This chapter describes how to configure class maps and policy maps to provide a global level of classification for filtering traffic received by or passing through the Cisco 4700 Series Application Control Engine (ACE) appliance. You create traffic policies and attach these policies to one or more VLAN interfaces associated with the ACE to apply feature-specific actions to the matching traffic.

The ACE uses the individual traffic policies to implement the following functions:

- Remote access using Secure Shell (SSH) or Telnet
- Server load balancing
- Application acceleration and optimization
- Network Address Translation (NAT)
- HTTP deep packet inspection, FTP command inspection, or application protocol inspection
- Secure Sockets Layer (SSL) security services between a web browser (the client) and the HTTP connection (the server)
- TCP/IP normalization and termination
Class Map and Policy Map Overview

This chapter contains the following major sections:

- Class Map and Policy Map Overview
- Class Map and Policy Map Configuration Quick Start
- Configuring Layer 3 and Layer 4 Class Maps
- Configuring Layer 7 Class Maps
- Configuring a Layer 3 and Layer 4 Policy Map
- Configuring a Layer 7 Policy Map
- Applying a Service Policy
- Class Maps and Policy Map Examples
- Example of a Traffic Policy Configuration
- Viewing Class Maps, Policy Maps, and Service Policies

Class Map and Policy Map Overview

You classify inbound network traffic destined to, or passing through, the ACE based on a series of flow match criteria specified by a class map. Each class map defines a traffic classification: network traffic that is of interest to you. A policy map defines a series of actions (functions) that you want applied to a set of classified inbound traffic.

Class maps enable you to classify network traffic based on the following criteria:

- Layer 3 and Layer 4 traffic flow information—Source or destination IP address, source or destination port, virtual IP address, IP protocol and port, or management protocol
- Layer 7 protocol information—HTTP cookie, HTTP URL, HTTP header, HTTP content, or FTP request commands

The traffic classification process consists of the following three steps:

1. Creating a class map by using the `class-map` command and the associated `match` commands, which comprise a set of match criteria related to Layer 3 and Layer 4 traffic classifications or Layer 7 protocol classifications.
2. Creating a policy map by using the `policy-map` command, which refers to the class maps and identifies a series of actions to perform based on the traffic match criteria.
3. Activating the policy map and attaching it to a specific VLAN interface or globally to all VLAN interfaces associated with a context by using the `service-policy` command that are to filter traffic received by the ACE.

Traffic policies support the following feature-specific actions performed by the ACE:

- Remote access using the following management protocols: HTTP, HTTPS, Internet Control Message Protocol (ICMP), Simple Network Management Protocol (SNMP), Secure Shell (SSH), or Telnet
- Server load balancing based on Layer 3 and Layer 4 connection information (virtual IP address)
- Application acceleration and optimization
- Server load balancing based on Layer 7 HTTP-related information (such as HTTP headers, cookies, and URLs), or client source IP address
- SSL security services between a web browser (the client) and the HTTP connection (the server)
- HTTP deep packet inspection
- FTP command request inspection
- Application protocol inspection (also known as protocol fixup)
- NAT
- TCP/IP termination and normalization
- Exchange XML documents over HTTP or secure HTTP (HTTPS)

This section contains the following overview topics:

- Class Maps
- Policy Maps
- Service Policies

The flow chart shown in Figure 4-1 shows a basic overview of the process required to configure class maps and policy maps (application protocol inspection). The figure also illustrates how the ACE associates the various components of the class map and policy map configuration with each other.
Chapter 4 Configuring Class Maps and Policy Maps

Class Map and Policy Map Overview

Figure 4-1 Class Map and Policy Map—Application Protocol Inspection Configuration Flow Diagram

1. **Layer 7 HTTP Inspection Class Map**
   (config)# class-map type http inspect match-all match-any HTTP_INSPECT_L7CLASS
   Defines multiple Layer 7 HTTP deep packet inspection match criteria, such as:
   - Content expressions and length
   - Header, header length, header MIME-type
   - Port misuse
   - URL expressions and length

2. **Layer 7 HTTP Inspection Policy Map**
   (config)# policy-map type inspect http all-match HTTP_INSPECT_L7POLICY
   Associates the Layer 7 HTTP inspection class map and specifies one or more of the following actions:
   - Permit
   - Reset

3. **Layer 7 FTP Inspection Class Map**
   (config)# class-map type ftp inspect match-any FTP_INSPECT_L7CLASS
   Defines multiple Layer 7 FTP request command inspection match criteria, including: appe, cdup, dele, get, help, mkd, put, rmd, rnmf, rnto, site, stou, and syst

4. **Layer 7 FTP Inspection Policy Map**
   (config)# policy-map type inspect ftp first-match FTP_INSPECT_L7POLICY
   Associates the Layer 7 FTP inspection class map and specifies one or more of the following actions:
   - Deny
   - Mask-reply

5. **Layer 3 and Layer 4 Traffic Class Map**
   (config)# class-map match-all match-any APP_INSPECT_L4CLASS
   Defines Layer 3 and Layer 4 traffic match criteria for application protocol inspection:
   - Access list
   - Port

6. **Layer 3 and Layer 4 Policy Map**
   (config)# policy-map multi-match HTTP_INSPECT_L4POLICY
   Creates a Layer 3 and Layer 4 policy map to perform one or more of the following actions:
   - Associate Layer 3 and Layer 4 traffic class map
   - Associate Layer 7 HTTP deep packet inspection policy map
   - Associate Layer 7 FTP command inspection policy map
   - Perform HTTP inspection
   - Perform DNS inspection
   - Perform FTP inspection
   - Perform ICMP inspection
   - Perform RTSP inspection

7. **Global Service Policy/VLAN**
   (config)# service-policy input HTTP_INSPECT_L4POLICY
   Service policy applies policy map to all VLAN interfaces or to a specific VLAN interface

8. **Specific Service Policy/VLAN**
   (config)# interface vlan 50
   (config-if)# service-policy input HTTP_INSPECT_L4POLICY
   Service policy applies policy map to a specific VLAN interface
Class Maps

The **class-map** command defines each Layer 3 and Layer 4 traffic class and each Layer 7 protocol class. You create class maps to classify the traffic received and transmitted by the ACE.

- Layer 3 and Layer 4 traffic classes contain match criteria that identify the IP network traffic that can pass through the ACE or network management traffic that can be received by the ACE.

- Layer 7 protocol-specific classes identify server load balancing based on HTTP traffic, deep inspection of HTTP traffic, or the inspection of FTP commands by the ACE.

A traffic class contains the following components:

- Class map name

- One or more **match** commands that define the match criteria for the class map

- Instructions on how the ACE evaluates **match** commands when you specify more than one **match** command in a traffic class (**match-any, match-all)**

The ACE supports a system-wide maximum of 8192 class maps.

The individual **match** commands specify the criteria for classifying Layer 3 and Layer 4 network traffic as well as the Layer 7 HTTP server load balancing and application protocol-specific fields. The ACE evaluates the packets to determine whether they match the specified criteria. If a statement matches, the ACE considers that packet to be a member of the class and forwards the packet according to the specifications set in the traffic policy. Packets that fail to meet any of the matching criteria are classified as members of the default traffic class if one is specified.
When multiple match criteria exist in the traffic class, you can identify evaluation instructions by using the `match-any` or `match-all` keywords. If you specify `match-any` as the evaluation instruction, the traffic being evaluated must match one of the specified criteria, which are typically `match` commands of the same type. If you specify `match-all` as the evaluation instruction, the traffic being evaluated must match all of the specified criteria, which are typically `match` commands of different types.

The specification of complex match criteria by using the `match-all` or `match-any` keywords for Layer 7 HTTP load-balancing applications is useful as a means to provide the nesting of one class map within a second class map. For example, you can specify a match criteria for load balancing where the URL is either /foo or /bar and the header “host” equals “thishost.”

```
host1/Admin(config)# class-map type http loadbalance match-any
  URLCHK_SLB_L7_CLASS
host1/Admin(config-cmap-http-lb)# match http url /foo
host1/Admin(config-cmap-http-lb)# match http url /bar
host1/Admin(config-cmap-http-lb)# exit
```

```
host1/Admin(config)# class-map type http loadbalance match-all
  URLHDR_SLB_L7_CLASS
host1/Admin(config-cmap-http-lb)# match http header host header-value thishost
host1/Admin(config-cmap-http-lb)# match class-map URLCHK_SLB_L7_CLASS
host1/Admin(config-cmap-http-lb)# exit
```

The ACE allows you to configure two Layer 7 HTTP load-balancing class maps in a nested traffic class configuration to create a single traffic class. You can perform Layer 7 class map nesting to achieve complex logical expressions. The ACE restricts the nesting of class maps to two levels to prevent you from including one nested class map under a different class map.

**Policy Maps**

The `policy-map` command creates the traffic policy. The purpose of a traffic policy is to implement specific ACE functions associated with a traffic class. A traffic policy contains the following components:

- Policy map name
- Previously created traffic class map or, optionally, the class-default class map
- One or more of the individual Layer 3 and Layer 4 or Layer 7 policies that specify the actions (functions) to be performed by the ACE
Chapter 4  Configuring Class Maps and Policy Maps

Class Map and Policy Map Overview

The ACE supports a system-wide maximum of 4096 policy maps.

A Layer 7 policy map is always associated within a Layer 3 and Layer 4 policy map to provide an entry point for traffic classification. Layer 7 policy maps are considered to be child policies and can only be nested under a Layer 3 and Layer 4 policy map.

Only a Layer 3 and Layer 4 policy map can be activated on a VLAN interface; a Layer 7 policy map cannot be directly applied on an interface. For example, to associate a Layer 7 load-balancing policy map, you nest the load-balancing policy map by using the Layer 3 and Layer 4 loadbalance policy command.

Depending on the policy-map command, the ACE executes the action specified in the policy map on the network traffic as follows:

- **first-match**—For policy-map commands that contain the first-match keyword, the ACE executes the specified action only for traffic that meets the first matching classification within a policy map. No additional actions are executed.

- **all-match**—For policy-map commands that contain the all-match keyword, the ACE attempts to match a packet against all classes in the policy map and executes the actions of all matching classes associated with the policy map.

- **multi-match**—For policy-map commands that contain the multi-match keyword, these commands specify that multiple sets of classes exist in the policy map and allow a multi-feature policy map. The ACE applies a first-match execution process to each class set in which a packet can match multiple classes within the policy map, but the ACE executes the action for only one matching class within each class set. The definition of which classes are in the same class set depends on the actions applied to the classes; the ACE associates each policy map action with a specific set of classes. Some ACE functions may be associated with the same class set as other features (for example, application protocol inspection actions would typically be associated with the same class set), while the ACE associates other features with a different class set.

When there are multiple instances of actions of the same type configured in a policy map, the ACE performs the first action encountered of the same type that has a match.
If none of the classifications specified in policy maps match, then the ACE executes the default actions specified against the class map configured with the class-default keyword (if one is specified). All traffic that fails to meet the other matching criteria in the named class map belongs to the default traffic class. The class map configured with the class-default keyword has an implicit match-any match statement in it and is used to match any traffic classification.

For example, with the following classifications for a specific request, the ACE attempts to match the incoming content request with the classification defined in class maps C1, C2, and C3:

```
host1/Admin(config)# policy-map type loadbalance first-match SLB_L7_POLICY
host1/Admin(config-pmap-lb)# class C1
host1/Admin(config-pmap-lb-c)# serverfarm SF1
host1/Admin(config-pmap-lb-c)# exit
host1/Admin(config-pmap-lb)# class C2
host1/Admin(config-pmap-lb-c)# serverfarm SF2
host1/Admin(config-pmap-lb-c)# exit
host1/Admin(config-pmap-lb)# class C3
host1/Admin(config-pmap-lb-c)# serverfarm SF3
host1/Admin(config-pmap-lb-c)# exit
host1/Admin(config-pmap-lb)# class class-default
host1/Admin(config-pmap-lb-c)# serverfarm SFBACKUP
```

If the match criteria satisfies, the ACE load balances a content request to serverfarm SF1; if not, the ACE evaluates the match criteria in class map C2 and class map C3. If the request does not match any of the classifications in class maps C1, C2, or C3, then the class defined with the class-default keyword is guaranteed to match because it contains a match-any match statement in it. This action results in the ACE load balancing the request to the SFBACKUP server farm.

The ACE supports flexible class map ordering within a policy map. The ACE executes only the actions for the first matching traffic classification, so the order of class maps within a policy map is very important. The policy lookup order is based on the security features of the ACE. The policy lookup order is implicit, irrespective of the order in which you configure policies on the interface.

The policy lookup order of the ACE is as follows:

1. Access control (permit or deny a packet)
2. Permit or deny management traffic
3. TCP/UDP connection parameters
4. Load balancing based on a virtual IP (VIP)
5. Application protocol inspection
6. Source NAT
7. Destination NAT

The sequence in which the ACE applies the actions for a specific policy are independent of the actions configured for a class inside a policy.

**Service Policies**

You activate policies on a single VLAN interface or globally to all VLAN interfaces associated with a context by using the `service-policy` command. The `service-policy` command attaches the traffic policy to each specified VLAN interface. The ACE evaluates all network traffic on the specified interface according to the actions specified in the named traffic policy. Policies and associated actions specify the behavior that you want applied to a traffic class.

Policy maps that are applied globally in a context are also internally applied to all interfaces that exist in the context. A policy that has been activated on the interface overwrites global policies for overlapping classifications and actions.

The ACE allows only one policy of a specific feature type to be activated on a VLAN interface. Because you can apply many policies of different features on a specific interface, policy lookup ordering in the ACE is important (see the “Policy Maps” section).

For example, to specify an interface VLAN and apply multiple service policies to the VLAN, enter:

```
host1/Admin(config)# interface vlan 50
host1/Admin(config-if)# ip address 172.16.1.100 255.255.255.0
host1/Admin(config-if)# service-policy input L4_HTTP_SLB_POLICY
host1/Admin(config-if)# service-policy input L4_MGMT_POLICY
```
Class Map and Policy Map Configuration Quick Start

Table 4-1 and Table 4-2 provide a quick overview of the steps required to create a class map with match criteria that define Layer 3 and Layer 4 network traffic classifications.

- Table 4-1 describes the steps to define Layer 3 and Layer 4 traffic classes with match criteria that identify the IP network traffic that can pass through the ACE.
- Table 4-2 describes the steps to define Layer 3 and Layer 4 network management traffic that can be received by the ACE.

Each step includes the CLI command required to complete the task.

Table 4-1  Layer 3 and Layer 4 Network Traffic Class Configuration Quick Start

<table>
<thead>
<tr>
<th>Task and Command Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. If you are operating in multiple contexts, observe the CLI prompt to verify that you are operating in the desired context. If necessary, log directly in to, or change to, the correct context.</td>
</tr>
<tr>
<td>host1/Admin# changeto C1</td>
</tr>
<tr>
<td>host1/C1#</td>
</tr>
<tr>
<td>The rest of the examples in this table use the Admin context, unless otherwise specified. For details on creating contexts, see the Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide.</td>
</tr>
<tr>
<td>2. Enter configuration mode.</td>
</tr>
<tr>
<td>host1/Admin# config</td>
</tr>
<tr>
<td>Enter configuration commands, one per line. End with CNTL/Z</td>
</tr>
<tr>
<td>host1/Admin(config)#</td>
</tr>
</tbody>
</table>
Table 4-1  Layer 3 and Layer 4 Network Traffic Class Configuration Quick Start (continued)

<table>
<thead>
<tr>
<th>Task and Command Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>3. Create one or more Layer 3 and Layer 4 class maps that classify the network traffic that passes through the ACE. If you do not specify the <strong>match-all</strong> or <strong>match-any</strong> keyword, the traffic must match all the match criteria in the class map to be classified as part of the traffic class.</td>
</tr>
</tbody>
</table>
  
  ```
  host1/Admin(config)# class-map match-any L4_SLB_VIP_CLASS
  host1/Admin(config-cmap)#
  ```

  After you create a class map, you will enter class map configuration mode.

<table>
<thead>
<tr>
<th>4. (Optional) Specify a description about the network traffic class map.</th>
</tr>
</thead>
<tbody>
<tr>
<td>host1/Admin(config-cmap)# description HTTP protocol deep inspection of incoming traffic</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>5. (Optional) Specify the <strong>match any</strong> command if you want the ACE to perform a match on any traffic passing through it.</th>
</tr>
</thead>
<tbody>
<tr>
<td>host1/Admin(config-cmap)# match any</td>
</tr>
</tbody>
</table>

**Note**  The **match any** command cannot be combined with any other match criteria.

<table>
<thead>
<tr>
<th>6. (Optional) Specify a VIP classification to be used as the server load-balancing matching criteria in the class map.</th>
</tr>
</thead>
<tbody>
<tr>
<td>host1/Admin(config-cmap)# match virtual-address 192.168.1.10 tcp port eq 80</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>7. (Optional) Specify a previously defined access list so that the ACE can check its contents against network traffic as a matching criteria in the class map.</th>
</tr>
</thead>
<tbody>
<tr>
<td>host1/Admin(config-cmap)# match access-list INBOUND</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>8. (Optional) Specify a source IP address and subnet mask as a matching criteria in the class map.</th>
</tr>
</thead>
<tbody>
<tr>
<td>host1/Admin(config-cmap)# match source-address 192.168.10.1 255.255.255.0</td>
</tr>
</tbody>
</table>
Table 4-1  Layer 3 and Layer 4 Network Traffic Class Configuration Quick Start (continued)

Task and Command Example

9. (Optional) Specify the destination IP address and subnet mask as a matching criteria in the class map.

   host1/Admin(config-cmap)# match destination-address 172.16.20.1 255.255.0.0

10. (Optional) Specify a TCP or UDP port number or port range as a matching criteria in the class map.

    host1/Admin(config-cmap)# match port tcp eq 23

Table 4-2  Layer 3 and Layer 4 Network Management Traffic Class Configuration Quick Start

Task and Command Example

1. If you are operating in multiple contexts, observe the CLI prompt to verify that you are operating in the desired context. If necessary, log directly in to, or change to, the correct context.

   host1/Admin# chanogeto C1
   host1/C1#

   The rest of the examples in this table use the Admin context, unless otherwise specified. For details on creating contexts, see the Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide.

2. Enter configuration mode.

   host1/Admin# config
   Enter configuration commands, one per line. End with CNTL/Z
   host1/Admin(config)#
3. Create one or more class maps that permit network management traffic to be received by the ACE based on a network management protocol (HTTP, HTTPS, ICMP, SNMP, SSH, or Telnet) and source IP address. If you do not specify the **match-all** or **match-any** keyword, the traffic must match all the match criteria in the class map to be classified as part of the traffic class.

```bash
host1/Admin(config)# class-map type management match-any L4_MGMT_CLASS host1/Admin(config-cmap-mgmt)#
```

After you create a class map, you will enter class map management configuration mode.

4. (Optional) Specify a description about the network management traffic class map.

```bash
host1/Admin(config-cmap)# description enable SSH and Telnet protocols
```

5. (Optional) Configure the class map to identify the IP network management traffic received by the ACE.

```bash
host1/Admin(config-cmap-mgmt)# match protocol ssh source-address 192.168.10.1 255.255.255.0 host1/Admin(config-cmap-mgmt)# match protocol telnet source-address 192.168.10.1 255.255.255.0 host1/Admin(config-cmap-mgmt)# match protocol icmp source-address 192.168.10.1 255.255.255.0 host1/Admin(config-cmap-mgmt)# exit
```
Table 4-3 provides a quick overview of the steps required to create a class map with match criteria that define specific Layer 7 protocol classifications. Each step includes the CLI command required to complete the task.

**Table 4-3   Layer 7 Class Map Configuration Quick Start**

<table>
<thead>
<tr>
<th>Task and Command Example</th>
<th>1. If you are operating in multiple contexts, observe the CLI prompt to verify that you are operating in the desired context. If necessary, log directly in to, or change to, the correct context.</th>
</tr>
</thead>
</table>
|                          | host1/Admin#  **changeto C1**  
|                          | host1/C1#  
|                          | The rest of the examples in this table use the Admin context, unless otherwise specified. For details on creating contexts, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*. |
|                          | 2. Enter configuration mode.  
|                          | host1/Admin#  **config**  
|                          | Enter configuration commands, one per line. End with CNTL/Z  
|                          | host1/Admin(config)#  
|                          | 3. (Optional) Create one or more class maps that define Layer 7 HTTP content load-balancing decisions based on cookies, HTTP headers, URLs, or source IP addresses. If you do not specify the **match-all** or **match-any** keyword, the traffic must match all the match criteria in the class map to be classified as part of the traffic class.  
|                          | After you create a class map, you will enter class map HTTP load balancing configuration mode. |
|                          | host1/Admin(config)#  **class-map type http loadbalance match-any L7_SLB_CLASS**  
|                          | host1/Admin(config-cmap-http-lb)#  **description HTTP LOAD BALANCE PROTOCOL 1**  
|                          | host1/Admin(config-cmap-http-lb)#  **match http url .*.gif**  
|                          | host1/Admin(config-cmap-http-lb)#  **match http url .*.html**  
|                          | host1/Admin(config-cmap-http-lb)#  **exit**  


### Task and Command Example

<table>
<thead>
<tr>
<th>Task and Command Example</th>
</tr>
</thead>
</table>
| **4.** (Optional) Create one or more class maps that define the Layer 7 SSL initiation functions applied to outbound traffic. If you do not specify the match-all or match-any keyword, the traffic must match all the match criteria in the class map to be classified as part of the traffic class. After you create a class map, you will enter class map HTTP load balancing configuration mode.  
host1/Admin(config)# class-map type http loadbalance match-any L7_SSL_CLASS  
host1/Admin(config-cmap-http-lb)# description HTTP LOAD BALANCE PROTOCOL 1  
host1/Admin(config-cmap-http-lb)# match header Host header-value .mycompanyexample.com  
host1/Admin(config-cmap-http-lb)# match http url .*.html  
host1/Admin(config-cmap-http-lb)# exit |
| **5.** (Optional) Create one or more class maps to be used for the deep packet application protocol inspection of HTTP traffic. If you do not specify the match-all or match-any keyword, the traffic must match all the match criteria to be classified as part of the traffic class. After you create a class map, you will enter class map HTTP application protocol inspection configuration mode.  
host1/Admin(config)# class-map type http inspect match-any HTTP_INSPECT_L7_CLASS  
host1/Admin(config-cmap-http-insp)# description HTTP protocol deep inspection of incoming traffic  
host1/Admin(config-cmap-http-insp)# match header length request eq 256  
host1/Admin(config-cmap-http-insp)# match header Host header-value .mycompanyexample.com  
host1/Admin(config-cmap-http-insp)# match url length eq 10000  
host1/Admin(config-cmap-http-insp)# exit |
Table 4-3  Layer 7 Class Map Configuration Quick Start (continued)

**Task and Command Example**

6. (Optional) Create one or more class maps to be used for the inspection of FTP commands.

   After you create a class map, you will enter FTP inspection class map configuration mode.

   ```
   host1/Admin(config)# class-map type ftp inspect match-any
                FTP_COMMAND_INSPECT_L7_CLASS
   host1/Admin(config-cmap-ftp-insp)# description FTP command inspection of incoming traffic
   host1/Admin(config-cmap-ftp-insp)# match request-method cdup
   host1/Admin(config-cmap-ftp-insp)# match request-method get
   host1/Admin(config-cmap-ftp-insp)# match request-method stou
   host1/Admin(config-cmap-ftp-insp)# match request-method put
   host1/Admin(config-cmap-ftp-insp)# exit
   ```

Table 4-4 provides a quick overview of the steps required to create and configure a Layer 3 and Layer 4 traffic policy map and to apply the policy to one or all of the VLAN interfaces associated with the context. Each step includes the CLI command required to complete the task.
Table 4-4  Layer 3 and Layer 4 Traffic Policy Map Configuration Quick Start

Task and Command Example

1. If you are operating in multiple contexts, observe the CLI prompt to verify that you are operating in the desired context. If necessary, log directly in to, or change to, the correct context.

   host1/Admin# changeto C1
   host1/C1#

   The rest of the examples in this table use the Admin context, unless otherwise specified. For details on creating contexts, see the Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide.

2. Enter configuration mode.

   host1/Admin# config
   Enter configuration commands, one per line. End with CNTL/Z
   host1/Admin(config)#

3. Configure a Layer 3 and Layer 4 policy map that defines the different actions of traffic passing through the ACE.

   After you configure a policy map, you will enter policy map configuration mode.

   host1/Admin(config)# policy-map multi-match L4_SLB_POLICY
   host1/Admin(config-pmap) #

4. Specify a traffic class previously created with the class-map command to associate network traffic with the traffic policy.

   host1/Admin(config-pmap)# class L4_SLB_CLASS
   host1/Admin(config-pmap-c)#

5. (Optional) Specify a description about the network traffic policy map.

   host1/Admin(config-pmap-c)# description HTTP protocol deep inspection of incoming traffic

6. (Optional) Specify the class-default class map for the Layer 3 and Layer 4 traffic policy.

   host1/Admin(config-pmap-c)# class class-default
   host1/Admin(config-pmap-c)#
Table 4-5 provides a quick overview of the steps required to create and configure a Layer 3 and Layer 4 network management policy map and to apply the policy to one or all of the VLAN interfaces associated with the context. Each step includes the CLI command required to complete the task.
Table 4-5  Layer 3 and Layer 4 Network Management Policy Map Configuration Quick Start

Task and Command Example

1. If you are operating in multiple contexts, observe the CLI prompt to verify that you are operating in the desired context. If necessary, log directly in to, or change to, the correct context.

   host1/Admin# `changeto C1`
   host1/C1#

   The rest of the examples in this table use the Admin context, unless otherwise specified. For details on creating contexts, see the Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide.

2. Enter configuration mode.

   host1/Admin# `config`
   Enter configuration commands, one per line. End with CNTL/Z
   host1/Admin(config)#

3. Configure a Layer 3 and Layer 4 policy map that permits specified IP management traffic to be received by the ACE.

   After you configure a policy map, you will enter policy map management configuration mode.

   host1/Admin(config)# `policy-map type management first-match L4_MGMT_POLICY`
   host1/Admin(config-pmap-mgmt)#

4. (Optional) Specify a description about the network management traffic policy map.

   host1/Admin(config-pmap-mgmt)# `description enable SSH and Telnet protocols`

5. Allow the IP network management traffic listed in the Layer 3 and Layer 4 class map to be received by the ACE by specifying the `permit` command in policy map class configuration mode.

   host1/Admin(config-pmap-mgmt)# `class TELNET_CLASS`
   host1/Admin(config-pmap-mgmt-c)# `permit`
   host1/Admin(config-pmap-mgmt-c)# `exit`
   host1/Admin(config-pmap-mgmt)# `class SSH_CLASS`
   host1/Admin(config-pmap-mgmt-c)# `permit`
   host1/Admin(config-pmap-mgmt-c)# `exit`
6. Attach the Layer 3 and Layer 4 traffic policy to a single VLAN interface or globally to all VLAN interfaces in the same context.

   host1/Admin(config)# interface vlan 50
   host1/Admin(config-if)# ip address 192.168.1.100 255.255.0.0
   host1/Admin(config-if)# service-policy input L4_MGMT_POLICY

7. (Optional) Save your configuration changes to Flash memory.

   host1/Admin(config)# exit
   host1/Admin# copy running-config startup-config
Table 4-6 provides a quick overview of the steps required to create and configure a Layer 7 policy map. Each step includes the CLI command required to complete the task.

**Table 4-6  Layer 7 Policy Map Configuration Quick Start**

<table>
<thead>
<tr>
<th>Task and Command Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. If you are operating in multiple contexts, observe the CLI prompt to verify that you are operating in the desired context. If necessary, log directly in to, or change to, the correct context.</td>
</tr>
<tr>
<td>host1/Admin# <strong>changeto C1</strong></td>
</tr>
<tr>
<td>host1/C1#</td>
</tr>
<tr>
<td>The rest of the examples in this table use the Admin context, unless otherwise specified. For details on creating contexts, see the <em>Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide</em>.</td>
</tr>
<tr>
<td>2. Enter configuration mode.</td>
</tr>
<tr>
<td>host1/Admin# <strong>config</strong></td>
</tr>
<tr>
<td>Enter configuration commands, one per line. End with CNTL/Z</td>
</tr>
<tr>
<td>host1/Admin(config)#</td>
</tr>
<tr>
<td>3. (Optional) Create and configure a policy map that defines Layer 7 HTTP content load-balancing decisions.</td>
</tr>
<tr>
<td>host1/Admin(config)# <strong>policy-map type loadbalance first-match</strong></td>
</tr>
<tr>
<td>L7_SLB_POLICY</td>
</tr>
<tr>
<td>host1/Admin(config-pmap-lb)# <strong>description</strong> HTTP LOAD BALANCE PROTOCOL 1</td>
</tr>
<tr>
<td>host1/Admin(config-pmap-lb)# <strong>class</strong> L7_SLB_CLASS</td>
</tr>
<tr>
<td>host1/Admin(config-pmap-lb-c)# <strong>serverfarm</strong> FARM2 backup FARM3 sticky</td>
</tr>
<tr>
<td>4. (Optional) Create and configure a policy map that defines Layer 7 application acceleration and optimization decisions.</td>
</tr>
<tr>
<td>host1/Admin(config)# <strong>policy-map type optimization http first-match</strong></td>
</tr>
<tr>
<td>L7_OPTIMIZATION_POLICY</td>
</tr>
<tr>
<td>host1/Admin(config-pmap-optmz)# <strong>description</strong> This policy map performs delta optimization along with SLB activities</td>
</tr>
<tr>
<td>host1/Admin(config-pmap-optmz)# <strong>class</strong> L7_SLB_CLASS</td>
</tr>
<tr>
<td>host1/Admin(config-pmap-optmz-c)# <strong>action</strong> ACT_LIST1 parameter OPTIMIZE_PARAM_MAP</td>
</tr>
</tbody>
</table>
### Task and Command Example

5. (Optional) Create and configure a Layer 7 application inspection policy map that enables the deep packet inspection of the HTTP protocol.

```bash
host1/Admin(config)# policy-map type inspect http all-match HTTP_INSPECT_L7_POLICY
host1/Admin(config-pmap-ins-http)# description HTTP protocol deep inspection of incoming traffic
host1/Admin(config-pmap-ins-http)# class HTTP_INSPECT_L7_CLASS
host1/Admin(config-pmap-ins-http-c)# permit log
```

6. (Optional) Create and configure a Layer 7 policy map that enables FTP command inspection.

```bash
host1/Admin(config)# policy-map type inspect ftp first-match FTP_INSPECTION_L7_POLICY
host1/Admin(config-pmap-ftp-ins)# description FTP command inspection of incoming traffic
host1/Admin(config-pmap-ftp-ins)# class FTP_INSPECT_L7_CLASS
host1/Admin(config-pmap-ftp-ins-c)# match request-method stou
host1/Admin(config-pmap-ftp-ins-c)# deny
```
Chapter 4  Configuring Class Maps and Policy Maps

Class Map and Policy Map Configuration Quick Start

Table 4-6  Layer 7 Policy Map Configuration Quick Start (continued)

<table>
<thead>
<tr>
<th>Task and Command Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>7. Associate the Layer 7 policy map with a Layer 3 and Layer 4 policy map by using the <strong>policy-map multi-match</strong> command as specified below.</td>
</tr>
<tr>
<td>- To associate a Layer 7 load-balancing policy map, nest the load-balancing policy map by using the Layer 3 and Layer 4 <strong>loadbalance policy</strong> command.</td>
</tr>
<tr>
<td>- To associate a Layer 7 optimization HTTP policy map, nest the optimization policy map by using the Layer 3 and Layer 4 <strong>optimize http policy</strong> command.</td>
</tr>
<tr>
<td>- To associate a Layer 7 HTTP application inspection policy map, nest the HTTP application traffic policy by using the Layer 3 and Layer 4 <strong>inspect http policy</strong> command.</td>
</tr>
<tr>
<td>- To associate a Layer 7 FTP command inspection policy map, nest the FTP command inspection traffic policy by using the Layer 3 and Layer 4 <strong>inspect ftp policy</strong> command.</td>
</tr>
<tr>
<td>For example, to nest the Layer 7 L7_SLB_POLICY policy map within the Layer 3 and Layer 4 L4_SLB_POLICY policy map, enter:</td>
</tr>
<tr>
<td>host1/Admin(config)# policy-map type loadbalance first-match L7_SLB_POLICY</td>
</tr>
<tr>
<td>host1/Admin(config-pmap-lb)# description HTTP LOAD BALANCE PROTOCOL 1</td>
</tr>
<tr>
<td>host1/Admin(config-pmap-lb)# class L7_SLB_CLASS</td>
</tr>
<tr>
<td>host1/Admin(config-pmap-lb-c)# serverfarm FARM2 backup FARM3 sticky</td>
</tr>
<tr>
<td>host1/Admin(config-pmap-lb-c)# exit</td>
</tr>
<tr>
<td>host1/Admin(config-pmap-lb)# exit</td>
</tr>
<tr>
<td>host1/Admin(config)# policy-map multi-match L4_SLB_POLICY</td>
</tr>
<tr>
<td>host1/Admin(config-pmap)# class L4_SLB_CLASS</td>
</tr>
<tr>
<td>host1/Admin(config-pmap-c)# loadbalance policy L7_SLB_POLICY</td>
</tr>
<tr>
<td>8. Attach the Layer 3 and Layer 4 traffic policy to a single VLAN interface or globally to all VLAN interfaces in the same context.</td>
</tr>
<tr>
<td>host1/Admin(config)# interface vlan 50</td>
</tr>
<tr>
<td>host1/Admin(config-if)# ip address 192.168.1.100 255.255.0.0</td>
</tr>
<tr>
<td>host1/Admin(config-if)# service-policy input L4_SLB_POLICY</td>
</tr>
<tr>
<td>9. (Optional) Save your configuration changes to Flash memory.</td>
</tr>
<tr>
<td>host1/Admin(config)# exit</td>
</tr>
<tr>
<td>host1/Admin# copy running-config startup-config</td>
</tr>
</tbody>
</table>
Configuring Layer 3 and Layer 4 Class Maps

A Layer 3 and Layer 4 class map contains match criteria that classifies network traffic that can pass through the ACE or network management traffic that can be received by the ACE. For more information about the role of class maps in the ACE, see the “Class Map and Policy Map Overview” section.

This section contains the following topics:

- Defining Layer 3 and Layer 4 Classifications for Network Traffic Passing Through the ACE
- Defining Layer 3 and Layer 4 Classifications for Network Management Traffic Received by the ACE

Defining Layer 3 and Layer 4 Classifications for Network Traffic Passing Through the ACE

Layer 3 and Layer 4 traffic classes contain match criteria that identify the IP network traffic that can pass through the ACE. You can classify network traffic based on the source or destination IP address, the source or destination port, the virtual IP address, or the IP protocol and port.

This section contains the following topics:

- Creating a Layer 3 and Layer 4 Network Traffic Class Map
- Defining a Class Map Description
- Defining Access-List Match Criteria
- Defining Match Any Criteria
- Defining Destination IP Address and Subnet Mask Match Criteria
- Defining TCP/UDP Port Number or Port Range Match Criteria
- Defining the Source IP Address and Subnet Mask Match Criteria
- Defining the VIP Address Match Criteria
Creating a Layer 3 and Layer 4 Network Traffic Class Map

To create a Layer 3 and Layer 4 class map to classify network traffic passing through the ACE, use the `class-map` command in configuration mode.

A single class map can have multiple `match` commands that you can use to specify the matching criteria. For example, you can configure class maps to define multiple access group, source IP address, destination IP address, or port commands in a group that you then associate with a traffic policy. The `match-all` and `match-any` keywords determine how the ACE evaluates multiple match statements operations when multiple match criteria exist in a class map.

The syntax of this command is:

```
class-map [match-all | match-any] map_name
```

The arguments and options are:

- **match-all | match-any**—(Optional) Determines how the ACE evaluates Layer 3 and Layer 4 network traffic when multiple match criteria exist in a class map. The class map is considered a match if the `match` commands meet one of the following conditions:
  - **match-all**—All of the match criteria listed in the class map match the network traffic class in the class map (typically `match` commands of different types).
  - **match-any**—Only one of the match criteria listed in the class map matches the network traffic class in the class map (typically `match` commands of the same type).

The default setting is to meet all of the match criteria (`match-all`) in a class map.

- **map_name**—Name assigned to the class map. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.
When you create a class map, you will enter class map configuration mode. To classify network traffic passing through the ACE, include one or more of the following commands to configure the match criteria for the class map:

- **description**—See the “Defining a Class Map Description” section
- **match access-list**—See the “Defining Access-List Match Criteria” section
- **match any**—See the “Defining Match Any Criteria”
- **match destination-address**—See the “Defining Destination IP Address and Subnet Mask Match Criteria” section
- **match port**—See the “Defining TCP/UDP Port Number or Port Range Match Criteria” section
- **match source-address**—See the “Defining the Source IP Address and Subnet Mask Match Criteria” section
- **match virtual-address**—See the “Defining the VIP Address Match Criteria” section

Following these guidelines when creating a class map to define a Layer 3 and Layer 4 match classification:

- You can include only one **match any** command within a class map and you cannot combine the **match any** command with other types of **match** commands in a class map since the other match criteria will be ignored.
- You may combine multiple **match access-list**, **match source-address**, **match destination-address**, and **match port** commands in a class map.
- You can include multiple **match virtual-address** commands within a class map. The **match virtual-address** command, however, cannot be combined with the other types of **match** commands in a class map. This command is intended to define a 3-tuple flow of VIP address, protocol, and port as matching criteria for server load balancing.
For example, to define the Layer 3 and Layer 4 HTTP_APP_PROTOCOL_INSPECTION_CLASS class map and specify that all commands in the class map must be satisfied for the ACE to indicate a match, enter:

```
host1/Admin(config)# class-map match-all HTTP_APP_PROTOCOL_INSPECTION_CLASS
host1/Admin(config-cmap)# description HTTP protocol deep inspection of incoming traffic
host1/Admin(config-cmap)# match port udp eq 53
```

To remove a Layer 3 and Layer 4 network traffic class map from the ACE, enter:

```
(config)# no class-map match-all HTTP_APP_PROTOCOL_INSPECTION_CLASS
```

### Defining a Class Map Description

To provide a brief summary about the Layer 3 and Layer 4 class map, use the `description` command in class map configuration mode.

The syntax of this command is:

```
description text
```

The `text` argument specifies the description that you want to provide. Enter an unquoted text string with a maximum of 240 alphanumeric characters.

For example, to specify a description that the class map is to filter network traffic to the server, enter:

```
host1/Admin(config)# class-map HTTP_APP_PROTOCOL_INSPECTION_CLASS
host1/Admin(config-cmap)# description HTTP inspection of incoming traffic
```

To remove the description from the class map, enter:

```
host1/Admin(config-cmap)# no description
```
Defining Access-List Match Criteria

To configure the class map to filter Layer 3 and Layer 4 network traffic using a predefined access control list (ACL), use the `match access-list` command in class map configuration mode. When a packet matches an entry in an ACL, and if it is a `permit` entry, the ACE allows the matching result. If it is a `deny` entry, the ACE blocks the matching result. Refer to the *Cisco 4700 Series Application Control Engine Appliance Security Configuration Guide* for details about creating ACLs in the ACE.

The syntax of this command is:

```
[line_number] match access-list name
```

The arguments are:

- `line_number`—(Optional) Line number to identify individual `match` commands. Enter an integer from 2 to 255 as the line number. You can enter `no line_number` to delete long `match` commands instead of entering the entire line. The line numbers do not dictate a priority or sequence for the match statements.

- `name`—Previously created access list identifier. Enter an unquoted text string with a maximum of 64 characters.

A single class map can have multiple `match access-list` commands. You may combine multiple `match access-list`, `match source-address`, `match destination-address`, and `match port` commands in a class map.

For example, to specify that the class map is to match on access control list INBOUND, enter:

```
host1/Admin(config)# class-map match-any L4_FILTERTRAFFIC_CLASS
host1/Admin(config-cmap)# match access-list INBOUND
```

To clear the access control list match criteria from the class map, enter:

```
host1/Admin(config-cmap)# no match access-list INBOUND
```

Defining Match Any Criteria

To instruct the ACE to perform a match on any network traffic that passes through the appliance, use the `match any` command in class map configuration mode. You can include only one `match any` command within a class map and you cannot combine the `match any` command with other types of `match` commands in a class map because the ACE ignores the match criteria.
The syntax of this command is:

```
[line_number] match any
```

The optional `line_number` argument to identify individual `match` commands to help you edit or delete them. Enter an integer from 2 to 255 as the line number. You can enter `no line_number` to delete long `match` commands instead of entering the entire line. The line numbers do not dictate a priority or sequence for the match statements.

For example, to specify that the class map is to match on any network traffic, enter:

```
host1/Admin(config)# class-map match-any L4_MATCHANYTRAFFIC_CLASS
host1/Admin(config-cmap)# match any
```

To remove the match any criteria from the class map, enter:

```
host1/Admin(config-cmap)# no match any
```

### Defining Destination IP Address and Subnet Mask Match Criteria

To specify the destination IP address and subnet mask as the Layer 3 and Layer 4 network traffic matching criteria, use the `match destination-address` command in class map configuration mode.

The syntax of this command is:

```
[line_number] match destination-address ip_address mask
```

The arguments are:

- `line_number`—(Optional) Line number to identify individual `match` commands. Enter an integer from 2 to 255 as the line number. You can enter `no line_number` to delete long `match` commands instead of entering the entire line. The line numbers do not dictate a priority or sequence for the match statements.
- `ip_address`—Destination IP address. Enter the IP address in dotted-decimal notation (for example, 192.168.11.1).
- `mask`—Subnet mask entry in dotted-decimal notation (for example, 255.255.255.0).
A single class map can have multiple `match destination-address` commands. You may combine multiple `match destination-address`, `match access-list`, `match source-address`, and `match port` commands in a class map.

For example, to specify that the ACE is to match on destination IP address 172.16.20.1 255.255.0.0, enter:

```
host1/Admin(config)# class-map L4_DEST_IP_CLASS
host1/Admin(config-cmap)# match destination-address 172.16.20.1 255.255.0.0
```

To clear the destination IP address and subnet mask match criteria from the class map, enter:

```
host1/Admin(config-cmap)# no match destination-address 172.16.20.1 255.255.0.0
```

### Defining TCP/UDP Port Number or Port Range Match Criteria

To specify a TCP or UDP port number or port range as the Layer 3 and Layer 4 network traffic matching criteria, use the `match port` command in class map configuration mode.

The syntax of this command is:

```
[line_number] match port {tcp | udp} {any | {eq port_number} | range port1 port2}
```

The keywords, arguments, and options are:

- `line_number`—(Optional) Line number to identify individual `match` commands. Enter an integer from 2 to 255 as the line number. You can enter `no line_number` to delete long `match` commands instead of entering the entire line. The line numbers do not dictate a priority or sequence for the match statements.
- `tcp | udp`—Specifies the protocol, TCP or UDP.
- `any`—Specifies a wildcard value for the TCP or UDP port number. With `any` used in place of either the `eq` or `range` values, packets from any incoming port match.
**eq port_number**—Specifies that the TCP or UDP port number must match the specified value. Enter an integer from 0 to 65535. A value of 0 instructs the ACE to include all ports. Alternatively, you can enter the name of a well-known TCP port as listed in Table 4-7 or a well-known UDP port as listed in Table 4-8.

**range port1 port2**—Specifies a port range to use for the TCP or UDP port. Valid port ranges are from 0 to 65535. A value of 0 instructs the ACE to match all ports.

A single class map can have multiple **match port** commands. You may combine multiple **match port**, **match access-list**, **match source-address**, and **match destination-address** commands in a class map.

For example, to specify that the class map is to match on TCP port number 23 (Telnet client), enter:

```plaintext
host1/Adm(config)# class-map L4_TCPPORT_CLASS
host1/Adm(config-cmap)# match port tcp eq 23
```

To clear the TCP or UDP port number match criteria from the class map, enter:

```plaintext
host1/Adm(config-cmap)# no match port tcp eq 23
```

### Defining the Source IP Address and Subnet Mask Match Criteria

To specify the client source IP address and subnet mask as the Layer 3 and Layer 4 network traffic matching criteria, use the **match source-address** command in class map configuration mode.

The syntax of this command is:

```
[line_number] match source-address ip_address mask
```

The arguments are:

- **line_number**—(Optional) Line number to identify individual **match** commands. Enter an integer from 2 to 255 as the line number. You can enter **no line_number** to delete long **match** commands instead of entering the entire line. The line numbers do not dictate a priority or sequence for the match statements.

- **ip_address**—Source IP address of the client. Enter the IP address in dotted-decimal notation (for example, 192.168.11.1).
• **mask**—Subnet mask of the client entry in dotted-decimal notation (for example, 255.255.255.0).

A single class map can have multiple **match source-address** commands. You may combine multiple **match source-address**, **match access-list**, **match destination-address**, and **match port** commands in a class map.

For example, to specify that the class map is to match on source IP address 172.16.20.1 255.255.0.0, enter:

```
host1/Admin(config)# class-map L4_SOURCE_IP_CLASS
host1/Admin(config-cmap)# match source-address 192.168.10.1 255.255.255.0
```

To clear the source IP address and subnet mask match criteria from the class map, enter:

```
host1/Admin(config-cmap)# no match source-address 192.168.10.1 255.255.255.0
```

### Defining the VIP Address Match Criteria

To define a 3-tuple flow of VIP address, protocol, and port as matching criteria for server load balancing, use the **match virtual-address** command in class map configuration mode. You can configure multiple match criteria statements to define the VIPs for server load balancing. See the *Cisco 4700 Series Application Control Engine Appliance Server Load-Balancing Configuration Guide* for details about configuring the ACE to perform server load balancing.

The syntax of this command is:

```
[line_number] match virtual-address vip_address {[netmask]
protocol_number | any | {tcp | udp} {any | eq port_number | range port1 port2}}
```

The keywords, arguments, and options are:

- **line_number**—(Optional) Line number to identify individual match commands. Enter an integer from 2 to 255 as the line number. You can enter **no line_number** to delete long match commands instead of entering the entire line. The line numbers do not dictate a priority or sequence for the match statements.

- **vip_address**—VIP server IP address of the ACE, specified in dotted decimal format (for example, 192.168.1.2).
• netmask—(Optional) Subnet mask for the VIP address, specified in dotted decimal format (for example, 255.255.255.0).

• protocol_number—(Optional) Number of an IP protocol. Enter an integer from 1 to 255 that represents the IP protocol number.

• any—Specifies a wildcard value that allows connections from any IP protocol.

• tcp | udp—Specifies the protocol, TCP or UDP.

• any—Specifies the wildcard value for the TCP or UDP port number. With any used in place of either the eq or range values, packets from any incoming port match.

• eq port_number—Specifies that the TCP or UDP port number must match the specified value. Enter an integer from 0 to 65535. A value of 0 instructs the ACE to include all ports. Alternatively, you can enter the name of a well-known TCP port as listed in Table 4-7 or a well-known UDP port as listed in Table 4-8.

• range port1 port2—Specifies a port range to use for the TCP or UDP port. Valid port ranges are from 0 to 65535. A value of 0 instructs the ACE to match all ports.

Table 4-7  Well-Known TCP Port Numbers and Keywords

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Port Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>domain</td>
<td>53</td>
<td>Domain Name System (DNS)</td>
</tr>
<tr>
<td>ftp</td>
<td>21</td>
<td>File Transfer Protocol (FTP)</td>
</tr>
<tr>
<td>ftp-data</td>
<td>20</td>
<td>FTP data connections</td>
</tr>
<tr>
<td>http</td>
<td>80</td>
<td>Hyper Text Transfer Protocol (HTTP)</td>
</tr>
<tr>
<td>https</td>
<td>443</td>
<td>HTTP over TLS or SSL (HTTPS)</td>
</tr>
<tr>
<td>irc</td>
<td>194</td>
<td>Internet Relay Chat (IRC)</td>
</tr>
<tr>
<td>matip-a</td>
<td>350</td>
<td>Mapping of Airline Traffic over Internet Protocol (MATIP) Type A</td>
</tr>
<tr>
<td>nntp</td>
<td>119</td>
<td>Network News Transport Protocol (NNTP)</td>
</tr>
<tr>
<td>pop2</td>
<td>109</td>
<td>Post Office Protocol (POP) v2</td>
</tr>
<tr>
<td>pop3</td>
<td>110</td>
<td>Post Office Protocol (POP) v3</td>
</tr>
</tbody>
</table>
Follow these guidelines when you define the VIP address match criteria:

- You can specify multiple `match virtual-address` commands within a class map.
- The `match virtual-address` command cannot be combined with other types of `match` commands.

For example, to specify that class map `L4_SLB_VIPCLASS` matches traffic destined to VIP address 192.168.1.10 and TCP port number 80, enter:

```
host1/Admin(config)# class-map L4_SLB_VIPCLASS
host1/Admin(config-cmap)# match virtual-address 192.168.1.10 tcp port eq 80
```

To remove the VIP match statement from the class map, enter:

```
host1/Admin(config-cmap)# no match virtual-address 192.168.1.10 tcp port eq 80
```
Defining Layer 3 and Layer 4 Classifications for Network Management Traffic Received by the ACE

Layer 3 and Layer 4 traffic classes contain match criteria that identify the network management traffic that can be received by the ACE. Class maps enable you to classify network traffic based on one or more of these management protocols: HTTP, HTTPS, ICMP, SNMP, SSH, or Telnet.

This section contains the following topics:
- Creating a Layer 3 and Layer 4 Network Management Traffic Class Map
- Defining Network Management Access Match Criteria

Creating a Layer 3 and Layer 4 Network Management Traffic Class Map

To create a Layer 3 and Layer 4 class map to classify the IP network management traffic received by the ACE, use the `class-map type management` configuration command. This command permits network management traffic by identifying the incoming IP management protocols that the ACE can receive as well as the client source host IP address and subnet mask as the matching criteria. A class map of type `management` provides access for one or more of the following management protocols: HTTP, HTTPS, ICMP, SNMP, SSH, or Telnet.

A class map can have multiple `match` commands. You can configure class maps to define multiple management protocol and source IP address commands in a group that you then associate with a traffic policy. The `match-all` and `match-any` keywords determine how the ACE evaluates multiple match statements operations when multiple match criteria exist in a class map.

The syntax of this command is:

```
class-map type management [match-all | match-any] map_name
```
The arguments and options are:

- **match-all | match-any**—(Optional) Determines how the ACE evaluates Layer 3 and Layer 4 network management traffic when multiple match criteria exist in a class map. The class map is considered a match if the match commands meet one of the following conditions:
  - **match-all**—(Default) All of the match criteria listed in the class map match the network traffic class in the class map (typically, the match commands of different types).
  - **match-any**—Only one of the match criteria listed in the class map matches the network traffic class in the class map (typically, the match commands of the same type).

- **map_name**—Specifies the name assigned to the class map. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

When you use the **class-map type management** command, you will access class map management configuration mode.

To classify the network management traffic received by the ACE, include one or more of the following commands to configure the match criteria for the class map:

- **description**—See the “Defining a Class Map Description” section
- **match protocol**—See the “Defining Network Management Access Match Criteria” section

You may include multiple **match protocol** commands in a class map.

For example, to permit ICMP packets from IP address 172.16.10.0 255.255.255.0 and allow global SSH access to the ACE, enter:

```
host1/Admin(config)# class-map type management match-any
MGMT-ACCESS_CLASS
host1/Admin(config-cmap-mgmt)# match protocol icmp source-address
172.16.10.0 255.255.255.0
host1/Admin(config-cmap-mgmt)# match protocol ssh any
```

To remove a Layer 3 and Layer 4 network management class map from the ACE, enter:

```
host1/Admin(config)# no class-map type management match-any
MGMT-ACCESS_CLASS
```
Defining Network Management Access Match Criteria

To configure the class map to identify the network management protocols that can be received by the ACE, use the `match protocol` command in class map management configuration mode. You configure the associated policy map to permit access to the ACE for the specified management protocols. As part of the network management access traffic classification, you also specify either a client source host IP address and subnet mask as the matching criteria or instruct the ACE to allow any client source address for the management traffic classification.

The syntax of this command is:

```
[line_number] match protocol { http | https | icmp | snmp | ssh | telnet | xml-https } { any | source-address ip_address mask }
```

- `line_number`—(Optional) Assists you in editing or deleting individual `match` commands. Enter an integer from 2 to 255 as the line number. You can enter `no line_number` to delete long `match` commands instead of entering the entire line. The line numbers do not dictate a priority or sequence for the `match` statements.
- `http`—Specifies the Hypertext Transfer Protocol (HTTP).
- `https`—Specifies secure (SSL) Hypertext Transfer Protocol (HTTP) for connectivity with the Device Manager GUI on the ACE.
- `icmp`—Specifies Internet Control Message Protocol messages to the ACE.
- `snmp`—Specifies the Simple Network Management Protocol (SNMP).
- `ssh`—Specifies a Secure Shell (SSH) remote connection to the ACE. The ACE supports the SSH remote shell functionality provided in SSH Version 1 and supports DES and 3DES ciphers.

  **Note**  
  SSH v1.x and v2 are entirely different protocols and are not compatible. Make sure that you use an SSH v1.x client when accessing the ACE.

- `telnet`—Specifies a Telnet remote connection to the ACE.
- `xml-https`—Specifies HTTPS as transfer protocol to send and receive XML documents between the ACE and a Network Management System (NMS).
- `any`—Specifies any client source address for the management traffic classification.
• **source-address**—Specifies a client source host IP address and subnet mask as the network traffic matching criteria. As part of the classification, the ACE implicitly obtains the destination IP address from the interface on which you apply the policy map.

• **ip_address**—Source IP address of the client. Enter the IP address in dotted-decimal notation (for example, 192.168.11.1).

• **mask**—The subnet mask of the client in dotted-decimal notation (for example, 255.255.255.0).

For example, to specify that the class map allows SSH access to the ACE from source IP address 192.168.10.1 255.255.255.0, enter:

```
host1/Admin(config)# class-map type management SSH-ALLOW_CLASS
host1/Admin(config-cmap-mgmt)# match protocol ssh source-address 192.168.10.1 255.255.255.0
```

To deselect the specified network management protocol match criteria from the class map, enter:

```
host1/Admin(config-cmap-mgmt)# no match protocol ssh source-address 192.168.10.1 255.255.255.0
```

## Configuring Layer 7 Class Maps

A Layer 7 class map contains match criteria that classifies specific Layer 7 protocol information. The match criteria enables the ACE to:

- Perform server load balancing based on an HTTP cookie, an HTTP header, an HTTP URL, protocol header fields, or source IP addresses
- Perform deep packet inspection of the HTTP protocol
- Perform FTP request command filtering

For more information about the role of class maps in the ACE, see the “Class Map and Policy Map Overview” section.

This section contains the following topics:

- Defining Layer 7 Classifications for HTTP Server Load Balancing
- Defining Layer 7 Classifications for HTTP Deep Packet Inspection
- Defining Layer 7 Classifications for FTP Command Inspection
Defining Layer 7 Classifications for HTTP Server Load Balancing

A Layer 7 HTTP server load-balancing class map contains match criteria that classifies specific Layer 7 network traffic. You create a Layer 7 server load-balancing class map based on HTTP cookies, HTTP headers, HTTP URLs, protocol header fields, or source IP addresses.

The Layer 7 HTTP server load balancing has the following features:

- Regular expression matching against the received packet data from a particular connection based on the cookie expression
- Regular expression matching against the received packet data from a particular connection based on the HTTP header expression
- Regular expression matching against the received packet data from a particular connection based on the HTTP URL string.
- Server load-balancing decisions based on a client source IP address
- Nesting of class maps to achieve complex logical expressions for Layer 7 HTTP-based server load balancing

To create a Layer 7 class map for HTTP server load balancing, use the `class-map type http loadbalance` command in configuration mode.

A single class map can have multiple `match` commands that you can use to specify the matching criteria. For example, you can configure a Layer 7 HTTP server load-balancing class map to define multiple URLs, cookies, and HTTP headers in a group that you then associate with a traffic policy. The `match-all` and `match-any` keywords determine how the ACE evaluates multiple match statements operations when multiple match criteria exist in a Layer 7 HTTP load-balancing class map.

The syntax of this command is:

```
class-map type http loadbalance [match-all | match-any] map_name
```
The arguments and options are:

- **match-all | match-any**—(Optional) Determines how the ACE evaluates Layer 7 HTTP server load-balancing operations when multiple match criteria exist in a class map. The class map is considered a match if the `match` commands meet one of the following conditions:

  - **match-all**—(Default) Network traffic needs to satisfy all of the match criteria (implicit AND) to match the Layer 7 load-balancing class map. The `match-all` keyword is applicable only for match statements of different Layer 7 load-balancing types. For example, specifying a `match-all` condition for URL, HTTP header, and URL cookie statements in the same class map is valid. However, specifying a `match-all` condition for multiple HTTP headers or multiple cookies with the same names or multiple URLs in the same class map is invalid.

  - **match-any**—Network traffic needs to satisfy only one of the match criteria (implicit OR) to match the HTTP load-balancing class map. The `match-any` keyword is applicable only for match statements of the same Layer 7 load-balancing type. For example, the ACE does not allow you to specify a `match-any` condition for URL, HTTP header, and URL cookie statements in the same class map but does allow you to specify a `match-any` condition for multiple URLs, or multiple HTTP headers or multiple cookies with different names in the same class map.

- **map_name**—Name assigned to the class map. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

When you use the `class-map type http loadbalance` command, you will access class map HTTP server load balancing configuration mode. For details on specifying the match criteria for a HTTP server load-balancing class map, see the *Cisco 4700 Series Application Control Engine Appliance Server Load-Balancing Configuration Guide*. 
Defining Layer 7 Classifications for HTTP Deep Packet Inspection

The ACE uses a Layer 7 class map for HTTP deep packet application protocol inspection. The ACE performs a stateful deep packet inspection of the HTTP protocol and permits or blocks traffic based on the actions in your configured policies.

HTTP deep packet inspection supports the following security features:

- RFC compliance monitoring and RFC method filtering
- Content, URL, and HTTP header length checks
- Transfer-encoding methods
- Content type verification and filtering
- Port 80 misuse
- URL logging

To create a Layer 7 class map to be used for the deep packet inspection of HTTP traffic through the ACE, use the `class-map type http inspect` command in configuration mode.

The syntax of this command is:

```
class-map type http inspect [match-all | match-any] map_name
```

The arguments and options are:

- `match-all | match-any`—(Optional) Determines how the ACE performs the deep packet inspection of HTTP traffic when multiple match criteria exist in a class map. The class map is considered a match if the `match` commands meet one of the following conditions:
  - `match-all`—(Default) Network traffic needs to satisfy all of the match criteria (implicit AND) to match the Layer 7 HTTP deep packet inspection class map. The `match-all` keyword is applicable only for match statements of different HTTP deep packet inspection types. For example, specifying a `match-all` condition for URL, HTTP header, and URL content statements in the same class map is valid. However, specifying a `match-all` condition for multiple HTTP headers with the same names or multiple URLs in the same class map is invalid.
– **match-any**—Network traffic needs to satisfy only one of the match criteria (implicit OR) to match the Layer 7 HTTP deep packet inspection class map. The **match-any** keyword is applicable only for match statements of the same Layer 7 HTTP deep packet inspection type. For example, the ACE does not allow you to specify a **match-any** condition for URL, HTTP header, and URL content statements in the same class map but does allow you to specify a **match-any** condition for multiple URLs, multiple HTTP headers, or multiple URL content statements with different names in the same class map.

- **map_name**—Name assigned to the class map. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

When you use the **class-map type http inspect** command, you will access class map HTTP inspection configuration mode. For details on specifying the match criteria for the HTTP application protocol inspection class map, see the *Cisco 4700 Series Application Control Engine Appliance Security Configuration Guide*.

### Defining Layer 7 Classifications for FTP Command Inspection

The ACE uses a Layer 7 FTP command class map to perform an FTP request inspection for FTP sessions, allowing you to restrict specific commands by the ACE. You can use this function to prevent web browsers from sending embedded commands to the ACE in FTP requests. The ACE must acknowledged each specified FTP command before it allows a new command.

To create a Layer 7 class map to be used for the inspection of FTP request commands, use the **class-map type ftp inspect** command in configuration mode.

The syntax of this command is:

```
class-map type ftp inspect match-any map_name
```

The keywords and arguments are:

- **match-any**—Specifies only one of the match criteria listed in the class map is satisfied to match the FTP command inspection class in the class map.

- **map_name**—Name assigned to the class map. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

When you use the **class-map type ftp inspect** command, you will access class map FTP inspection configuration mode. For details on specifying the match criteria for the FTP command inspection class map, see the *Cisco 4700 Series Application Control Engine Appliance Security Configuration Guide*. 
Configuring a Layer 3 and Layer 4 Policy Map

For a Layer 3 and Layer 4 traffic classification, you create a Layer 3 and Layer 4 policy map with actions to configure the following tasks:

- Network management traffic received by the ACE (HTTP, HTTPS, ICMP, SSH, or Telnet)
- Server load balancing
- Application acceleration and optimization
- SSL security services between a web browser (the client) and the HTTP connection (the server)
- Static or dynamic NATs
- HTTP deep packet inspection
- FTP command inspection
- Application protocol inspection
- IP, TCP, HTTP, and UDP connection behavior

For more information about the role of policy maps in the ACE, see the “Class Map and Policy Map Overview” section.

This section outlines the general steps to configure a Layer 3 and Layer 4 network traffic policy and contains the following topics:

- Creating a Layer 3 and Layer 4 Policy Map for Network Management Traffic Received by the ACE
- Creating a Layer 3 and Layer 4 Policy Map for Network Traffic Passing Through the ACE
- Defining a Layer 3 and Layer 4 Policy Map Description
- Specifying a Layer 3 and Layer 4 Traffic Class With the Traffic Policy
- Specifying Layer 3 and Layer 4 Policy Actions
- Using Parameter Maps in a Layer 3 and Layer 4 Policy Map
Creating a Layer 3 and Layer 4 Policy Map for Network Management Traffic Received by the ACE

To configure a Layer 3 and Layer 4 policy map that defines the different actions that are applied to the IP management traffic received by the ACE, use the `policy-map type management first-match` configuration command. The ACE executes the specified action only for traffic that meets the first matching classification with a policy map. The ACE does not execute any additional actions.

The syntax of this command is:

```
policy-map type management first-match map_name
```

The `map_name` argument specifies the name assigned to the Layer 3 and Layer 4 network management policy map. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

When you use this command, you will access policy map management configuration mode.

For example, to create a Layer 3 and Layer 4 network traffic management policy map, enter:

```
host1/Admin(config)# policy-map type management first-match L4_MGMT_POLICY
host1/Admin(config-pmap-mgmt)#
```

To remove a network traffic management policy map from the ACE, enter:

```
host1/Admin(config)# no policy-map type management first-match L4_MGMT_POLICY
```
Creating a Layer 3 and Layer 4 Policy Map for Network Traffic Passing Through the ACE

To configure a Layer 3 and Layer 4 policy map that defines the different actions applied to traffic that passes through the ACE, use the `policy-map multi-match` configuration command. The ACE attempts to match multiple classes within the Layer 3 and Layer 4 policy map to allow for multi-feature policies. The ACE executes the action for only one matching class within each of the class sets. The definition of which classes are in the same class set depends on the actions applied to the classes; the ACE associates each policy map action with a specific set of classes.

The syntax of this command is:

```
policy-map multi-match map_name
```

The `map_name` argument specifies the name assigned to the policy map. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

When you use this command, you will access policy map configuration mode.

For example, to create a Layer 3 and Layer 4 application protocol inspection policy map, enter:

```
host1/Admin(config)# policy-map multi-match L4_HTTP_APP_INSPECTION_POLICY
host1/Admin(config-pmap)#
```

To remove a policy map from the ACE, enter:

```
host1/Admin(config)# no policy-map multi-match L4_HTTP_APP_INSPECTION_POLICY
```

Defining a Layer 3 and Layer 4 Policy Map Description

To provide a brief summary about the Layer 3 and Layer 4 policy map, use the `description` command in policy map configuration mode.

The syntax of this command is:

```
description text
```
The text argument specifies the description that you want to provide. Enter an unquoted text string with a maximum of 240 alphanumeric characters.

For example, to specify a description that the policy map is to filter network traffic to a VIP, enter:

```
host1/Admin(config-pmap)# description filter traffic matching a VIP
```

To remove the description from the class map, enter:

```
host1/Admin(config-pmap)# no description
```

### Specifying a Layer 3 and Layer 4 Traffic Class With the Traffic Policy

To specify a Layer 3 and Layer 4 traffic class created with the class-map command to associate network traffic with the traffic policy, use the class command in policy map configuration mode.

The syntax of this command is:

```
class map_name
```

*The map_name* argument specifies the name of a previously defined Layer 3 and Layer 4 traffic class, configured with the class-map command, to associate traffic to the traffic policy. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

When you use this command, you will access policy map class configuration mode.

For example, to specify an existing class map within the Layer 3 and Layer 4 policy map, enter:

```
host1/Admin(config-pmap)# class L4_SLB_VIP_CLASS
host1/Admin(config-pmap-c)#
```

To remove a class map from a Layer 3 and Layer 4 policy map, enter:

```
host1/Admin(config-pmap)# no class L4_SLB_VIP_CLASS
```

To manually insert the class map ahead of a previously specified class map, use the class command with the insert-before keyword. However, the ACE does not save this reordering as part of the configuration.
The syntax of the class command with the optional `insert-before` keyword is:

```
class map_name1 insert-before map_name2
```

When you use this command, the ACE places the current class map (as specified by the `map_name1` argument) ahead of an existing class map (as specified by the `map_name2` argument).

For example, to define the sequential order of two class maps in the policy map, enter:

```
host1/Admin(config-pmap-c)# class L4_HTTP_APP_INSPECTION_CLASS
insert-before L4_SLB_VIP_CLASS
```

To specify the class-default class map for the Layer 3 and Layer 4 traffic policy, use the `class class-default` command in policy map configuration mode. All network traffic that fails to meet the other matching criteria in the named class map belongs to the default traffic class. If none of the specified classifications match, the ACE then matches the action specified under the `class class-default` command. The class-default class map has an implicit match any statement in it and is used to match any traffic classification.

When you use this command, you will access policy map class configuration mode.

For example, to use the `class class-default` command, enter:

```
host1/Admin(config-pmap)# class class-default
host1/Admin(config-pmap-c)# loadbalance vip replicate-connections
```

**Specifying Layer 3 and Layer 4 Policy Actions**

To allow the network management traffic listed in the Layer 3 and Layer 4 class map to be received or rejected by the ACE, specify either the `permit` or `deny` command in policy map class configuration mode.

- Use the `permit` command in policy map class configuration mode to allow the remote network management protocols listed in the class map to be received by the ACE.

- Use the `deny` command in policy map class configuration mode to refuse the remote network management protocols listed in the class map to be received by the ACE.
For example, to create a Layer 3 and Layer 4 traffic management policy map that permits ICMP and SSH connections to be received by the ACE, enter:

```
host1/Admin(config)# policy-map type management first-match L4_MGMT_POLICY
host1/Admin(config-pmap-mgmt)# class ICMP_CLASS
host1/Admin(config-pmap-mgmt-c)# permit
host1/Admin(config-pmap-mgmt-c)# exit
host1/Admin(config-pmap-mgmt)# class SSH_CLASS
host1/Admin(config-pmap-mgmt-c)# permit
host1/Admin(config-pmap-mgmt-c)# exit
```

To specify the different policy map actions that you want applied to the Layer 3 and Layer 4 network traffic that passes through the ACE, see the appropriate ACE document and chapter as outlined in Table 4-9. Table 4-9 defines the associated actions for the different Layer 3 and Layer 4 network traffic policies based on the function of the Layer 3 and Layer 4 policy map.

For example, to specify server load-balancing actions for the Layer 3 and Layer 4 policy map, enter:

```
host1/Admin(config-pmap)# class L4_SLB_CLASS
host1/Admin(config-pmap-c)# loadbalance vip inservice
host1/Admin(config-pmap-c)# loadbalance policy L7SLBPOLICY
host1/Admin(config-pmap-c)# exit
```

<table>
<thead>
<tr>
<th>Layer 3 and Layer 4 Policy Map/Actions</th>
<th>Document</th>
<th>Chapter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application acceleration and optimization</td>
<td>Cisco 4700 Series Application Control Engine Appliance Application Acceleration and Optimization Configuration Guide</td>
<td>Chapter 4, Configuring a Traffic Policy for HTTP Optimization</td>
</tr>
<tr>
<td>Secure Sockets Layer (SSL) security services</td>
<td>Cisco 4700 Series Application Control Engine Appliance SSL Configuration Guide</td>
<td>Chapter 3, Configuring SSL Termination and Chapter 4, Configuring SSL Initiation</td>
</tr>
</tbody>
</table>
Table 4-9   Layer 3 and Layer 4 Policy Map Actions and Related Documentation (continued)

<table>
<thead>
<tr>
<th>Layer 3 and Layer 4 Policy Map/Actions</th>
<th>Document</th>
<th>Chapter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection redundancy</td>
<td><em>Cisco 4700 Series Application Control Engine Appliance Administration Guide</em> (this book)</td>
<td>Chapter 7, Configuring Redundant ACE Modules</td>
</tr>
<tr>
<td>Application protocol inspection</td>
<td><em>Cisco 4700 Series Application Control Engine Appliance Security Configuration Guide</em></td>
<td>Chapter 3, Configuring Application Protocol Inspection</td>
</tr>
<tr>
<td>Static or dynamic NATs</td>
<td><em>Cisco 4700 Series Application Control Engine Appliance Security Configuration Guide</em></td>
<td>Chapter 5, Configuring Network Address Translation</td>
</tr>
<tr>
<td>IP, TCP, and UDP connection behavior</td>
<td><em>Cisco 4700 Series Application Control Engine Appliance Security Configuration Guide</em></td>
<td>Chapter 4, Configuring TCP/IP Normalization and IP Reassembly Parameters</td>
</tr>
</tbody>
</table>

Using Parameter Maps in a Layer 3 and Layer 4 Policy Map

To combine related actions for TCP, IP, HTTP, or UDP connections in a Layer 3 and Layer 4 policy map, create one or more parameter maps for use with the ACE. The ACE supports the following Layer 3 and Layer 4 parameter map types:

- **parameter-map type connection** *map_name*—Combines all TCP and IP connection-related parameters pertaining to TCP normalization, termination, and server re-use as well as IP normalization, fragmentation, and reassembly. See the *Cisco 4700 Series Application Control Engine Appliance Security Configuration Guide* for details.

- **parameter-map type http**—Configures advanced HTTP behavior for HTTP load-balanced connections. See the *Cisco 4700 Series Application Control Engine Appliance Server Load-Balancing Configuration Guide* for details.

- **parameter-map type http**—Configures advanced HTTP behavior for HTTP deep packet inspection. See the *Cisco 4700 Series Application Control Engine Appliance Security Configuration Guide* for details.
- **parameter-map type udp**—Combines all UDP connection related configuration parameters. See the *Cisco 4700 Series Application Control Engine Appliance Security Configuration Guide* for details.

To specify the SSL session parameters that the ACE uses in an SSL proxy service, you can create an SSL parameter map. Use the **parameter-map type ssl** command to specify SSL termination parameters. Refer to the *Cisco 4700 Series Application Control Engine Appliance SSL Configuration Guide* for details.

For example, to specify the **parameter-map type connection** command to combine TCP connection-related parameters in a parameter map, enter:

```plaintext
host1/Admin(config)# parameter-map type connection TCP_MAP
host1/Admin(config-parammap-conn)# reserved-bit allow
host1/Admin(config-parammap-conn)# exceed-mss allow
host1/Admin(config-parammap-conn)# nagle
host1/Admin(config-parammap-conn)# set conn-max 64
host1/Admin(config-parammap-conn)# set tcp queue-limit 10
host1/Admin(config-parammap-conn)# set tcp syn-retry 3
host1/Admin(config-parammap-conn)# set tcp timeout embryonic 60
host1/Admin(config-parammap-conn)# exit
host1/Admin(config)#
host1/Admin(config)# policy-map multi-match L4_SLB_POLICY
host1/Admin(config-pmap)# class VIP_CLASS
host1/Admin(config-pmap-c)# loadbalance policy L7_SLB_POLICY
host1/Admin(config-pmap-c)# loadbalance vip inservice
host1/Admin(config-pmap-c)# connection advanced-options TCP-MAP
host1/Admin(config-pmap-c)# exit
host1/Admin(config-pmap)# exit
host1/Admin(config)#
```

### Configuring a Layer 7 Policy Map

To use a Layer 7 policy map, you must first create the Layer 7 policy map. For a Layer 7 traffic classification, you create a policy map with actions to configure the following tasks:

- HTTP content load-balancing decisions
- Application acceleration and optimization
- Deep packet inspection of the HTTP protocol
- FTP command inspection
You associate the Layer 7 policy map within the appropriate Layer 3 and Layer 4 policy map to provide an entry point for the traffic classification. Layer 7 policy maps are considered to be child policies and can only be associated within a Layer 3 and Layer 4 policy map. Only a Layer 3 and Layer 4 policy map can be activated on a VLAN interface; a Layer 7 policy map cannot be directly applied on an interface.

For more information about the role of policy maps in the ACE, see the “Class Map and Policy Map Overview” section.

This section describes how to configure a Layer 7 traffic policy and contains the following topics:

- Creating a Layer 7 Policy Map
- Adding a Layer 7 Policy Map Description
- Including Inline Match Statements in a Layer 7 Policy Map
- Specifying a Layer 7 Traffic Class with the Traffic Policy
- Specifying Layer 7 Policy Actions
- Associating the Layer 7 Policy Map with a Layer 3 and Layer 4 Policy Map

### Creating a Layer 7 Policy Map

To specify the type of Layer 7 traffic policy map, use the `policy-map type` command in configuration mode. The syntax of this command is:

```
policy-map type {loadbalance first-match | inspect http all-match | inspect ftp first-match | optimization http first-match} map_name
```

The keywords and arguments are:

- **loadbalance first-match**—Defines Layer 7 server load-balancing decisions. You will enter policy map load balancing configuration mode. The ACE executes the specified action only for traffic that meets the first matching load-balancing classification with a policy map. The ACE does not execute any additional actions.

- **inspect http all-match**—Defines the deep inspection of HTTP traffic. You will enter policy map HTTP inspection configuration mode. The ACE attempts to match a packet against all classes in the policy map and executes the actions of all matching classes associated with the policy map.
• **inspect ftp first-match**—Configures the inspection of FTP request commands by the ACE. You will enter policy map FTP inspection configuration mode. The ACE executes the specified deny or mask-reply action only for traffic that meets the first matching FTP request command inspection classification with a policy map. The ACE does not execute any additional actions.

• **optimization http first-match**—Defines the application acceleration and optimization operations to be performed by the ACE. You will enter policy map optimization configuration mode. The ACE executes the specified action only for traffic that meets the first matching optimization classification with a policy map. The ACE does not execute any additional actions.

• **map_name**—Specifies the name assigned to the policy map. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

---

**Note**

You can include multiple Layer 7 load balancing or FTP class maps within the policy map; however, the match operation of the ACE in this configuration is to always perform a “first-match” on the specified class maps. If none of the class maps within the policy map match, and you include the class-default class map, the ACE will match the traffic classification.

For example, to create a Layer 7 load-balancing policy map, enter:

```
host1/Admin(config)# policy-map type loadbalance first-match L4_SLB_POLICY
host1/Admin(config-pmap-lb)#
```

To remove a policy map from the ACE, enter:

```
host1/Admin(config)# no policy-map type loadbalance first-match L4_SLB_POLICY
```
Adding a Layer 7 Policy Map Description

To provide a brief summary about the Layer 7 policy map, use the `description` command in policy map configuration mode.

The syntax of this command is:

```
description text
```

The `text` argument specifies the description that you want to provide. Enter an unquoted text string with a maximum of 240 alphanumeric characters.

For example, to add a description that the policy map is to perform HTTP deep packet inspection, enter:

```
host1/Admin(config-pmap-ins-http)# description HTTP protocol deep inspection of incoming traffic
```

To remove the description from the policy map, enter:

```
host1/Admin(config-pmap-ins-http)# no description
```

Including Inline Match Statements in a Layer 7 Policy Map

To include a single inline match criterion in the policy map without specifying a traffic class, enter an applicable Layer 7 `match` command. The inline Layer 7 policy map `match` commands function similarly to the Layer 7 class map `match` commands. This difference is that when you use an inline `match` command, you can specify an action for only a single match statement in the Layer 7 policy map.

```
match name match_statement [insert-before map_name]
```

Note

To specify actions for multiple match statements, use a class map as described in the “Specifying a Layer 7 Traffic Class with the Traffic Policy” section.
The arguments are:

- **name**—Name assigned to the inline `match` command. Enter an unquoted text string with no spaces. The length of the inline match statement name plus the length of the policy map name with which it is associated cannot exceed a total maximum of 64 alphanumeric characters. For example, if the policy map name is L7_POLICY (nine characters), an inline match statement name under this policy cannot exceed 55 alphanumeric characters (64 - 9 = 55).

- **match_statement**—Inline match criteria to be used by the policy map.

- **insert-before map_name**—(Optional) Places the inline `match` command ahead of an existing class map in the policy map configuration.

For example:

```
host1/Admin(config-pmap-lb)# match L7loadbalance http url /finance
host1/Admin(config-pmap-lb-m)# serverfarm FARM1
host1/Admin(config-pmap-lb-m)# class TEST_CLASS
host1/Admin(config-pmap-lb-m)# serverfarm FARM2
```

### Specifying a Layer 7 Traffic Class with the Traffic Policy

To specify a traffic class created with the `class-map` command to associate network traffic with the traffic policy, use the `class` command in policy map configuration mode. The syntax of this command is:

```
class map_name
```

The `map_name` argument specifies the name of a previously defined traffic class, configured with the `class-map` command, to associate traffic to the traffic policy. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

When you use this command, you will access policy map class configuration mode.

For example, to specify an existing class map in the Layer 7 policy map, enter:

```
host1/Admin(config-pmap-lb)# class L7_SLB_SERVER_CLASS
host1/Admin(config-pmap-lb-c)#
```

To remove a class map from a Layer 7 policy map, enter:

```
host1/Admin(config-pmap-lb)# no class L7_SLB_SERVER_CLASS
```
To manually insert a class map ahead of a previously specified class map, use the `class` command with the `insert-before` keyword. Note that the ACE does not save this sequence reordering as part of the configuration.

The syntax of the class command with the `insert-before` keyword is:

```
class map_name1 insert-before map_name2
```

When you use this command, the ACE places the current class map (as specified by the `map_name1` argument) ahead of an existing class map (as specified by the `map_name2` argument).

For example, to define the sequential order of two class maps in the policy map, enter:

```
host1/Admin(config-pmap-lb-c)# class L7_HTTP_SLB_CLASS insert-before L7_SLB_SERVER_CLASS
```

To specify the class-default class map for the traffic policy, use the `class class-default` command in policy map configuration mode. All traffic that fails to meet the other matching criteria in the named class map belongs to the default traffic class. If none of the specified classifications match, the ACE then matches the action specified under the `class class-default` command. The class-default class map has an implicit match any statement in it and is used to match any traffic classification.

When you use this command, you will access policy map class configuration mode.

For example, to use the `class class-default` command, enter:

```
host1/Admin(config-pmap)# class class-default
host1/Admin(config-pmap-lb-c)# insert-http Host
```

### Specifying Layer 7 Policy Actions

To specify the policy map actions that you want applied to the Layer 7 policy map, see the appropriate ACE document and chapter as outlined in Table 4-10. Table 4-10 defines the associated actions for the different Layer 7 application policies based on the function of the Layer 7 policy map.
For example, to specify an server farm action in the Layer 7 load-balancing policy map, enter:

```
host1/Admin(config)# policy-map type loadbalance first-match L7_SLB_POLICY
host1/Admin(config-pmap-lb)# class SPORTS-MAP_CLASS
host1/Admin(config-pmap-lb-c)# serverfarm SPORTS-SERVER
host1/Admin(config-pmap-lb-c)# exit
host1/Admin(config-pmap-lb)# class SPORTS-MAP_CLASS
host1/Admin(config-pmap-lb-c)# serverfarm NEWS-SERVER
host1/Admin(config-pmap-lb-c)# exit
host1/Admin(config-pmap-lb)# class-default
host1/Admin(config-pmap-lb-c)# serverfarm SERVER-HANDLE-ALL
host1/Admin(config-pmap-lb-c)# exit
```

To disable an action from the Layer 7 load-balancing policy map, enter:

```
host1/Admin(config-pmap-lb-c)# no serverfarm SERVER-HANDLE-ALL
```

### Table 4-10 Layer 7 Policy Map Actions and Related Documentation

<table>
<thead>
<tr>
<th>Layer 7 Policy Map/Actions</th>
<th>Document</th>
<th>Chapter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application acceleration and optimization</td>
<td><em>Cisco 4700 Series Application Control Engine Appliance Application Acceleration and Optimization Configuration Guide</em></td>
<td>Chapter 4, Configuring a Traffic Policy for HTTP Optimization</td>
</tr>
<tr>
<td>Secure Sockets Layer (SSL) security services</td>
<td><em>Cisco 4700 Series Application Control Engine Appliance SSL Configuration Guide</em></td>
<td>Chapter 3, Configuring SSL Termination and Chapter 4, Configuring SSL Initiation</td>
</tr>
<tr>
<td>HTTP application protocol inspection</td>
<td><em>Cisco 4700 Series Application Control Engine Appliance Security Configuration Guide</em></td>
<td>Chapter 3, Configuring Application Protocol Inspection</td>
</tr>
<tr>
<td>FTP command inspection</td>
<td><em>Cisco 4700 Series Application Control Engine Appliance Security Configuration Guide</em></td>
<td>Chapter 3, Configuring Application Protocol Inspection</td>
</tr>
</tbody>
</table>
Associating the Layer 7 Policy Map with a Layer 3 and Layer 4 Policy Map

When you use the `policy-map multi-match` command in configuration mode, you can associate the following Layer 7 policy maps with a Layer 3 and Layer 4 policy map:

- To associate a Layer 7 HTTP server load-balancing policy map, nest the load-balancing policy map by using the Layer 3 and Layer 4 `loadbalance` policy command.
- To associate a Layer 7 optimization HTTP policy map, nest the optimization policy map by using the Layer 3 and Layer 4 `optimize http policy` command.
- To associate a Layer 7 HTTP application inspection policy map, nest the HTTP application traffic policy by using the Layer 3 and Layer 4 `inspect http policy` command.
- To associate a Layer 7 FTP command inspection policy map, nest the FTP command inspection traffic policy by using the Layer 3 and Layer 4 `inspect ftp policy` command.

See the “Configuring a Layer 3 and Layer 4 Policy Map” section and the documents listed in Table 4-9 for the specific procedure to create a Layer 3 and Layer 4 policy map that associates a Layer 7 HTTP server load balancing, HTTP deep packet inspection, or FTP command inspection policy map.

For example, to nest the Layer 7 L7_SLB_POLICY policy map within the Layer 3 and Layer 4 L4_SLB_POLICY policy map, enter:

```
host1/Admin(config)# policy-map type loadbalance first-match L7_SLB_POLICY
host1/Admin(config-pmap-lb)# class L7_SLB_CLASS
host1/Admin(config-pmap-lb-c)# serverfarm FARM2 backup FARM3 sticky
host1/Admin(config-pmap-lb-c)# exit
host1/Admin(config-pmap-lb)# exit
host1/Admin(config)# policy-map multi-match L4_SLB_POLICY
host1/Admin(config-pmap)# class L4_SLB_CLASS
host1/Admin(config-pmap-c)# loadbalance policy L7_SLB_POLICY
```
Applying a Service Policy

The `service-policy` command allows you to perform the following tasks:

- Apply a previously created policy map.
- Attach the traffic policy to a specific VLAN interface or globally to all VLAN interfaces in the same context.
- Specify that the traffic policy is to be attached to the input direction of an interface.

The `service-policy` command is available at both interface configuration mode and configuration mode. Specifying a Layer 3 and Layer 4 policy map in interface configuration mode applies the policy map to the specified VLAN interface. Specifying a policy map in configuration mode applies the policy to all of the VLAN interfaces associated with a context.

The syntax of this command is:

```
service-policy input policy_name
```

The keywords, arguments, and options are:

- `input`—Specifies that the traffic policy is to be attached to the input direction of an interface. The traffic policy evaluates all traffic received by that interface.
- `policy_name`—Specifies the name of a previously defined policy map, configured with a previously created `policy-map` command. The name can be a maximum of 40 alphanumeric characters.

For example, to specify an interface VLAN and apply multiple service policies to the VLAN, enter:

```
host1/Admin(config)# interface vlan 50
host1/Admin(config-if)# ip address 172.16.1.100 255.255.255.0
host1/Admin(config-if)# service-policy input L4_SLB_POLICY
host1/Admin(config-if)# service-policy input REMOTE_MGMT_ALLOW_POLICY
```

For example, to globally apply multiple service policies to all VLANs associated with the context, enter:

```
host1/Admin(config)# service-policy input L4_SLB_POLICY
host1/Admin(config)# service-policy input REMOTE_MGMT_ALLOW_POLICY
```
To detach a traffic policy from an interface VLAN, enter:

```
host1/Admin(config-if)# no service-policy input L4_SLB_POLICY
```

To globally detach a traffic policy from all VLANs associated with a context, enter:

```
host1/Admin(config)# no service-policy input L4_SLB_POLICY
```

You can detach a traffic policy by one of these methods:

- Individually from the last VLAN interface on which you applied the service policy
- Globally from all VLAN interfaces in the same context

When you detach a policy, the ACE automatically resets the associated service policy statistics to provide a new starting point for the service policy statistics the next time that you attach a traffic policy to a specific VLAN interface or globally to all VLAN interfaces in the same context.

The following guidelines and restrictions apply when you create a service policy:

- Policy maps, applied globally in a context, are internally applied on all interfaces associated with the context.
- A policy activated on a VLAN interface overwrites any specified global policies for overlapping classification and actions.
- The ACE allows only one policy of a specific feature type to be activated on a VLAN interface.
Class Maps and Policy Map Examples

This section includes a series of examples that will show you how to use class maps and policy maps to perform various operations on the ACE. This section contains the following examples:

- Firewall Example
- Layer 7 Load-Balancing Example
- Layer 3 and Layer 4 Load-Balancing Example
- VIP With Connection Parameters Example

Firewall Example

This example shows how to create a firewall traffic policy (for inside interface VLAN50) that enables the following processes to occur on the ACE:

- Permits ICMP packets from IP address 172.16.10.0 255.255.255.254.
- Permits SSH access to the ACE.
- Includes an ACL that allows the ACE to receive any HTTP traffic through the VLAN.
- Filters on content to allow only HTTL headers that contain the “html” expression.
- Filters a subset of the HTTP traffic using a content filtering rule that permits the following packet types:
  - With an HTTP header length of 255 or less
  - Without the string “BAD” included in the URL
To create a series of class maps and policy maps to classify and permit the identified traffic, perform the following steps:

---

**Step 1** Permit ICMP packets from IP address 172.16.10.0 255.255.255.254 and allow global SSH access to the ACE by entering the following commands:

```plaintext
host1/Admin(config)# class-map type management ICMP-ALLOW_CLASS
host1/Admin(config-cmap-mgmt)# match protocol icmp source-address 172.16.10.0 255.255.255.254
host1/Admin(config-cmap-mgmt)# exit

host1/Admin(config)# class-map type management SSH-ALLOW_CLASS
host1/Admin(config-cmap-mgmt)# match protocol ssh any
host1/Admin(config-cmap-mgmt)# exit

host1/Admin(config)# policy-map type management first-match L4_MGMT_POLICY
host1/Admin(config-pmap-mgmt)# class ICMP-ALLOW_CLASS
host1/Admin(config-pmap-mgmt-c)# permit
host1/Admin(config-pmap-mgmt-c)# exit
host1/Admin(config-pmap-mgmt)# class SSH-ALLOW_CLASS
host1/Admin(config-pmap-mgmt-c)# permit
host1/Admin(config-pmap-mgmt-c)# exit
host1/Admin(config-pmap-mgmt)# exit
```

**Step 2** Create a class map to filter HTTP traffic to include an ACL that allows the ACE to receive any HTTP traffic through the VLAN by entering the following commands:

```plaintext
host1/Admin(config)# access-list 200 extended permit tcp any any eq http
host1/Admin(config)# class-map match-all L4_FILTERHTTP_CLASS
host1/Admin(config-cmap)# match access-list 200
```

**Step 3** Define the following Layer 7 class maps and policy maps to filter on content and allow HTTL headers that contain the “html” expression:

a. Identify HTTP headers that contain the “html” expression with a header length of 255 or less by entering the following commands:

```plaintext
host1/Admin(config)# class-map type http inspect match-all L7_FLTRHTML1_CLASS
host1/Admin(config-cmap-http-insp)# match header accept header-value html
host1/Admin(config-cmap-http-insp)# match header length request eq 255
```
host1/Admin(config-cmap-http-insp)# exit
host1/Admin(config)#

b. Reject URLs containing the “BAD” string by entering the following commands:

host1/Admin(config)# class-map type http inspect L7_FLTRHTML2_CLASS
host1/Admin(config-cmap-http-insp)# match url BAD
host1/Admin(config-cmap-http-insp)# exit
host1/Admin(config)#

c. Create a Layer 7 HTTP application inspection policy by entering the following commands:

host1/Admin(config)# policy-map type inspect http all-match L7_FILTERHTML_POLICY
host1/Admin(config-pmap-ins-http)# class L7_FLTRHTML1_CLASS
host1/Admin(config-pmap-ins-http-c)# permit
host1/Admin(config-pmap-ins-http-c)# exit
host1/Admin(config-pmap-ins-http)# class L7_FLTRHTML2_CLASS
host1/Admin(config-pmap-ins-http-c)# reset
host1/Admin(config-pmap-ins-http-c)# exit

Step 4 Create a Layer 3 and Layer 4 policy map to activate the traffic classifications outlined in the previous steps by entering the following commands:

host1/Admin(config)# policy-map multi-match L4_FILTER_POLICY
host1/Admin(config-pmap)# class L4_FILTERHTTP_CLASS
host1/Admin(config-pmap-c)# inspect http policy L7_FILTERHTML_POLICY
host1/Admin(config-pmap-c)# exit
host1/Admin(config-pmap)# exit
host1/Admin(config)#

Step 5 Apply the completed policies to interface VLAN 50 by entering the following commands:

host1/Admin(config)# interface vlan 50
host1/Admin(config-if)# ip address 172.16.1.100 255.255.255.0
host1/Admin(config-if)# service-policy input L4_MGMT_POLICY
host1/Admin(config-if)# service-policy input L4_FILTER_POLICY
Layer 7 Load-Balancing Example

This example shows how to create a Layer 7 load-balancing traffic policy that enables the following processes to occur on the ACE:

- Load balances traffic to the SPORTS-SERVER and NEWS-SERVER server farms based on the following criteria:
  - HTTP header and header value expression
  - URL expression
- Classifies the 3-tuple flow of the VIP address, protocol, and port as matching criteria for server load balancing
- Utilizes an HTTP parameter map to enable HTTP persistence

Perform the following steps:

---

**Step 1**  Create a Layer 7 class map that defines an HTTP header and header value expression string and URL expression for load balancing to the SPORTS-SERVER server farm.

```
host1/Admin(config)# class-map type http loadbalance match-all SPORTS-MAP_CLASS
host1/Admin(config-cmap-http-lb)# match http header host header-value .*test.com
host1/Admin(config-cmap-http-lb)# match http url /sports/
host1/Admin(config-cmap-http-lb)# exit
```

**Step 2**  Create a Layer 7 class map that defines a URL expression for load balancing to the NEWS-SERVER server farm.

```
host1/Admin(config)# class-map type http loadbalance NEWS-MAP_CLASS
host1/Admin(config-cmap-http-lb)# match http url /news/
host1/Admin(config-cmap-http-lb)# exit
```

**Step 3**  Create a Layer 7 server load-balancing policy by entering the following commands:

```
host1/Admin(config)# policy-map type loadbalance first-match L7_SLB_POLICY
host1/Admin(config-pmap-lb)# class SPORTS-MAP_CLASS
host1/Admin(config-pmap-lb-c)# serverfarm SPORTS-SERVER
host1/Admin(config-pmap-lb-c)# exit
host1/Admin(config-pmap-lb)# class NEWS-MAP_CLASS
host1/Admin(config-pmap-lb-c)# serverfarm NEWS-SERVER
host1/Admin(config-pmap-lb-c)# exit
```
Step 4  Create a Layer 3 and Layer 4 class map that classifies the 3-tuple flow of the VIP address, protocol, and port as matching criteria for server load balancing by entering the following commands:

```
host1/Admin(config)# class-map L4_SLBVIP_CLASS
host1/Admin(config-cmap)# match virtual-address 192.168.5.10 tcp port eq 80
host1/Admin(config-cmap)# exit
host1/Admin(config)#
```

Step 5  Create an HTTP parameter map to enable HTTP persistence by entering the following commands:

```
host1/Admin(config)# parameter-map type http HTTP_PARAMETER_MAP
host1/Admin(config-parammap-http)# persistent-rebalance
host1/Admin(config-parammap-http)# exit
host1/Admin(config)#
```

Step 6  Create a Layer 3 and Layer 4 policy map to activate the traffic classifications outlined in the previous steps by entering the following commands:

```
host1/Admin(config)# policy-map multi-match L4_SLB_POLICY
host1/Admin(config-pmap)# class L4_SLBVIP_CLASS
host1/Admin(config-pmap-c)# loadbalance policy L7_SLB_POLICY
host1/Admin(config-pmap-c)# loadbalance vip inservice
host1/Admin(config-pmap-c)# appl-parameter http advanced-options HTTP_PARAMETER_MAP
host1/Admin(config-pmap-c)# exit
host1/Admin(config-pmap)# exit
host1/Admin(config)#
```

Step 7  Apply the completed policies to interface VLAN 10 by entering the following commands:

```
host1/Admin(config)# interface VLAN 10
host1/Admin(config-if)# service-policy input L4_SLB_POLICY
```
Layer 3 and Layer 4 Load-Balancing Example

This example shows how to create a Layer 3 and 4 load-balancing traffic policy that enables the following processes to occur on the ACE:

- Load balances traffic to the SERVER-HANDLE-ALL server farm
- Classifies the 3-tuple flow of VIP address, protocol, and port as matching criteria for server load balancing

Perform the following steps:

**Step 1** Create a Layer 7 server load-balancing policy by entering the following commands:

```sh
host1/Admin(config)# policy-map type loadbalance first-match L7_SLB_POLICY
host1/Admin(config-pmap-lb)# class class-default
host1/Admin(config-pmap-lb-c)# serverfarm SERVER-HANDLE-ALL
host1/Admin(config-pmap-lb-c)# exit
host1/Admin(config-pmap-lb)# exit
host1/Admin(config)#
```

**Step 2** Create a Layer 3 and Layer 4 class map that classifies the 3-tuple flow of the VIP address, protocol, and port as matching criteria for server load balancing by entering the following commands:

```sh
host1/Admin(config)# class-map L4_SLBVIP_CLASS
host1/Admin(config-cmap)# match virtual-address 192.168.5.10 tcp port any
host1/Admin(config-cmap)# exit
host1/Admin(config)#
```

**Step 3** Create a Layer 3 and Layer 4 policy map to activate the traffic classifications outlined in the previous steps by entering the following commands:

```sh
host1/Admin(config)# policy-map multi-match L4_SLB_POLICY
host1/Admin(config-pmap)# class L4_SLBVIP_CLASS
host1/Admin(config-pmap-c)# loadbalance policy L7_SLB_POLICY
host1/Admin(config-pmap-c)# loadbalance vip inservice
host1/Admin(config-pmap-c)# exit
host1/Admin(config-pmap)# exit
host1/Admin(config)#
```
Step 4  
Apply the completed policies to interface VLAN 10 by entering the following commands:

```plaintext
host1/Admin(config)# interface VLAN 10
host1/Admin(config-if)# service-policy input L4_SLB_POLICY
```

---

**VIP With Connection Parameters Example**

This example creates a Layer 3 and 4 traffic policy that enables the following processes to occur on the ACE:

- Load balances traffic to the SERVER-HANDLE-ALL server farm
- Classifies the 3-tuple flow of VIP address, protocol, and port as matching criteria for server load balancing
- Utilizes a TCP connection parameter map to group together TCP connection-related commands that pertain to normalization, termination, and reuse

Perform the following steps:

---

**Step 1**  
Create a Layer 7 server load-balancing policy by entering the following commands:

```plaintext
host1/Admin(config)# policy-map type loadbalance first-match L7_SLB_POLICY
host1/Admin(config-pmap-lb)# class class-default
host1/Admin(config-pmap-lb-c)# serverfarm SERVER-HANDLE-ALL
host1/Admin(config-pmap-lb-c)# exit
host1/Admin(config-pmap-lb)# exit
host1/Admin(config)#
```

**Step 2**  
Create a Layer 3 and Layer 4 class map that classifies 3-tuple flow of VIP address, protocol, and port as matching criteria for server load balancing by entering the following commands:

```plaintext
host1/Admin(config)# class-map L4_SLBVIP_CLASS
host1/Admin(config-cmap)# match virtual-address 192.168.5.10 tcp port any
host1/Admin(config-cmap)# exit
host1/Admin(config)#
```
Step 3  Create a TCP connection parameter map by entering the following commands:

```bash
host1/Admin(config)# parameter-map type connection TCP_MAP
host1/Admin(config-parammap-conn)# reserved-bits allow
host1/Admin(config-parammap-conn)# exceed-mss allow
host1/Admin(config-parammap-conn)# nagle
host1/Admin(config-parammap-conn)# set tcp queue-limit 10
host1/Admin(config-parammap-conn)# set tcp syn-retry 3
host1/Admin(config-parammap-conn)# set tcp timeout embryonic 60
host1/Admin(config-parammap-conn)# exit
host1/Admin(config)#
```

Step 4  Create a Layer 3 and Layer 4 policy map to activate the traffic classifications outlined in the previous steps by entering the following commands:

```bash
host1/Admin(config)# policy-map multi-match L4_SLB_POLICY
host1/Admin(config-pmap)# class L4_SLBVIP_CLASS
host1/Admin(config-pmap-c)# loadbalance policy L7_SLB_POLICY
host1/Admin(config-pmap-c)# loadbalance vip inservice
host1/Admin(config-pmap-c)# connection advanced-options TCP_MAP
host1/Admin(config-pmap-c)# exit
host1/Admin(config-pmap)# exit
host1/Admin(config)#
```

Step 5  Apply the completed policies to interface VLAN 10 by entering the following commands:

```bash
host1/Admin(config)# interface VLAN 10
host1/Admin(config-if)# service-policy input L4_SLB_POLICY
```
Example of a Traffic Policy Configuration

The following example illustrates a running configuration that includes multiple class maps and policy maps that define a traffic policy for SLB. The class map and policy map configuration appears in bold in the example.

In this configuration, when a server farm is chosen for a connection, the connection is sent to a real server based on one of several load-balancing predictors. The leastconns predictor method load balances connections to the server that has the lowest number of open connections.

access-list ACL1 line 10 extended permit ip any any

probe tcp TCP
  interval 5
  faildetect 2
  passdetect interval 10
  open 3

parameter-map type http PERSIST-REBALANCE
  persistence-rebalance
parameter-map type connection PRED-CONNS-UDP_CONN
  set timeout inactivity 300

serverfarm host PRED-CONNS
  predictor leastconns
  rserver SERVER1
    inservice
  rserver SERVER2
    inservice
  rserver SERVER3
    inservice
  rserver SERVER4
    inservice
  rserver SERVER5
    inservice
  rserver SERVER6
    inservice
  rserver SERVER7
    inservice
  rserver SERVER8
    inservice
Example of a Traffic Policy Configuration

serverfarm host PRED-CONNS-UDP
failaction purge
predictor leastconns
rserver SERVER1
    inservice
rserver SERVER2
    inservice
rserver SERVER3
    probe ICMP
    inservice
rserver SERVER5
    inservice
rserver SERVER6
    inservice
rserver SERVER7
    inservice
serverfarm host PREDICTOR
probe TCP
rserver SERVER1
    inservice
rserver SERVER2
    inservice
rserver SERVER6
    inservice
rserver SERVER7
    inservice

sticky http-cookie COOKIE_TEST STKY-GRP-43
    cookie offset 1 length 999
    timeout 30
    replicate sticky
serverfarm PREDICTOR

class-map type management match-any L4_REMOTE-MGT_CLASS
    description Enables remote access to the ACE
    2 match protocol telnet any
    3 match protocol ssh any
    4 match protocol icmp any
    5 match protocol http any
    6 match protocol snmp any
class-map match-all L4PRED-CONNS-UDP-VIP_128:2222_CLASS
    2 match virtual-address 192.168.120.128 udp eq 0
class-map match-all L4PRED-CONNS-VIP_128:80_CLASS
    2 match virtual-address 192.168.120.128 tcp eq www
class-map match-all L4PREDICTOR_117:80_CLASS
    2 match virtual-address 192.168.120.117 tcp eq www
policy-map type management first-match L4_REMOTE-MGT_POLICY
    class L4_REMOTE-MGT_CLASS
        permit

Cisco 4700 Series Application Control Engine Appliance Administration Guide
policy-map type loadbalance first-match L7PLBSF_PRED-CONNS_POLICY
  class class-default
    serverfarm PRED-CONNS
policy-map type loadbalance first-match L7PLBSF_PRED-CONNS-UDP_POLICY
  class class-default
    serverfarm PRED-CONNS-UDP
policy-map type loadbalance first-match L7PLBSF_PREDICTOR_POLICY
  class class-default
    serverfarm PREDICTOR
policy-map multi-match L4SH-Gold-VIPs_POLICY
  class L4PREDICTOR_117:80_CLASS
    loadbalance vip inservice
    loadbalance policy L7PLBSF_PREDICTOR_POLICY
    loadbalance vip icmp-reply active
    nat dynamic 1 vlan 120
    appl-parameter http advanced-options PERSIST-REBALANCE
  class L4PRED-CONNS-VIP_128:80_CLASS
    loadbalance vip inservice
    loadbalance policy L7PLBSF_PRED-CONNS_POLICY
    loadbalance vip icmp-reply active
    nat dynamic 1 vlan 120
    appl-parameter http advanced-options PERSIST-REBALANCE
  class L4PRED-CONNS-UDP-VIP_128:2222_CLASS
    loadbalance vip inservice
    loadbalance policy L7PLBSF_PRED-CONNS-UDP_POLICY
    loadbalance vip icmp-reply active
    nat dynamic 1 vlan 120
    appl-parameter http advanced-options PERSIST-REBALANCE
    connection advanced-options PRED-CONNS-UDP_CONN

interface vlan 120
  description Upstream VLAN_120 - Clients and VIPs
  ip address 192.168.120.1 255.255.255.0
  fragment chain 20
  fragment min-mtu 68
  access-group input ACL1
  nat-pool 1 192.168.120.70 192.168.120.70 netmask 255.255.255.0 pat
  service-policy input L4SH-Gold-VIPs_POLICY
  no shutdown
  ip route 10.1.0.0 255.255.255.0 192.168.120.254
Viewing Class Maps, Policy Maps, and Service Policies

The ACE CLI provides a comprehensive set of \texttt{show} commands that display the class map, policy map, and service policy configuration. This section contains the following topics:

- Displaying Class Map Configuration Information
- Displaying Policy Map Configuration Information
- Displaying Service Policy Configuration Information

Displaying Class Map Configuration Information

To display the class map configurations in the ACE, use the \texttt{show running-config class-map} command in Exec mode.

For example, enter:

```
host1/Admin# show running-config class-map
Generating configuration....

class-map type management match-any Mgmt_allow_class
  10 match protocol telnet source-address 172.16.1.2 255.255.255.254
  20 match protocol ssh source-address 172.16.1.2 255.255.255.254

class-map type http loadbalance match-any L4_SLB_class
```

Displaying Policy Map Configuration Information

To display the policy map configurations in the ACE, use the \texttt{show running-config policy-map} command in Exec mode.

For example, enter:

```
host1/Admin# show running-config policy-map
Generating configuration....

policy-map type management first-match REMOTE_MGMT_ALLOW
  class SSH-ALLOW
    permit
  class TELNET-ALLOW
    permit

policy-map type loadbalance first-match L4_SLB_policy
  class L4_SLB_class
```
Displaying Service Policy Configuration Information

To display service policy statistics, use the `show service-policy` command in Exec mode. The statistics that appear in the output are dependent on the configuration of the associated Layer 3 and Layer 4 policy map. The `show service-policy` command displays the following information:

- VLAN to which the policy is applied
- Class map associated with the policy
- Status of any load-balancing operations

The syntax of this command is:

```
show service-policy policy_name [detail]
```

The keywords, options, and arguments are as follows:

- `policy_name` — Identifier of an existing policy map that is currently in service (applied to an interface) as an unquoted text string with a maximum of 64 alphanumeric characters.
- `detail` — (Optional) Displays a more detailed listing of policy map statistics and status information.

---

**Note**

The ACE updates the counters that the `show service-policy` command displays after the applicable connections are closed.

For example, to display the service policy statistics for the HTTP_INSPECT_L4POLICY policy map, enter:

```
host1/Admin# show service-policy HTTP_INSPECT_L4POLICY
```

To clear the service policy statistics, use the `clear service-policy` command. The syntax of this command is:

```
clear service-policy policy_name
```

For the `policy_name` argument, enter the identifier of an existing policy map that is currently in service (applied to an interface).

For example, to clear the statistics for the policy map REMOTE_MGMT_POLICY that is currently in service, enter:

```
host1/Admin# clear service-policy REMOTE_MGMT_POLICY
```
Table 4-11 describes the various fields that can appear in the `show service-policy detail` command output.

**Table 4-11  Field Descriptions for the show service-policy detail Command Output**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Status of the policy map as applied in a service policy to a VLAN interface: Active or Inactive.</td>
</tr>
<tr>
<td>Description</td>
<td>Optional description about the policy map.</td>
</tr>
<tr>
<td>Context Global Policy</td>
<td>Status whether the service policy has been applied globally in configuration mode to all VLAN interfaces for the context.</td>
</tr>
<tr>
<td>Interface</td>
<td>VLAN identifier of the interface associated with the service policy.</td>
</tr>
<tr>
<td>Service-Policy</td>
<td>Identifier of the policy map.</td>
</tr>
<tr>
<td>Class</td>
<td>Identifier of the class map associated with the policy map.</td>
</tr>
<tr>
<td>Inspect DNS</td>
<td>DNS application protocol inspection statistics.</td>
</tr>
<tr>
<td>Inspect HTTP</td>
<td>HTTP application protocol inspection statistics.</td>
</tr>
<tr>
<td>Inspect FTP</td>
<td>FTP application protocol inspection statistics.</td>
</tr>
<tr>
<td>Inspect ICMP</td>
<td>ICMP application protocol inspection statistics.</td>
</tr>
<tr>
<td>Inspect RTSP</td>
<td>RTSP application protocol inspection statistics.</td>
</tr>
<tr>
<td>Loadbalance</td>
<td>Server load-balancing statistics.</td>
</tr>
<tr>
<td>Nat</td>
<td>NAT statistics.</td>
</tr>
<tr>
<td>Max Length</td>
<td>Maximum length of a DNS reply.</td>
</tr>
<tr>
<td>Strict FTP</td>
<td>Status of the strict FTP function for FTP application protocol inspection: Enabled or Disabled.</td>
</tr>
<tr>
<td>URL Logging</td>
<td>Status of the URL logging function for HTTP application protocol inspection: Enabled or Disabled.</td>
</tr>
<tr>
<td>ICMP Error</td>
<td>Status of the ICMP error function for ICMP application protocol inspection: Enabled or Disabled.</td>
</tr>
<tr>
<td>Nat Dynamic</td>
<td>NAT pool identifier with the configured interface VLAN.</td>
</tr>
<tr>
<td>VIP Route Metric</td>
<td>Not applicable for the ACE appliance.</td>
</tr>
</tbody>
</table>
### Table 4-11 Field Descriptions for the show service-policy detail Command Output (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VIP Route Advertise</td>
<td>Not applicable for the ACE appliance.</td>
</tr>
<tr>
<td>VIP State</td>
<td>Operational state of the virtual server: INSERVICE or OUTOFSERVICE.</td>
</tr>
<tr>
<td>Curr Conns</td>
<td>Number of active connections to the ACE.</td>
</tr>
<tr>
<td>Hit Count</td>
<td>Number of times a connection was established.</td>
</tr>
<tr>
<td>Dropped Conns</td>
<td>Number of connections that the ACE discarded.</td>
</tr>
<tr>
<td>Client Pkt Count</td>
<td>Number of packets received from clients.</td>
</tr>
<tr>
<td>Client Byte Count</td>
<td>Number of bytes received from clients.</td>
</tr>
<tr>
<td>Server Pkt Count</td>
<td>Number of packets received from servers.</td>
</tr>
<tr>
<td>Server Byte Count</td>
<td>Number of bytes received from servers.</td>
</tr>
</tbody>
</table>
### Table 4-11  Field Descriptions for the show service-policy detail Command Output (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>L4 Policy Stats</td>
<td></td>
</tr>
<tr>
<td>TotalReq/Resp</td>
<td>Total number of requests and responses for the policy map.</td>
</tr>
<tr>
<td>Total Allowed</td>
<td>Total number of packets received and allowed.</td>
</tr>
<tr>
<td>Total Dropped</td>
<td>Total number of packets received and discarded.</td>
</tr>
<tr>
<td>Total Logged</td>
<td>Total number of errors logged.</td>
</tr>
<tr>
<td>L7 Policy</td>
<td>Identifier of the policy map associated with the service policy.</td>
</tr>
<tr>
<td>L7 Policy Stats</td>
<td>Current status of the Layer 7 policy map, including the total number of Layer 7 rules.</td>
</tr>
<tr>
<td>L7 Class/Match</td>
<td>Identifier of the Layer 7 HTTP deep packet inspection class map and the associated policy map match actions.</td>
</tr>
<tr>
<td>Total Inspected</td>
<td>Total number of packets inspected.</td>
</tr>
<tr>
<td>Total Matched</td>
<td>Total number of packets matched.</td>
</tr>
<tr>
<td>Total Reply Masked</td>
<td>Total number of masked system replies to the FTP SYST command. Applicable to only the FTP SYST command and its associated reply.</td>
</tr>
<tr>
<td>Total Dropped On Error</td>
<td>Total number of packets dropped due to an error in the match.</td>
</tr>
<tr>
<td>TotalLogged</td>
<td>Total number of errors logged.</td>
</tr>
</tbody>
</table>