In the Conditions table, click **Add** to add a new set of conditions, or select an existing entry, and 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 and configure protocol-specific criteria using the information in Table 5-6. 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: – Permit—Indicates that the specified traffic is to be received by the virtual server if it meets the specified deep inspection match criteria. – Reset—Indicates that 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	1. In the Conditions Type field, select the type of inline match condition that is to be met for protocol inspection. Table 5-6 describes the types of conditions and their related configuration options. 2. Provide condition-specific criteria using the information in Table 5-6. 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: – Permit—Indicates that the specified traffic is to be received by the virtual server if it meets the specified deep inspection match criteria. – Reset—Indicates that 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 5-6 HTTP and HTTPS Protocol Inspection Conditions and Options

Condition	Description
Content	Specific content contained within the HTTP entity-body is to be used for application inspection decisions. 1. In the Content Expression field, enter the content that is to be matched. Valid entries are alphanumeric strings from 1 to 255 characters. 2. 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	The content parse length is used for application inspection decisions. 1. In the Content Length Operator field, select the operand to use to compare content length: – 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. 2. Enter values to apply for content length comparison: – 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: 1. 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. 2. 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	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.

Table 5-6 HTTP and HTTPS Protocol Inspection Conditions and Options (continued)

Condition	Description
Header	The name and value in an HTTP header are used for application inspection decisions. **1.** In the Header field, select one of the predefined HTTP headers to match, or select HTTP Header to specify a different HTTP header. **2.** 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. **3.** 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 12-33 for a list of the supported characters that you can use in regular expressions.
Header Length	The length of the header in the HTTP message is used for application inspection decisions. **1.** In the Header Length Type field, specify whether HTTP header request or response messages are to be used for application inspection decisions: – Request—HTTP header request messages are to be checked for header length. – Response—HTTP header response messages are to be checked for header length. **2.** In the Header Length Operator field, select the operand to be used to compare header length: – 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. **3.** Enter values to apply for header length comparison: – 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: 1. 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. 2. 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	Multipurpose Internet Mail Extension (MIME) message types are used for application inspection decisions. In the Header MIME Type field, select the MIME message type to use for this match condition.

Table 5-6 HTTP and HTTPS Protocol Inspection Conditions and Options (continued)

Condition	Description
Port Misuse	The misuse of port 80 (or any other port running HTTP) is to be used for application inspection decisions. Indicate the application category to use for this match condition: • 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	A request method is to be used for protocol inspection decisions. By default, the ACE allows all request and extension methods. This option allows you to configure protocol inspection decisions based on compliance to request methods defined in RFC 2616 and by HTTP extension methods. 1. Select the type of request method to use for this match condition: – Ext—An HTTP extension method is to be used. **Note** The list of available HTTP extension methods from which to choose varies depending on the version of software installed in the ACE. – 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	Compliance with HTTP RFC 2616 is to be used for application inspection decisions.
Transfer Encoding	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. In the Transfer Encoding field, select the type of encoding that is to be checked: • Chunked—The message body is transferred as a series of chunks. • Compress—The encoding format that is produced by the UNIX file compression program *compress*. • 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 5-6 HTTP and HTTPS Protocol Inspection Conditions and Options (continued)

Condition	Description
URL	URL names are to be used for application inspection decisions. 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 www.*hostname.domain*. For example, in the URL www.anydomain.com/latest/whatsnew.html, include only /latest/whatsnew.html.
URL Length	URL length is to be used for application inspection decisions. **1.** In the URL Length Operator field, select the operand to use to compare URL length: – 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. **2.** Enter values to apply for URL length comparison: – 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: 1. 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. 2. 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.

e. Do the following:

– Click **OK** to save your entries. The Conditions table refreshes with the new entry.

– Click **Cancel** to exit the Policy subset without saving your entries.

f. 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:

– Permit—Indicates that the specified HTTP traffic is to be received by the virtual server.

– Reset—Indicates that the specified HTTP traffic is to be denied by the virtual server.

– N/A—Indicates that this attribute is not set.

Step 8 For SIP inspection, do the following:

a. In the Actions subset, click **Add** to add a new match condition and action, or select an existing match condition and action, and then click **Edit** to modify it. The Actions configuration pane appears.

b. 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 the "Shared Objects and Virtual Servers" section on page 5-9 for more information about modifying shared objects.

c. Configure match criteria and related actions using the information in Table 5-7.

Table 5-7 SIP Protocol Inspection Conditions and Options

Condition	Description
Called Party	The destination or called party specified in the URI of the SIP To header is used for SIP protocol inspection decisions. 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 12-33 lists the supported characters that you can use for matching string expressions.
Calling Party	The source or caller specified in the URI of the SIP From header is used for SIP protocol inspection decisions. 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 12-33 lists the supported characters that you can use for matching string expressions.
IM Subscriber	An IM (instant messaging) subscriber is used for application inspection decisions. 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 12-33 lists the supported characters that you can use for matching string expressions.
Message Path	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 URIs in the form of regular expressions and checks this list against the VIA header field in each SIP packet. 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 12-33 lists the supported characters that you can use for matching string expressions.
SIP Content Type	The content type in the SIP message body is used for SIP protocol inspection decisions. 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 12-33 lists the supported characters that you can use for matching string expressions.

Table 5-7 SIP Protocol Inspection Conditions and Options (continued)

Condition	Description
SIP Content Length	The SIP message body content length is used for SIP protocol inspection decisions. To specify SIP traffic based on SIP message body length: 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 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 12-33 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, do the following: 1. In the URI Type field, indicate the type of URI to be used: – 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. 2. In the URI Operator field, confirm that Greater Than is selected. 3. 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.

d. In the Action field, select the action that the virtual server is to take when the specified match conditions are met:

- Drop—The specified SIP traffic is to be discarded by the virtual server.
- Permit—The specified SIP traffic is to be received by the virtual server.
- Reset—The specified SIP traffic is to be denied by the virtual server.

e. Do the following:

- Click **OK** to save your entries. The Conditions table refreshes with the new entry.
- Click **Cancel** to exit the Conditions subset without saving your entries and to return to the Conditions table.

f. In the SIP 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 the "Shared Objects and Virtual Servers" section on page 5-9 for more information about modifying shared objects.

g. Configure SIP parameter map options using the information in Table 8-9.

h. 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 the "Shared Objects and Virtual Servers" section on page 5-9 for more information about modifying shared objects.

i. Configure secondary connection parameter map options using the information in Table 8-3.

j. 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:

- Drop—The specified SIP traffic is to be discarded by the virtual server.
- Permit—The specified SIP traffic is to be received by the virtual server.
- Reset—The specified SIP traffic is to be denied by the virtual server.

k. 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.

Step 9 When you finish configuring virtual server properties, do the following:

- Click **Deploy Now** to deploy this configuration on the ACE appliance.
- Click **Cancel** to exit this procedure without saving your entries.

Related Topics

- Configuring Virtual Server Properties, page 5-10
- Configuring Virtual Server SSL Termination, page 5-18
- Configuring Virtual Server Layer 7 Load Balancing, page 5-30

Configuring Virtual Server Layer 7 Load Balancing

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 the "Configuring Virtual Server Properties" section on page 5-10 for information on configuring these protocols.

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 SIP0

Procedure

Step 1 Select **Config** > **Virtual Contexts** > *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, and 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, and 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 the "Shared Objects and Virtual Servers" section on page 5-9 for more information about modifying shared objects.
- If you click ***New*** or ***Inline Match***, the Rule Match configuration subset appears.

Step 6 Configure match criteria by following the steps in Table 5-8.

Table 5-8 Layer 7 Load-Balancing Match Criteria Configuration

Selection	Action
Existing class map	1. Click **View** to review the match condition information for the selected class map. 2. Do the following: – Click **Cancel** to continue without making changes and to return to the previous screen. – Click **Edit** to modify the existing configuration. – Click **Duplicate** to create a new class map with the same attributes without affecting other virtual servers using the same class map. See the "Shared Objects and Virtual Servers" section on page 5-9 for more information about modifying shared objects.
New	1. In the Name field, enter a unique name for this class map. 2. In the Matches field, select the method to be used to evaluate multiple match statements when multiple match conditions exist: – Any—Indicates that a match exists if at least one of the match conditions is satisfied. – All—Indicates that 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, and then click **Edit** to modify it. 4. In the Type field, select the match condition and configure any protocol-specific options: – For Generic protocol options, see Table 12-8. – For HTTP and HTTPS protocol options, see Table 5-9. – For RADIUS protocol options, see Table 12-9. – For RTSP protocol options, see Table 12-10. – For SIP protocol options, see Table 12-11. 5. Configure any condition-specific options using the information in Table 5-9. 6. Do the following: – Click **OK** to accept your entries and to return to the Conditions table. – Click **Cancel** to exit this procedure without saving your entries and to return to the Conditions table.
Inline Match	In the Conditions Type field, select the type of inline match condition and configure any protocol-specific options: • For Generic protocol options, see Table 12-8 • For HTTP and HTTPS protocol options, see Table 5-9 • For RADIUS protocol options, see Table 12-9 • For RTSP protocol options, see Table 12-10 • For SIP protocol options, see Table 12-11

Table 5-9 Layer 7 HTTP/HTTPS Load-Balancing Rule Match Configuration

Match Condition	Description
Class Map	Indicates that this rule is to use an existing class map to establish match conditions. If you select this method, in the Class Map field, select the class map to be used. **Note** This option is not available for inline match conditions.
HTTP Content	Specific content contained within the HTTP entity-body is used to establish a match condition. **1.** In the Content Expression field, enter the content that is to be matched. Valid entries are alphanumeric strings from 1 to 255 characters. **2.** 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	Indicates that HTTP cookies are to be used for this rule. If you select this method: **1.** 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. **2.** 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 appliance supports regular expressions for matching string expressions. Table 12-33 lists the supported characters that you can use for matching string expressions. **3.** Check the Secondary Cookie Matching check box to indicate that the ACE appliance 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 appliance is to use either the cookie name or the cookie value to satisfy this match condition.
HTTP Header	Indicates that the HTTP header and a corresponding value are to be used for this rule. If you select this method: **1.** In the Header Name field, enter the name of the generic field in the HTTP header. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters. **2.** 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 appliance 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 12-33 lists the supported characters that you can use in regular expressions.

Table 5-9 Layer 7 HTTP/HTTPS Load-Balancing Rule Match Configuration (continued)

Match Condition	Description
HTTP URL	Indicates that this rule is to perform regular expression matching against the received packet data from a particular connections based on the HTTP URL string. If you select this method: 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 appliance supports regular expressions for matching URL strings. Table 12-33 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 64 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).

Table 5-9 Layer 7 HTTP/HTTPS Load-Balancing Rule Match Configuration (continued)

Match Condition	Description
Source Address	Indicates that this rule is to use a client source IP address to establish match conditions. If you select this method: 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 Netmask field, select the subnet mask to apply to the source IP address.
SSL	**Note** The SSL option does not apply to the ACE NPE software version (see the "Information About the ACE No Payload Encryption Software Version" section on page 1-2). Defines load balancing decisions based on the specific SSL cipher or cipher strength. Enables the ACE to load balance client traffic to different server farms based on the SSL encryption level negotiated with the ACE during SSL termination. If you select this method: 1. In the SSL Cipher Match Type field, select the match type. Options are as follows: – Equal To—Specifies an SSL cipher for the load balancing decision. – Less Than—Specifies SSL cipher strength for the load balancing decision. 2. If you selected Equal To, in the Cipher Name field specify an SSL cipher for the load balancing decision. The possible values are as follows: – RSA_EXPORT1024_WITH_DES_CBC_SHA – RSA_EXPORT1024_WITH_RC4_56_MD5 – RSA_EXPORT1024_WITH_RC4_56_SHA – RSA_EXPORT_WITH_DES40_CBC_SHA – RSA_EXPORT_WITH_RC4_40_MD5 – RSA_WITH_3DES_EDE_CBC_SHA – RSA_WITH_AES_128_CBC_SHA – RSA_WITH_AES_256_CBC_SHA – RSA_WITH_DES_CBC_SHA – RSA_WITH_RC4_128_MD5 – RSA_WITH_RC4_128_SHA 3. If you selected Less Than, in the Specify Minimum Cipher Strength field specify a non-inclusive minimum SSL cipher bit strength. For example, if you specify a cipher strength value of 128, any SSL cipher that was no greater than 128 would hit the traffic policy. If the SSL cipher was 128-bit or greater, the connection would miss the policy. The possible values are as follows: – 128—128-bit strength – 168—168-bit strength – 256—256-bit strength – 56—56-bit strength

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**—Indicates that client requests for content are to be discarded when match conditions are met. Continue with Step 10.
- **Forward**—Indicates that client requests for content are to be forwarded without performing load balancing on the requests when match conditions are met. Continue with Step 10.
- **Load Balance**—Indicates that 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 handled by a sticky group when match conditions are met. Continue with Step 8.

Step 8 If you select Load Balance as the primary action, you can configure load balancing using a server farm, a server farm/backup server farm pair, an existing sticky group, or a new sticky group.

If you select an existing object in any of these scenarios, you can view, modify, or duplicate the selected object's existing configuration. See the "Shared Objects and Virtual Servers" section on page 5-9 for more information about modifying shared objects in virtual servers.

Note To display statistics and status information for an existing server farm, choose a server farm in the list, and click **Details**. DM accesses the **show serverfarm** *name* **detail** CLI command to display detailed server farm information. See the "Displaying Server Farm Statistics and Status Information" section on page 6-39.

Configure load balancing using the information in Table 5-10.

Table 5-10 Virtual Server Load-Balancing Options

To configure...	Do this...
Load balancing using a server farm	In the Server Farm field, select the server farm[1] to be used for load balancing for this virtual server, or select ***New*** to configure a new server farm (see Table 5-11).
Load balancing using a server farm/backup server farm pair	1. In the Server Farm field, select the primary server farm[1] to use for load balancing, or select ***New*** to configure a new server farm (see Table 5-11). 2. In the Backup Server Farm field, select the server farm[1] 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 5-11).

Table 5-10 Virtual Server Load-Balancing Options (continued)

To configure...	Do this...
Load balancing using an existing sticky group	**1.** In the Server Farm field, select the primary server farm[1] to use for load balancing. This must be the primary server farm specified in the existing sticky group. **2.** In the Backup Server Farm field, select the backup server farm[1] to use for load balancing. This must be the backup server farm specified in the existing sticky group. **3.** In the Sticky Group field, select the sticky group to use. **Note** Sticky groups appear in the Sticky Group field **only** when their configured primary and backup server farms are selected, respectively. If you select a sticky group and then select a different primary or backup server farm, the sticky group that you selected in the Sticky Group field no longer appears. To change an existing sticky group configuration, modify it in the Stickiness configuration screen (**Config** > **Virtual Contexts** > *context* > **Load Balancing** > **Stickiness**).
Load balancing using a new sticky group	**1.** In the Server Farm field, select the primary server farm[1] to use for load balancing, or select ***New*** to configure a new server farm (see Table 5-11). **2.** In the Backup Server Farm field, select the server farm[1] 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 5-11). **3.** In the Sticky Group field, select ***New***, and then configure a new sticky group using the information in Table 5-13. **Note** The context in which you configure a sticky group must be associated with a resource class that allocates a portion of ACE appliance resources to stickiness. See the "Managing Resource Classes" section on page 4-35 for more information on resource classes.

1. When you select an existing server farm, you can do the following using the function buttons that appear:

- Click **View** to display the server farm configuration, which you can then edit or duplicate using the functions buttons that appear.
- Click **Details** to display the **show serverfarm** *sf_name* **detail** command output in a pop-up window. This command output provides server farm configuration information.
- Click **Buddy Group** to display the **show buddy group** command output in a pop-up window. This command output shows the list of buddy groups that are configured in the virtual context (for more information, see the "Buddy Sticky Groups" section on page 7-6).

Table 5-11 New Server Farm Attributes

Field	Description
Name	Enter a unique name for this server farm. Valid entries are unquoted text strings with no spaces and a maximum of 64 characters.
Type	Select the type of server farm: • 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. **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	Select the action the ACE appliance is to take with respect to connections if any real server in the server farm fails: • N/A—Indicates that the ACE appliance is to take no action if any server in the server farm fails. • Purge—Indicates that the ACE appliance is to remove connections to a real server if that real server in the server farm fails. The ACE appliance 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.

Table 5-11 New Server Farm Attributes (continued)

Field	Description
Failaction Reassign Across Vlans	This field appears only when the L7 Load-Balancing Action parameters are set as follows: Primary Action: LoadBalance, ServerFarm: New, Fail Action: Reassign. Check the check box to specify that the ACE reassigns the existing server connections to the backup real server on a different VLAN interface (commonly referred to as a bypass VLAN) if the real server fails. If a backup real server has not been configured for the failing server, this option has no effect and leaves the existing connections untouched in the failing real server. Note the following configuration requirements and restrictions when you enable this option: • Enable the Transparent option (see the next Field) to instruct the ACE not to use NAT to translate the ACE VIP address to the server IP address. The Failaction Reassign Across Vlans option is intended for use in stateful firewall load balancing (FWLB) on your ACE, where the destination IP address for the connection coming in to the ACE is for the end-point real server, and the ACE reassigns the connection so that it is transmitted through a different next hop. • Enable the MAC Sticky option on all server-side interfaces to ensure that packets that are going to and coming from the same server in a flow will traverse the same firewalls or stateful devices (see the "Configuring Virtual Context VLAN Interfaces" section on page 10-10). • Configure the Predictor Hash Address option. See Table 5-12 for the supported predictor methods and configurable attributes for each predictor method. • You must configure identical policies on the primary interface and the backup-server interface. The backup interface must have the same feature configurations as the primary interface. • If you configure a policy on the backup-server interface that is different from the policies on the primary-server interface, that policy will be effective only for new connections. The reassigned connection will always have only the primary-server interface policies. • Interface-specific features (for example, NAT, application protocol inspection, outbound ACLs, or SYN cookie) are not supported. • You cannot reassign connections to the failed real server after it comes back up. This restriction also applies to same-VLAN backup servers. • Real servers must be directly connected to the ACE. This requirement also applies to same-VLAN backup server. • You must disable sequence number randomization on the firewall (see the "Configuring Connection Parameter Maps" section on page 8-5). • Probe configurations should be similar on both ACEs and the interval values should be low. For example, if you configure a high interval value on ACE-1 and a low interval value on ACE-2, the reassigned connections may become stuck because of the probe configuration mismatch. ACE-2 with the low interval value will detect the primary server failure first and will reassign all its incoming connections to the backup-server interface VLAN. ACE-1 with the high interval value may not detect the failure before the primary server comes back up and will still point to the primary server. To minimize packet loss, we recommend the following probe parameter values on both ACEs: Interval: 2, Faildetect: 2, Passdetect interval: 2, and Passdetect count: 5.

Table 5-11 New Server Farm Attributes (continued)

Field	Description
Transparent	This field appears only for real servers identified as host servers. Check the check box to specify that network address translation from the VIP address to the server IP is to occur. Clear the check box to indicates that network address translation from the VIP address to the server IP address is not to occur (default).
Dynamic Workload Scaling	This field appears only for host server farms. Allows the ACE to burst traffic to remote VMs when the average CPU usage, memory usage, or both of the local VMs has reached its specified maximum threshold value. The ACE stops bursting traffic to the remote VMs when the average CPU or memory usage of the local VMs has dropped to its specified minimum threshold value. This option requires that you have the ACE configured for Dynamic Workload Scaling using a Nexus 7000, VM Controller, and VM probe (see the "Configuring Dynamic Workload Scaling" section on page 6-14). Click one of the following radio button options: • N/A—Not applicable (default). • Local—The ACE can use the VM Controller local VMs only for load balancing (bursting is not allowed). • Burst—Enables the ACE to burst traffic to a remote VM Controller VMs. When you choose Burst, the VM Probe Name field appears along with a list of available VM probes. Choose an available VM probe or click **Add** to display the Health Monitoring pop-up window and create a new VM probe or edit an existing one (see the "Configuring Health Monitoring" section on page 6-39).
Fail-On-All	This field appears only for host server farms. 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. 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. Check this check box to configure the real servers in a server farm to use AND logic with respect to multiple server farm probes. The Fail On All function is applicable to all probe types.

Table 5-11 New Server Farm Attributes (continued)

Field	Description
Inband-Health Check	This field appears only for host server farms. By default, the ACE monitors the health of all real servers in a configuration through the use of ARPs and health probes. However, there is latency period between when the real server goes down and when the ACE becomes aware of the state. The inband health monitoring feature allows the ACE to monitor the health of the real servers in the server farm through the following connection failures: • For TCP, resets (RSTs) from the server or SYN timeouts. • For UDP, ICMP Host, Network, Port, Protocol, and Source Route unreachable messages. When you configure the failure-count threshold and the number of these failures exceeds the threshold within the reset-time interval, the ACE immediately marks the server as failed, takes it out of service, and removes it from load balancing. The server is not considered for load balancing until the optional resume-service interval expires. Choose one of the following: • Count—Tracks the total number of TCP or UDP failures, and increments the counters as displayed by the s**how serverfarm** *name* **inband** CLI command. • Log—Logs a syslog error message when the number of events reaches the configured connection failure threshold. • Remove—Logs a syslog error message when the number of events reaches the threshold and removes the server from service. **Note** You can configure this feature and health probes to monitor a server. When you do, both are required to keep a real server in service within a server farm. If either feature detects a server is out of service, the ACE does not select the server for load balancing.
Connection Failure Threshold Count	This field appears only when the Inband-Health Check is set to Log or Remove. Enter the maximum number of connection failures that a real server can exhibit in the reset-time interval before ACE marks the real server as failed. Valid entries are integers from 1 to 4294967295.
Reset Timeout (Milliseconds)	This field appears only when the Inband-Health Check is set to Log or Remove. Enter the number of milliseconds for the reset-time interval. Valid entries are integers from 100 to 300000. The default interval is 100. This interval starts when the ACE detects a connection failure. If the connection failure threshold is reached during this interval, the ACE generates a syslog message. When the Inband-Health Check is set to Remove, the ACE also removes the real server from service. Changing the setting of this option affects the behavior of the real server, as follows: • When the real server is in the OPERATIONAL state, even if several connection failures have occurred, the new reset-time interval takes effect the next time that a connection error occurs. • When the real server in the INBAND-HM-FAILED state, the new reset-time interval takes effect the next time that a connection error occurs after the server transitions to the OPERATIONAL state.

Table 5-11 New Server Farm Attributes (continued)

Field	Description
Resume Service (Seconds)	This field appears only when the Inband-Health Check is set to Remove. Enter the number of seconds after a server has been marked as failed to reconsider it for sending live connections. Valid entries are integers from 30 to 3600. The default setting is 0. The setting of this option affects the behavior of the real server in the inband failed state, as follows: • When this field is not configured and has the default setting of 0, the real server remains in the failed state until you manually suspend and then reactivate it. • When this field is not configured and has the default setting of 0 and then you configure this option with an integer between 30 and 3,600, the failed real server immediately transitions to the Operational state. • When you configure this field and then increase the value, the real server remains in the failed state for the duration of the previously-configured value. The new value takes effect the next time the real server transitions to the failed state. • When you configure this field and then decrease the value, the failed real server immediately transitions to the Operational state. • When you configure this field with an integer between 30 and 3,600 and then reset it to the default of 0, the real server remains in the failed state for the duration of the previously-configured value. The default setting takes effect the next time the real server transitions to the failed state. Then the real server remains in the failed state until you manually suspend and then reactivate it. • When you change this field within the reset-time interval and the real server is in the OPERATIONAL state with several connection failures, the new threshold interval takes effect the next time that a connection error occurs, even if it occurs within the current reset-time interval.
Predictor	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. See Table 5-12 for the supported predictor methods and configurable attributes for each predictor method.

Table 5-11 New Server Farm Attributes (continued)

Field	Description
Probes	Specify the health monitoring probes to use: • To include a probe that you want to use for health monitoring, select it in the Available list, and then click **Add**. The probe appears in the Selected list. The redirect real server probe list contains only configured probes of the type Is Routed, which means that the ACE routes the probe address according to the ACE internal routing table (see the "Configuring Health Monitoring for Real Servers" section on page 6-41). **Note** You can associate both IPv6 and IPv4 probes to a server farm. **Note** The list of available probes does not include VM health monitoring probes. To choose a VM probe for monitoring local VM usage, see the Dynamic Workload Scaling field. • To remove a probe that you do not want to use for health monitoring, select it in the Selected list, and then click **Remove**. The probe appears in the Available list. • To specify a sequence for probe use, select probes in the Selected list, and 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, and then click **View**. • To display statistics and status information for an existing probe, choose a probe in the list on the right, and click **Details**. DM accesses the **show probe** *name* **detail** CLI command to display detailed probe information. See the "Displaying Health Monitoring Statistics and Status Information" section on page 6-69. To add a new probe, click **Create**. See the "Configuring Health Monitoring for Real Servers" section on page 6-41 for details on adding a new health monitoring probe and defining attributes for the specific probe type. In addition, set the following probe configuration parameters in the Probes section under Server Farm: • Expect Addresses—To configure expect addresses for a DNS probe in Expect Addresses configuration screen, in the IPv4/IPv6 Address field, enter the IP address that the ACE appliance expects as a server response to a DNS request. You can enter multiple addresses in this field. However, you cannot mix IPv4 and IPv6 addresses. • 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 *header_name=header_value* where: – *header_name* 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. – *header_value* 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.

Table 5-11 New Server Farm Attributes (continued)

Field	Description
Probes (Cont.)	• 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: – 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 the "Configuring an OID for SNMP Probes" section on page 6-68. 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 the "Configuring Health Monitoring for Real Servers" section on page 6-41. You can also delete an existing health probe from the Health Monitoring table.

Table 5-11 New Server Farm Attributes (continued)

Field	Description
Real Servers	The Real Servers table allows you to add, modify, remove, or change the order of real servers. **1.** Select an existing server, or click **Add** to add a real server to the server farm: – If you select an existing server, you can view, modify, or duplicate the server's existing configuration. See the "Shared Objects and Virtual Servers" section on page 5-9 for more information about modifying shared objects. – If you click **Add**, the table refreshes and allows you to enter server information. **2.** For the IP Address Type, select either IPv6 or IPv4. **3.** In the IP Address field, enter the IP address. **4.** In the Name field, enter the name of the real server. **5.** In the Port field, enter the port number to be used for server port address translation (PAT). Valid entries are integers from 1to 65535. **6.** 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. **7.** In the Redirection Code field, select the appropriate redirection code. This field appears only for real servers identified as redirect servers. – 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. **8.** 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 http://host.com:port 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. The relocation string supports the following special characters: – %h—Inserts the hostname from the request Host header – %p—Inserts the URL path string from the request **9.** In the Rate Bandwidth, field, specify the real server bandwidth limit in bytes per second. Valid entries are integers from 1 to 300000000. **10.** In the Rate Connection field, specify the limit for connections per second. Valid entries are integers from 1 to 350000. **11.** In the State field, select the administrative state of this server: – 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 is to remain 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.

Table 5-11 New Server Farm Attributes (continued)

Field	Description
Real Servers (continued)	**12.** In the Buddy Real Group field, associate the real server with a buddy group by creating a buddy real server group or select an existing one (for more information, see the "Buddy Sticky Groups" section on page 7-6). **13.** In the Fail-On-All field, check this check box 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. **14.** In the Cookie String field, enter a cookie string value of the real server, which is to be used for HTTP cookie insertion when establishing a sticky connection. Valid entries are text strings with a maximum of 32 alphanumeric characters. You can include spaces and special characters in a cookie string value. See Chapter 7, "Configuring Stickiness" for details on HTTP cookie sticky connections. Cookie String is applicable only for host real servers **15.** Do the following: – Click **OK** to accept your entries and add this real server to the server farm. The table refreshes with updated information. – Click **Cancel** to exit this procedure without saving your entries and to return to the Real Servers table. To display statistics and status information for an existing real server, choose a real server in the list, and then click **Details**. DM accesses the **show rserver** *name* **detail** CLI command to display detailed real server information. See the "Displaying Real Server Statistics and Status Information" section on page 6-8.

Table 5-12 Predictor Methods and Attributes

Predictor Method	Description / Action
Hash Address	The ACE selects the server using a hash value based on the source or destination IP address. To configure the hash address predictor method: **1.** In the Mask Type field, indicate whether server selection is based on the source IP address or the destination IP address: – N/A—Indicates that this option is not defined. – Destination—Indicates that the server is selected based on the destination IP address. – Source—Indicates that the server is selected based on the source 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.
Hash Content	The ACE selects the server by using a hash value based on the specified content string of the HTTP packet body. **1.** 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 12-33 lists the supported characters that you can use for matching string expressions. **2.** 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 12-33 lists the supported characters that you can use for matching string expressions. **3.** 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. You cannot specify both the length and the end-pattern options for a Hash Content predictor. **4.** 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	The ACE selects the server by using a hash value based on the cookie name. 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.

Table 5-12 Predictor Methods and Attributes (continued)

Predictor Method	Description / Action
Hash Secondary Cookie	The ACE selects the server by using the hash value based on the specified cookie name in the URL query string, not the cookie header. 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.
Hash Header	The ACE selects the server by using a hash value based on the header name. In the Header Name field, select the HTTP header to be used for server selection: • 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, and then select one of the HTTP headers from the list.
Hash Layer 4	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. **1.** 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. 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 12-33 lists the supported characters that you can use for matching string expressions. **2.** 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 12-33 lists the supported characters that you can use for matching string expressions. **3.** 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. 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. You cannot specify both the length and end-pattern options for a Hash Layer 4 predictor. **4.** 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.

Table 5-12 Predictor Methods and Attributes (continued)

Predictor Method	Description / Action
Hash URL	The ACE selects the server by using a hash value based on the URL. Use this method to load balance firewalls. Enter values in one or both of the pattern fields: • 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. Valid entries for these fields are unquoted text strings with no spaces and a maximum of 255 alphanumeric characters for each pattern you configure.
Least Bandwidth	The ACE selects the server with the least amount of network traffic over a specified sampling period. **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	The ACE selects the server with the fewest number of connections. 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. The slow-start mechanism is used to avoid sending a high rate of new connections to servers that you have just put into service.
Least Loaded	The ACE selects the server with the lowest load based on information from SNMP probes. **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 instruct the ACE to apply the maximum load of 16000 to a real server whose load reaches zero or override the default behavior. By default, the ACE applies the average load of the server farm to a real server whose load is zero. The ACE periodically adjusts this load value based on feedback from the server's SNMP probe and other configured options. Options are as follows: – Average—Applies the average load of the server farm to a real server whose load is zero. This setting allows the server to participate in load balancing, while preventing it from being flooded by new connections. This is the default setting. – Maxload—Instruct the ACE to apply the maximum load of 16000 to a real server whose load reaches zero. – Off—Instruct the ACE to send 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. If two servers have the same lowest load (either zero or nonzero), the ACE load balances the connections between the two servers in a round-robin manner. **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 5-12 Predictor Methods and Attributes (continued)

Predictor Method	Description / Action
Response	The ACE selects the server with the lowest response time for a requested response-time measurement. **1.** In the Response Type field, select the type of measurement to use: – 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	The ACE selects the next server in the list of servers based on server weight. This is the default predictor method.

Table 5-13 Sticky Group Attributes

Field	Description
Group Name	Enter a unique identifier for the sticky type. 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	Select the method to be used when establishing sticky connections: • 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 7-2 for additional configuration options. • HTTP Cookie—Indicates that 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. • HTTP Header—Indicates that the virtual server is to stick client connections to the same real server based on HTTP headers. • IP Netmask—Indicates that 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 IPv4 address, the destination IPv4 address, or both. **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. • V6 Prefix—Indicates that 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 IPv6 address, the destination IPv6 address, or both. • 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 7-6 for additional configuration options. • RADIUS—The virtual server is to stick client connections to the same real server based on a RADIUS attribute. See Table 7-7 for additional configuration options. • RTSP Header—The virtual server is to stick client connections to the same real server based on the RTSP Session header field. Table 7-8 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.
Cookie Name	This option appears for sticky type HTTP Cookie. Enter a unique identifier for the cookie. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters.

Table 5-13 Sticky Group Attributes (continued)

Field	Description
Enable Insert	This option appears for sticky type HTTP Cookie. Check this check box if the virtual server is to insert a cookie in the Set-Cookie header of the response from the server to the client. This option is useful when you want to use a session cookie for persistence but the server is not currently setting the appropriate cookie. When selected, the virtual server selects a cookie value that identifies the original server from which the client received a response. For subsequent connections of the same transaction, the client uses the cookie to stick to the same server. Clear this check box to disable cookie insertion.
Browser Expire	This option appears for sticky type HTTP Cookie and you select Enable Insert. Check this check box to allow the client's browser to expire a cookie when the session ends. Clear this check box to disable browser expire.
Offset (Bytes)	This option appears for sticky types HTTP Cookie and HTTP Header. Enter the number of bytes the virtual server is to ignore starting with the first byte of the cookie. Valid entries are integers from 0 to 999. The default is 0 (zero), which indicates that the virtual server does not exclude any portion of the cookie.
Length (Bytes)	This option appears for sticky types HTTP Cookie and HTTP Header. Enter the length of the portion of the cookie (starting with the byte after the offset value) that the ACE appliance is to use for sticking the client to the server. Valid entries are integers from 1 to 1000.
Secondary Name	This option appears for sticky type HTTP Cookie. Enter an alternate cookie name that is to appear in the URL string of the Web page on the server. The virtual server uses this cookie to maintain a sticky connection between a client and a server and adds a secondary entry in the sticky table. Valid entries are unquoted text strings with no spaces and a maximum of 64 characters.
Header Name	This option appears for sticky type HTTP Header. Select the HTTP header to use for sticking client connections.
Netmask	This field appears for sticky type IP Netmask. This field is optional for the sticky type V6 Prefix. Select the netmask to apply to the source IPv4 address, destination IPv4 address, or both.
Prefix Length	This field appears for sticky type V6 Prefix. This field is optional for the sticky type IP Netmask. Enter the prefix length to apply to the source IPv6 address, destination IPv6 address, or both.
Address Type	This field appears for sticky type IP Netmask. Indicate whether this sticky type is to be applied to the client source IP address, the destination IP address, or both: • Both—Indicates that this sticky type is to be applied to both the source IP address and the destination IP address. • Destination—Indicates that this sticky type is to be applied to the destination IP address only. • Source—Indicates that this sticky type is to be applied to the source IP address only.
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 5-11.

Table 5-13 Sticky Group Attributes (continued)

Field	Description
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 5-11.
Aggregate State	Check this 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 appliance 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. Clear this 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.
Enable Sticky On Backup Server Farm	Check this check box to specify that the backup server farm is sticky. Clear this check box if the backup server farm is not sticky.
Buddy Group	Associate the serverfarm with a buddy member group by creating a buddy sticky group or selecting an existing one (for more information, see the "Buddy Sticky Groups" section on page 7-6).
Replicate On HA Peer	Check this 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 this 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 this 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 this 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 9 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 ACE 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 *Administration Guide, Cisco ACE Application Control Engine* for information on ACE licensing options.

Options are as follows:

- 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 configuring HTTP compression, we recommend that you exclude the following MIME types from HTTP compression: ".*gif", ".*css", ".*js", ".*class", ".*jar", ".*cab", ".*txt", ".*ps", ".*vbs", ".*xsl", ".*xml", ".*pdf", ".*swf", ".*jpg", ".*jpeg", ".*jpe", or ".*png".

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 10 In the SSL Initiation field, select an existing service, or select ***New*** to create a new service.

Note The SSL Initiation field appears only in the Advanced View, and when TCP is the selected protocol and Other, HTTP, or HTTPS is the application protocol.

Note The SSL initiation option does not apply to the ACE NPE software version (see the "Information About the ACE No Payload Encryption Software Version" section on page 1-2).

SSL initiation allows the virtual server to act as an SSL proxy client to initiate and maintain an SSL connection between itself and an SSL server. In this particular application, the ACE receives clear text from an HTTP client, and encrypts and transmits the data as ciphertext to the SSL server. On the reverse side, the ACE decrypts the ciphertext that it receives from the SSL server and sends the data to the client as clear text.

- If you select an existing SSL service, you can view, modify, or duplicate the existing configuration. See the "Shared Objects and Virtual Servers" section on page 5-9 for more information about modifying shared objects.
- If you select ***New***, configure the service using the information in Table 5-14.

Table 5-14 Virtual Server SSL Initiation 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.
CRL Best-Effort	This option appears if you select an authentication group in the Auth Group Name field. Check the check box to allow the ACE 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.

Table 5-14 Virtual Server SSL Initiation Attributes

Field	Description
CRL Name	This option appears if the CRL Best-Effort check box is clear. Select the Certificate Revocation List if the ACE is to use for this proxy service.
Parameter Maps	Select the SSL parameter map to associate with this proxy server service.

For more information about SSL, see the "Configuring SSL" section on page 9-1.

Step 11 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 appliance 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 12-33 lists the supported characters that you can use in regular expressions.

For example, you might enter `Host=www.cisco.com`.

Step 12 Do the following:

- Click **OK** to save your entries and to return to the Rule Match table.
- Click **Cancel** to exit this procedure without saving your entries and to return to the Rule Match table.

Step 13 If you are adding Rule Match entries for a new virtual server and you want to modify the sequence of rules in the L7 Load Balancing section of the Virtual Server configuration page, click **Up** or **Down** to change the order of the entries in the Rule Match table.

Note The Up and Down buttons are not available for an existing virtual server, only for a new virtual server. To reorder the entries in the Rule Match table for an existing virtual server, go to Config > Expert > Policy Maps and choose the Layer 7 load balancing policy map, delete the rule entry that you want to reorder, and then add it again by using the Insert Before option to put it in the correct order. See the "Configuring Rules and Actions for Policy Maps" section on page 12-36 for details.

Step 14 When you finish configuring virtual server properties, do the following:

- Click **Deploy Now** to deploy this configuration on the ACE appliance.
- Click **Cancel** to exit this procedure without saving your entries.

Related Topics

- Configuring Virtual Servers, page 5-2
- Configuring Virtual Server Properties, page 5-10
- Configuring Virtual Server SSL Termination, page 5-18

- Configuring Virtual Server Protocol Inspection, page 5-20

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 the "Configuring Virtual Servers" section on page 5-2 for information on configuring a virtual server.

Procedure

Step 1 Select **Config** > **Virtual Contexts** > *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, and 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**—Indicates that client requests that do not meet specified match conditions are to be discarded. Continue with Step 7.
- **Forward**—Indicates that client requests that do not meet specified match conditions are to be forwarded without performing load balancing on the requests. Continue with Step 7.
- **Load Balance**—Indicates that client requests for content are to be directed to a server farm. If you select Load Balance, server farm, backup server farm, and sticky configuration options appear. Continue with Step 5.
- **Sticky**—Client requests for content are handled by a sticky group when match conditions are met. Continue with Step 6.

Step 5 If you select Load Balance as the primary action, you can configure load balancing using a server farm, a server farm/backup server farm pair, an existing sticky group, or a new sticky group.

Note If you select an existing object in any of these scenarios, you can view, modify, or duplicate the selected object's existing configuration. See the "Shared Objects and Virtual Servers" section on page 5-9 for more information about modifying shared objects in virtual servers.

Configure load-balancing using the information in Table 5-10.

Step 6 (Optional) If you chose Sticky as the primary action, in the Sticky Group field, choose an existing sticky group or click ***New*** to add a new sticky group (see Table 5-13).

Note To display statistics and status information for an existing server farm, choose a server farm in the list, and then click **Details**. DM accesses the **show serverfarm** *name* **detail** CLI command to display detailed server farm information. See the "Displaying Server Farm Statistics and Status Information" section on page 6-39.

Note If you chose an existing sticky group, you can view, modify, or duplicate the selected object's existing configuration. See the "Shared Objects and Virtual Servers" section on page 5-9 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 ACE 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 *Administration Guide, Cisco ACE Application Control Engine* for information on ACE licensing options.

Options are as follows:

- 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 configuring HTTP compression, we recommend that you exclude the following MIME types from HTTP compression: ".*gif", ".*css", ".*js", ".*class", ".*jar", ".*cab", ".*txt", ".*ps", ".*vbs", ".*xsl", ".*xml", ".*pdf", ".*swf", ".*jpg", ".*jpeg", ".*jpe", or ".*png".

Note If you enable the Gzip or Deflate compression format, the DM GUI automatically inserts a L7 Load Balance Primary Action to exclude the MIME types listed above. However, if you disable HTTP compression later on, you will need to remove the auto-inserted Load Balance Primary Action.

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.

Note The SSL Initiation field appears only in the Advanced View, and when TCP is the selected protocol and Other, HTTP, or HTTPS is the application protocol.

Note The SSL initiation option does not apply to the ACE NPE software version (see the "Information About the ACE No Payload Encryption Software Version" section on page 1-2).

SSL initiation allows the virtual server to act as an SSL proxy client to initiate and maintain an SSL connection between itself and an SSL server. In this particular application, the ACE receives clear text from an HTTP client, and encrypts and transmits the data as ciphertext to the SSL server. On the reverse side, the ACE decrypts the ciphertext that it receives from the SSL server and sends the data to the client as clear text.

- If you select an existing SSL service, you can view, modify, or duplicate the existing configuration. See the "Shared Objects and Virtual Servers" section on page 5-9 for more information about modifying shared objects.
- If you select ***New***, configure the service using the information in Table 5-14.

For more information about SSL, see the "Configuring SSL" section on page 9-1.

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 appliance 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 12-33 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, do the following:

- Click **Deploy Now** to deploy this configuration on the ACE appliance.
- Click **Cancel** to exit this procedure without saving your entries and to return to the Virtual Servers table.

Related Topics

- Configuring Virtual Server Properties, page 5-10
- Configuring Virtual Server SSL Termination, page 5-18
- Configuring Virtual Server Protocol Inspection, page 5-20
- Configuring Virtual Server Layer 7 Load Balancing, page 5-30

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. The application acceleration functionality in

the ACE appliance enables enterprises to optimize network performance and improve access to critical business information. This capability accelerates the performance of Web applications, including customer relationship management (CRM), portals, and online collaboration by up to 10 times.

See the "Configuring Application Acceleration and Optimization" section on page 13-1 or the *Application Acceleration and Optimization Guide, Cisco ACE 4700 Series Application Control Engine Appliance* for more information about application acceleration and optimization.

Use this procedure to configure acceleration and optimization on virtual servers.

Assumption

A virtual server has been configured. See the "Configuring Virtual Servers" section on page 5-2 for information on configuring a virtual server.

Consideration

Application acceleration and optimization is only supported in IPv4 to IPv4 server load-balancing configurations.

Procedure

Step 1 Select **Config > Virtual Contexts >** *context* **> Load Balancing > Virtual Servers**. The Virtual Servers table appears.

Step 2 Select the virtual server you want to configure for optimization, and 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—Indicates that you want to use standard acceleration and optimization options. Continue with Step 5.
- Custom—Indicates that you want to associate specific match criteria, actions, and parameter maps for application acceleration and optimization for this virtual server. If you choose this option, continue with Step 6.

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 this 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 the "Optimization Overview" section on page 13-2.

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 this 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 Delta optimization, see the "Optimization Overview" section on page 13-2 and the "Configuring an HTTP Optimization Action List" section on page 13-3.

c. Continue with Step 11.

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, and then click **Edit** to modify it. The configuration subset refreshes with the available configuration options.

Step 7 In the Apply Template field, select one of the configuration templates for the type of optimization you want to configure, or leave blank to configure optimization without a template:

- 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 do not select a template and select ***New*** in the Rule Match and Actions fields, you are creating your own optimization rules and actions.

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 the "Shared Objects and Virtual Servers" section on page 5-9 for more information about modifying shared objects.
- If you click ***New***, the screen refreshes with the default configuration settings for the template you selected. You can accept the default settings or modify them using the information in Table 5-15.

Table 5-15 Optimization Rule Match Configuration Options

Field	Description
Name	Enter a unique name for this match criteria rule.
Matches	Select the method to be used to evaluate multiple match statements when multiple match conditions exist: • 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.
Conditions	Click **Add** to add a new set of conditions or select an existing entry, and then click **Edit** to modify it: 1. In the Type field, select the match condition to be used, and then configure any condition-specific options using the information in Table 5-9. 2. Click **OK** to save your entries, or **Cancel** to exit this procedure without saving your entries.

Step 9 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 optimization action list, you can view, modify, or duplicate the existing configuration. See the "Shared Objects and Virtual Servers" section on page 5-9 for more information about modifying shared objects.
- If you click ***New***, the screen refreshes with the default configuration settings for the template you selected. You can accept the default settings or modify them using the information in Table 5-16.

Table 5-16 Optimization Action List Configuration Options

Field	Description
Action List Name	Enter a unique name for the optimization 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 delta optimization for the specified URLs. **Note** The ACE restricts you from enabling delta optimization if you have previously specified either Cache Dynamic or Dynamic Entity Tag.
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 AppScope performance monitoring for use with the ACE appliance.
Flash Forward	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. Specify how the ACE appliance is to implement FlashForward: • N/A—Indicates that this feature is not enabled. • Flash Forward—Indicates that FlashForward is to be enabled for the specified URLs and that embedded objects are to be transformed. • Flash Forward Object—Indicates that 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.
Cache Dynamic	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. Clear this check box to disable this feature. **Note** The ACE restricts you from enabling Cache Dynamic if you have previously specified either Enable Delta or Dynamic Entity Tag.
Cache Forward	Check this check box to enables the cache forward feature for the corresponding URLs. Cache forward allows the ACE to serve the object from its cache (static or dynamic) even when the object has expired if the maximum cache TTL time period has not yet expired (set by specifying the Cache Time-To-Live Duration (%): field in an Optimization parameter map). At the same time, the ACE sends an asynchronous request to the origin server to refresh its cache of the object. Clear this check box to disable this feature.

Table 5-16 Optimization Action List Configuration Options (continued)

Field	Description
Dynamic Entity Tag	This feature enables the acceleration of noncacheable embedded objects, which results in improved application response time. When enabled, this feature eliminates the need for users to download noncacheable objects on each request. Check this check box to indicate that the ACE appliance is to implement just-in-time object acceleration for noncacheable embedded objects. Clear this check box to disable this feature. **Note** The ACE restricts you from enabling Dynamic Entity Tag if you have previously specified either Enable Delta or Cache Dynamic.
Fine Tune Optimization Parameters	Click this header to configure additional optimization attributes. When expanded, the configuration pane displays options specific to the type of optimization you are configuring and features that you enable. Refer to Table 8-5 for information about specific options that appear.

Step 10 When you finish configuring match criteria and actions, do the following:

- Click **OK** to save your entries and to return to the Rule Match and Actions table.
- Click **Cancel** to exit this procedure without saving your entries and to return to the Rule Match and Actions table.

Step 11 When you finish configuring virtual server properties, do the following:

- Click **Deploy Now** to save your entries. The ACE appliance validates the optimization action list configuration and deploys it on the ACE appliance.
- Click **Cancel** to exit this procedure without saving your entries and to return to the Virtual Servers table.

Related Topics

- Configuring Virtual Server Properties, page 5-10
- Optimization Traffic Policies and Typical Configuration Flow, page 13-2
- Configuring Traffic Policies for HTTP Optimization, page 13-6
- Configuring Virtual Server Protocol Inspection, page 5-20
- Configuring Virtual Server Layer 7 Load Balancing, page 5-30
- Configuring Virtual Server Default Layer 7 Load Balancing, page 5-55

Configuring Virtual Server NAT

Use this procedure to configure Name Address Translation (NAT) for virtual servers.

Assumptions

- A virtual server has been configured. See the "Configuring Virtual Servers" section on page 5-2 for information on configuring a virtual server.

- A VLAN has been configured. See the "Configuring Virtual Context VLAN Interfaces" section on page 10-10 for information on configuring a VLAN interface.
- At least one NAT pool has been configured on a VLAN interface. See the "Configuring VLAN Interface NAT Pools and Displaying NAT Utilization" section on page 10-32 for information on configuring a NAT pool.

Procedure

Step 1 Select **Config** > **Virtual Contexts** > *context* > **Load Balancing** > **Virtual Servers**. The Virtual Servers table appears.

Step 2 Select the virtual server you want to configure for NAT, and 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, and 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 the "Configuring VLAN Interface NAT Pools and Displaying NAT Utilization" section on page 10-32.

Step 6 In the NAT Pool ID field, select the NAT pool that you want to associate with the selected VLAN.

Step 7 Do the following:

- Click **OK** to save your entries and to return to the NAT table. The NAT table refreshes with the new entry.
- Click **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, do the following:

- Click **Deploy Now** to deploy this configuration on the ACE appliance.
- Click **Cancel** to exit this procedure without saving your entries and to return to the Virtual Servers table.

Related Topics

- Configuring Virtual Servers, page 5-2
- Configuring Virtual Server Properties, page 5-10
- Configuring Virtual Server SSL Termination, page 5-18
- Configuring Virtual Server Protocol Inspection, page 5-20
- Configuring Virtual Server Layer 7 Load Balancing, page 5-30
- Configuring Virtual Server Default Layer 7 Load Balancing, page 5-55

Displaying Virtual Server Statistics and Status Information

You can display virtual server statistics and status information for a particular virtual server by using the **Details** button.

Procedure

Step 1 Choose **Config** > **Virtual Contexts** > *context* > **Load Balancing** > **Virtual Servers**.

The Virtual Servers table appears.

Step 2 In the Virtual Servers table, choose a virtual server from the Virtual Servers table, and click **Details**.

The **show service-policy** *policy_name* **class-map** *class_name* **detail** CLI command output appears. For details about the displayed fields, see the *Server Load-Balancing Guide, Cisco ACE Application Control Engine*.

Note This feature requires ACE software Version A3(2.1) or later. An error displays with earlier software versions.

Step 3 (Optional) Click **Update Details** to refresh the window information.

Step 4 Click **Close** to return to the Virtual Servers table.

Related Topics

- Configuring Virtual Servers, page 5-2
- Managing Virtual Servers, page 5-63
- Viewing All Virtual Servers, page 5-65

Managing Virtual Servers

After you have created a virtual server the following options are available:

Task	Related Topics
Modify a virtual server configuration	Configuring Virtual Servers, page 5-2
List virtual servers by virtual context	Viewing Virtual Servers by Context, page 5-63
Activate a virtual server	Activating Virtual Servers, page 5-64
Suspend a virtual server	Suspending Virtual Servers, page 5-65
View all virtual servers and its configured state	Viewing All Virtual Servers, page 5-65

Viewing Virtual Servers by Context

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

Procedure

Step 1 Select **Config > Virtual Contexts**. The All Virtual Contexts table appears.

Step 2 Select the context associated with the virtual servers you want to view, and then select **Load Balancing > Virtual Servers**. The Virtual Servers table appears with the following information:

- Virtual server name
- Configured state, such as Inservice
- Virtual IP address

- Port
- Associated VLANs
- Associated server farms
- Virtual context name

Related Topics

- Configuring Virtual Servers, page 5-2
- Managing Virtual Servers, page 5-63

Displaying Virtual Server Statistics and Status Information

You can display virtual server statistics and status information for a particular virtual server by using the **Details** button. DM accesses the **show service-policy** *policy_name* **detail** CLI command to display detailed virtual server information.

Procedure

Step 1 Choose **Config > Virtual Contexts >** *context* **> Load Balancing > Virtual Servers**.

The Virtual Servers table appears.

Step 2 In the Virtual Servers table, choose a virtual server from the Virtual Servers table, and click **Details**.

The **show service-policy** *policy_name* **detail** CLI command output appears. For details on the displayed output fields, see the *Server Load-Balancing Guide, Cisco ACE Application Control Engine*.

Step 3 Click **Update Details** to refresh the output for the **show service-policy** *policy_name* **detail** CLI command.

Step 4 Click **Close** to return to the Virtual Servers table.

Related Topics

- Configuring Virtual Servers, page 5-2
- Managing Virtual Servers, page 5-63
- Viewing All Virtual Servers, page 5-65

Activating Virtual Servers

Use this procedure to activate a virtual server.

Procedure

Step 1 Select **Config > Operations > Virtual Servers**. The Virtual Servers table appears.

Step 2 Select the server that you want to activate, and 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 5-63
- Viewing All Virtual Servers, page 5-65
- Suspending Virtual Servers, page 5-65

Suspending Virtual Servers

Use this procedure to suspend a virtual server.

Procedure

Step 1 Select **Config > Operations > Virtual Servers**. The Virtual Servers table appears.

Step 2 Select the virtual server that you want to suspend, and 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.

Caution **Do not enter a password in the Reason field.**

Step 4 Do the following:

- Click **Deploy Now** to deploy this configuration. The virtual server is taken out of service and the Device Manager returns to the Virtual Servers table. The screen refreshes with updated information in the Oper State column.
- Click **Cancel** to exit this procedure without suspending the virtual server and to return to the Virtual Servers table.

Related Topics

- Managing Virtual Servers, page 5-63
- Viewing All Virtual Servers, page 5-65
- Activating Virtual Servers, page 5-64

Viewing All Virtual Servers

To view all virtual servers, choose **Config > Operations > Virtual Servers**. The Virtual Servers table appears with the following information for each server: Table 5-17 describes the Virtual Servers table information.

Table 5-17 Virtual Server Table Fields

Item	Description
Name	Server farm name sorted by virtual context.
Policy Map	Associated policy map.
IP Address/Protocol/Port	Server farm IP address, protocol, and port number used for communications.
Context	Virtual context associated with the server farm.
Admin	Administrative state of the virtual server: Up or Down.
Oper	Operational state of the virtual server: Up or Down. To display detailed information about the virtual server in a popup window, click the linked state value in this column. **Note** The display virtual server details feature requires ACE software Version A3(2.1) or later. An error displays with earlier software versions.
DWS	Operating state of Dynamic Workload Scaling for the virtual server, which can be: • N/A—Not applicable; he server farms associated with the virtual server are not configured to use Dynamic Workload Scaling. • Local—At least one server farm associated the virtual server is configured to use Dynamic Workload Scaling, but the ACE is sending traffic to the VM Controller's local VMs only. • Expanded—At least one server farm associated the virtual server is configured to use Dynamic Workload Scaling and the ACE is sending traffic to the VM Controller's local and remote VMs.
Conn	Number of active connections.
Stat Age	Time as of the loading of the page since the SNMP values were polled.
Server farms	Associated server farms.
VLANs	Associated VLANs.

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 5-64
- Suspending Virtual Servers, page 5-65