



Draft - CISCO CONFIDENTIAL

# CHAPTER 7

## Configuring Parameter Maps

**Revised Date: 2/18/09**

Parameter maps provide a means of performing actions on traffic ingressing an ACE interface based on certain criteria, such as protocol or connection attributes. After you configure a parameter map, you associate it with a policy map to implement configured behavior. [Table 7-1](#) describes the parameter maps you can configure using the ANM and the ACE devices that support them.

**Table 7-1** *Parameter Map Types and ACE Support*

Parameter Map	Description	ACE Modules and Devices			
		ACE 1.0 Module	ACE 2.0 Module	ACE 4710 Running Image A1(8)	ACE 4710 Running Image A3(1.0)
Connection	Connection parameter maps combine all IP and TCP connection-related behaviors pertaining to: <ul style="list-style-type: none"> <li>TCP normalization, termination, and server reuse</li> <li>IP normalization, fragmentation, and reassembly</li> </ul>	X	X	X	X
Generic	Generic parameter maps combine related generic protocol actions for server load-balancing connections.		X	X	X
HTTP	HTTP parameter maps configure ACE behavior for HTTP load-balanced connections.	X	X	X	X
Optimization	Optimization parameter maps specify optimization-related commands that pertain to application acceleration and optimization functions performed by the ACE.			X	X
RTSP	RTSP parameter maps configure advanced RTSP behavior for server load-balancing connections.		X	X	X
SIP	Session Initiation Protocol (SIP) parameter maps configure SIP deep packet inspection on the ACE.		X	X	X
Skinny	Skinny Client Control Protocol (SCCP) parameter maps configure SCCP packet inspection on the ACE.		X	X	X

**Draft - CISCO CONFIDENTIAL****Related Topics**

- [Configuring Connection Parameter Maps, page 7-2](#)
- [Configuring Generic Parameter Maps, page 7-7](#)
- [Configuring HTTP Parameter Maps, page 7-8](#)
- [Configuring Optimization Parameter Maps, page 7-10](#)
- [Configuring RTSP Parameter Maps, page 7-17](#)
- [Configuring SIP Parameter Maps, page 7-18](#)
- [Configuring Skinny Parameter Maps, page 7-20](#)
- [Configuring Traffic Policies, page 11-1](#)
- [Configuring Parameter Maps, page 7-1](#)
- [Configuring Virtual Contexts, page 3-5](#)

## Configuring Connection Parameter Maps

Connection parameter maps combine all IP and TCP connection-related behaviors pertaining to:

- TCP normalization, termination, and server reuse
- IP normalization, fragmentation, and reassembly

Use this procedure to configure a Connection parameter map for use with a Layer 3/Layer 4 policy map.

**Procedure**

- 
- Step 1** Select **Config > Devices > context > Load Balancing > Parameter Maps > Connection Parameter Map**. The Connection Parameter Map table appears.
- Step 2** Click **Add** to add a new parameter map, or select an existing parameter map, then click **Edit** to modify it. The Connection Parameter Map configuration screen appears.
- Step 3** Configure the parameter map using the information in [Table 7-2](#).

**Table 7-2** Connection Parameter Map Attributes

Field	Description
Parameter Name	Enter a unique name for the parameter map. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters.
Exceeds MSS	Indicate how the ACE is to handle segments that exceed the maximum segment size (MSS): <ul style="list-style-type: none"> <li>• Allow—The ACE is to permit segments that exceed the configured MSS.</li> <li>• Drop—The ACE is to discard segments that exceed the configured MSS.</li> </ul>
Max Connection Limit	This option appears for ACE 2.0 modules and the ACE 4710 A3(1.0) release only. Enter the maximum number of concurrent connections to allow for the parameter map. Valid entries are integers from 0-4000000.

Table 7-2 Connection Parameter Map Attributes (continued)

Field	Description
Nagle	<p>The Nagle algorithm instructs a sender to buffer any data to be sent until all outstanding data has been acknowledged or until there is a full segment of data to send. Enabling the Nagle algorithm increases throughput, but it can increase latency in your TCP connection.</p> <p>Select the check box to enable the Nagle algorithm. Clear the check box to disable the Nagle algorithm.</p> <p><b>Note</b> Disable the Nagle algorithm when you observe unacceptable delays in TCP connections.</p>
Random Sequence Number	<p>Randomizing TCP sequence numbers adds a measure of security to TCP connections by making it more difficult for a hacker to guess or predict the next sequence number in a TCP connection.</p> <p>Select the check box to enable the use of random TCP sequence numbers. Clear the check box to disable the use of random TCP sequence numbers.</p> <p>This option is enabled by default.</p>
Bandwidth Rate Limit	<p>This option appears for ACE 2.0 modules only.</p> <p>Enter the bandwidth-rate limit in bytes per second for the parameter map. Valid entries are integers from 0-300000000 bytes.</p>
Connection Rate Limit	<p>This option appears for ACE 2.0 modules and the ACE 4710 A3(1.0) release only.</p> <p>Enter the connection-rate limit in connections per second. Valid entries are integers from 0-350000.</p>
Reserved Bits	<p>Indicate how the ACE is to handle segments with the reserved bits set in the TCP header:</p> <ul style="list-style-type: none"> <li>• Allow—Segments with the reserved bits are to be permitted.</li> <li>• Drop—Segments with the reserved bits are to be discarded.</li> <li>• Clear—Reserved bits in TCP headers are to be cleared and segments are to be allowed.</li> </ul>
Type-of-Service IP Header	<p>The type of service for an IP packet determines how the network handles the packet and balances its precedence, throughput, delay, reliability, and cost.</p> <p>Enter the type-of-service value to be applied to IP packets. Valid entries are integers from 0 to 255.</p> <p>For more information about type of service, refer to RFCs 791, 1122, 1349, and 3168.</p>
ACK Delay Time	<p>Enter the number of milliseconds that the ACE is to wait before sending an acknowledgement from a client to a server. Valid entries are integers from 0 to 400.</p>
TCP Buffer Share	<p>This option appears for only ACE 2.0 modules and ACE 1.0 modules running software versions 3.0(0)A1(6.2) and later.</p> <p>To improve throughput and overall performance, the ACE buffers the number of bytes you specify before processing received data or transmitting data. Use this option to increase the default buffer size and thereby realize improved network performance.</p> <p>Enter the maximum size of the TCP buffer in bytes. Valid entries are integers from 8192 to 262143 bytes. Default is 32768.</p> <p><b>Note</b> If you enter a value in this field for an ACE device that does not support this option, an error message appears. Leave this field blank when creating or modifying a connection parameter map for devices that do not support this option.</p>
Smallest TCP MSS	<p>Enter the size of the smallest segment of TCP data that the ACE is to accept. Valid entries are integers from 0 to 65535 bytes. The value 0 indicates that the ACE is not to set a minimum limit.</p>
Largest TCP MSS	<p>Enter the size of the largest segment of TCP data that the ACE is to accept. Valid entries are integers from 0 to 65535 bytes. The value 0 indicates that the ACE is not to set a maximum limit.</p>

**Draft - CISCO CONFIDENTIAL****Table 7-2 Connection Parameter Map Attributes (continued)**

Field	Description
SYN Retries	Enter the number of attempts that the ACE is to make to transmit a TCP segment when initiating a Layer 7 connection. Valid entries are integers from 1 to 15 with a default of 4.
TCP WAN Optimization RTT	<p>This option specifies how the ACE is to apply TCP optimizations to packets on a connection associated with a Layer 7 policy map using a round-trip time (RTT) value:</p> <ul style="list-style-type: none"> <li>• An entry of <b>0</b> (zero) indicates that the ACE is to apply TCP optimizations to packets for the life of a connection.</li> <li>• An entry of <b>65535</b> (the default) indicates that the ACE is to perform normal operations (that is, without optimizations) for the life of a connection.</li> <li>• Entries from 1 to 65534 indicate that the ACE is to use the following guidelines: <ul style="list-style-type: none"> <li>– If the actual client RTT is less than the configured RTT, the ACE performs normal operations for the life of the connection.</li> <li>– If the actual client RTT is greater than or equal to the configured RTT, the ACE performs TCP optimizations on the packets for the life of a connection.</li> </ul> </li> </ul> <p>Valid entries are integers from 0 to 65535.</p>
Timeout for Embryonic Connections	<p>An embryonic connection is a TCP three-way handshake for a connection that does not complete for some reason.</p> <p>Enter the number of seconds that the ACE is to wait before timing out an embryonic connection. Valid entries are integers from 0 to 4294967295 with a default of 5. A value of 0 indicates that the ACE is never to time out an embryonic connection.</p>
Half Closed Timeout	<p>A half-closed connection is one in which the client or server sends a FIN and the server or client acknowledges the FIN without sending a FIN itself.</p> <p>Enter the number of seconds the ACE is to wait before closing a half-closed connection. Valid entries are integers from 0 to 4294967295 with a default of 3600 (1 hour). A value of 0 indicates that the ACE is never to time out a half-closed connection.</p>
Inactivity Timeout	Enter the number of seconds that the ACE is to wait before disconnecting idle connections. Valid entries are integers from 0-3217203. A value of 0 indicates that ACE is never to time out a TCP connection.
Slow Start Algorithm	<p>When enabled, the slow start algorithm increases TCP window size as ACK handshakes arrive so that new segments are injected into the network at the rate at which acknowledgements are returned by the host at the other end of the connection.</p> <p>Select this check box to enable the slow start algorithm, and clear this check box to disable the slow start algorithm. This option is disabled by default.</p>
SYN Segments with Data	<p>Indicate how the ACE is to handle TCP SYN segments that contain data:</p> <ul style="list-style-type: none"> <li>• Allow—The ACE is to permit SYN segments that contain data and mark them for processing.</li> <li>• Drop—The ACE is to discard SYN segments that contain data.</li> </ul>
Urgent Pointer Policy	<p>Urgent data, as indicated by a control bit in the TCP header, indicates that urgent data is to be processed as soon as possible, even before normal data.</p> <p>Indicate how the ACE is to handle urgent data as identified by the Urgent data control bit:</p> <ul style="list-style-type: none"> <li>• Allow—The ACE is to permit the status of the Urgent control bit.</li> <li>• Clear—The ACE is to set the Urgent control bit to 0 (zero) and thereby invalidate the Urgent Pointer which provides segment information.</li> </ul>

**Table 7-2** Connection Parameter Map Attributes (continued)

Field	Description
TCP Window-Scale Factor	<p>The TCP window scaling extension expands the definition of the TCP window to 32 bits and uses a scale factor to carry the 32-bit value in the 16-bit window of the TCP header. Increasing the window size improves TCP performance in network paths with large bandwidth, long-delay characteristics.</p> <p>Enter the window scale factor in this field. Valid entries are integers from 0 to 14 (the maximum scale factor).</p> <p>For more information on TCP window scaling, refer to RFC 1323.</p>
Action for TCP Options Range	<p>Indicate how the ACE is to handle the TCP options:</p> <ul style="list-style-type: none"> <li>• Selective ACK</li> <li>• Timestamps</li> <li>• TCP Window Scaling</li> </ul> <p>by selecting one of the options:</p> <ul style="list-style-type: none"> <li>• N/A—This option is not set.</li> <li>• Allow—The ACE is to allow any segment with the specified option set.</li> <li>• Drop—The ACE is to discard any segment with the specified option set.</li> </ul>
Lower TCP Options	<p>Appears if you select Allow or Drop for the Action for TCP Options Range.</p> <p>Enter the lower limit of the TCP option range. Valid entries are 6, 7, or an integer from 9 to 255. See <a href="#">Table 7-3</a> for information on TCP options.</p>
Upper TCP Options	<p>Appears if you select Allow or Drop for the Action for TCP Options Range.</p> <p>Enter the upper limit of the TCP option range. Valid entries are 6, 7, or an integer from 9 to 255. See <a href="#">Table 7-3</a> for information on TCP options.</p>
Selective ACK	<p>Indicate how the ACE is to handle the selective ACK option that is specified in SYN segments:</p> <ul style="list-style-type: none"> <li>• Allow—The ACE is to allow any segment with the specified option set.</li> <li>• Clear—The ACE is to clear the specified option from any segment that has it set and allow the segment.</li> </ul>
Timestamps	<p>Indicate how the ACE is to handle the timestamp option that is specified in SYN segments:</p> <ul style="list-style-type: none"> <li>• Allow—The ACE is to allow any segment with the specified option set.</li> <li>• Clear—The ACE is to clear the specified option from any segment that has it set and allow the segment.</li> </ul>
TCP Window Scale Factor	<p>Indicate how the ACE is to handle the TCP window scale factor option that is specified in SYN segments:</p> <ul style="list-style-type: none"> <li>• Allow—The ACE is to allow any segment with the specified option set.</li> <li>• Clear—The ACE is to clear the specified option from any segment that has it set and allow the segment.</li> <li>• Drop—The ACE is to discard any segment with the specified option set.</li> </ul>

**Draft - CISCO CONFIDENTIAL****Table 7-3 TCP Options for Connection Parameter Maps<sup>1</sup>**

Kind	Length	Meaning
6	6	Echo (obsoleted by option 8)
7	6	Echo Reply (obsoleted by option 8)
9	2	Partial Order Connection Permitted
10	3	Partial Order Service Profile
11		CC
12		CC.NEW
13		CC.ECHO
14	3	TCP Alternate Checksum Request
15	N	TCP Alternate Checksum Data
16		Skeeter
17		Bubba
18	3	Trailer Checksum Option
19	18	MD5 Signature Option
20		SCPS Capabilities
21		Selective Negative Acknowledgements (SNACK)
22		Record Boundaries
23		Corruption Experienced
24		SNAP
25		Unassigned (released 12/18/2000)
26		TCP Compression Filter

1. For more information on TCP options, refer to the *Cisco 4700 Series Application Control Engine Appliance Security Configuration Guide*.

**Step 4** Click:

- **Deploy Now** to deploy this configuration on the ACE.
- **Cancel** to exit this procedure without accepting your entries and to return to the Parameter Map table.
- **Next** to accept your entries and to add another parameter map.

**Related Topics**

- [Configuring Parameter Maps, page 7-1](#)
- [Configuring Traffic Policies, page 11-1](#)
- [Configuring Virtual Contexts, page 3-5](#)

# Configuring Generic Parameter Maps

Generic parameter maps are available for ACE 2.0 modules and the ACE 4710 A3(1.0) release only.

Generic parameter maps allow you to specify nonprotocol-specific behavior for data parsing. Generic parameter maps examine the payload and make decisions regardless of the protocol.

Use this procedure to configure a generic parameter map.

## Procedure

- 
- Step 1** Select **Config > Devices > context > Load Balancing > Parameter Maps > Generic Parameter Map**. The Generic Parameter Map table appears.
- Step 2** Click **Add** to add a new parameter map, or select an existing parameter map, then click **Edit** to modify it. The Parameter Maps configuration screen appears.
- Step 3** Configure the parameter map using the information in [Table 7-4](#).

**Table 7-4**      **Generic Parameter Map Attributes**

Field	Description
Parameter Name	Enter a unique name for the parameter map. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters.
Case-insensitive	Select this check box to indicate that the ACE is to be case insensitive for this parameter map. Clear this check box to indicate that the ACE is to be case sensitive for this parameter map.
Max Parse Length	Enter the number of bytes to parse for the total length of all generic headers. Valid entries are integers from 1 to 65535 with a default of 2048 bytes.

- Step 4** Click:
- **Deploy Now** to deploy this configuration.
  - **Cancel** to exit this procedure without saving your entries and to return to the Generic Parameter Map table.
  - **Next** to deploy your entries and to configure another generic parameter map.
- 

## Related Topics

- [Configuring Parameter Maps, page 7-1](#)
- [Configuring Traffic Policies, page 11-1](#)
- [Configuring Parameter Maps, page 7-1](#)
- [Configuring Virtual Contexts, page 3-5](#)

**Draft - CISCO CONFIDENTIAL**

# Configuring HTTP Parameter Maps

HTTP parameter maps allow you to configure ACE behavior for HTTP load-balanced connections.

Use this procedure to configure an HTTP parameter map for use with a Layer 3/Layer 4 policy map.

**Procedure**

- Step 1** Select **Config > Devices > context > Load Balancing > Parameter Maps > HTTP Parameter Map**. The HTTP Parameter Map table appears.
- Step 2** Click **Add** to add a new parameter map, or select an existing parameter map, then click **Edit** to modify it. The Parameter Maps configuration screen appears.
- Step 3** Configure the parameter map using the information in [Table 7-5](#).

**Table 7-5** HTTP Parameter Map Attributes

Field	Description
Parameter Name	Enter a unique name for the parameter map. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters.
Case-insensitive	Select this check box to indicate that the ACE is to be case insensitive. Clear this check box to indicate that the ACE is to be case sensitive. This check box is cleared by default.
Header Modify Per-Request	This option appears for ACE 2.0 modules and the ACE 4710 A3(1.0) release only. Select the check box to require SSL information be inserted for every HTTP GET request. Current functionality only requires that the information be inserted at the first GET request.
Exceed Max Parse Length	Indicate how the ACE is to handle cookies, HTTP headers, and URLs that exceed the maximum parse length: <ul style="list-style-type: none"> <li>• Continue—The ACE is to continue load balancing. When this option is selected, the HTTP Persistence Rebalance option is disabled if the total length of all cookies, HTTP headers, and URLs exceeds the maximum parse value.</li> <li>• Drop—The ACE is to stop load balancing and to discard the packet.</li> </ul>
HTTP Persistence Rebalance	Select this check box to indicate that the ACE is to: <ul style="list-style-type: none"> <li>• Separately load balance each subsequent HTTP request on the same TCP connection.</li> <li>• Insert the header and cookie for every request instead of only the first request.</li> </ul> Clear this check box to indicate that this option is disabled. This option is enabled by default.

Table 7-5 HTTP Parameter Map Attributes (continued)

Field	Description
TCP Server Connection Reuse	<p>Select this check box to indicate that the ACE is to reduce the number of open connections on a server by allowing connections to persist and be reused by multiple client connections. If you enable this feature:</p> <ul style="list-style-type: none"> <li>• Ensure that the ACE maximum segment size (MSS) is the same as the server maximum segment size.</li> <li>• Configure port address translation (PAT) on the interface that is connected to the real server.</li> <li>• Configure on the ACE the same TCP options that exist on the TCP server.</li> <li>• Ensure that each server farm is homogeneous (all real servers within a server farm have identical configurations).</li> </ul> <p>Clear this check box to disable this option.</p>
Content Max Parse Length	Enter the maximum number of bytes to parse in HTTP content. Valid entries are integers from 1 to 65535 with a default of 4096.
Header Max Parse Length	Enter the maximum number of bytes to parse for the total length of cookies, HTTP headers, and URLs. Valid entries are integers from 1 to 65535 with a default of 4096.
Secondary Cookie Delimiters	Enter the ASCII-character delimiters to be used to separate cookies in a URL string. Valid entries are unquoted text strings with no spaces and a maximum of 4 characters. The default delimiters are /&#+.
MIME Type to Compress	<p>This option appears for ACE appliances only.</p> <p>In the field on the left, enter the Multipurpose Internet Mail Extension (MIME) type to compress, then click <b>Add</b>. The MIME type appears in the column on the right. To remove or change a MIME type, select it in the column on the right, then click <b>Remove</b>. The selected MIME type appears in the field on the left where you can modify or delete it.</p> <p>To specify the sequence in which compression is to be applied, select MIME types in the column on the right, then click <b>Up</b> or <b>Down</b> to arrange the MIME types.</p> <p><a href="#">Supported MIME Types, page 7-21</a> lists the supported MIME types. You can use an asterisk (*) to indicate a wildcard, such as <code>text/*</code>, which would include all text MIME types (text/html, text/plain, and so on).</p>

**Draft - CISCO CONFIDENTIAL****Table 7-5 HTTP Parameter Map Attributes (continued)**

Field	Description
User Agent Not to Compress	<p>This option appears for ACE appliances only.</p> <p>A user agent is a client that initiates a request. Examples of user agents include browsers, editors, and other end-user tools. When you specify a user agent string in this field, the ACE does not compress the response to a request when the request contains the matching user agent string.</p> <p>In the field on the left, enter the user agent string to be matched, then click <b>Add</b>. The string appears in the column on the right. To remove or change a user agent string, select it in the column on the right, then click <b>Remove</b>. The selected string appears in the field on the left where you can modify or delete it.</p> <p>To specify the sequence in which strings are to be matched, select strings in the column on the right, then click <b>Up</b> or <b>Down</b> to arrange the strings in the desired sequence.</p> <p>Valid entries are 64 characters.</p>
Minimum Size to Compress	<p>This option appears for ACE appliances only.</p> <p>Enter the threshold at which compression is to occur. The ACE compresses files that are the minimum size or larger. Valid entries are integers from 1 to 4096 bytes.</p>

**Step 4** Click:

- **Deploy Now** to deploy this configuration on the ACE.
- **Cancel** to exit this procedure without accepting your entries and to return to the Parameter Map table.
- **Next** to accept your entries and to add another parameter map.

**Related Topics**

- [Configuring Parameter Maps, page 7-1](#)
- [Configuring Traffic Policies, page 11-1](#)
- [Configuring Parameter Maps, page 7-1](#)
- [Configuring Virtual Contexts, page 3-5](#)

## Configuring Optimization Parameter Maps

Optimization parameter maps are available for ACE appliances only.

Optimization parameter maps specify optimization-related commands that pertain to application acceleration and optimization functions performed by the ACE.

Use this procedure to configure an Optimization parameter map for use with a Layer 3/Layer 4 policy map.

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

### Procedure

- Step 1** Select **Config > Devices > context > Load Balancing > Parameter Maps > Optimization Parameter Map**. The Optimization Parameter Map table appears.
- Step 2** Click **Add** to add a new parameter map, or select an existing parameter map, then click **Edit** to modify it. The Optimization Parameter Map configuration screen appears.
- Step 3** Configure the parameter map using the information in [Table 7-6](#).

**Table 7-6 Optimization Parameter Map Attributes**

Field	Description
Parameter Name	Enter a unique name for the parameter map. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters.
Set Browser Freshness Period	Select the method that the ACE is to use to determine the freshness of objects in the client's browser: <ul style="list-style-type: none"> <li>• N/A—This option is not configured.</li> <li>• Set freshness similar to FlashForward objects—The ACE is to set freshness similar to that used for FlashForwarded objects and to use the values specified in the <i>Maximum Time for Cache Time-to-Live</i> and <i>Minimum Time for Cache Time-to-Live</i> fields.</li> <li>• Disable browser object freshness control—Browser freshness control is not to be used.</li> </ul>
Duration for Browser Freshness (seconds)	This field appears if the Set Browser Freshness Period option is not configured. Enter the number of seconds that objects in the client's browser are considered fresh. Valid entries are 0 to 2147483647 seconds.
Response Codes to Ignore	Enter a comma-separated list of HTTP response codes for which the response body must not be read. For example, an entry of 302 indicates that the ACE is to ignore the response body of a 302 (redirect) response from the origin server. Valid entries are unquoted text strings with a maximum of 64 alphanumeric characters and integers from 100 to 599, inclusive.
Allow URL Mapping on non-HTML Files	URL mapping refers to the capability of ACEs to modify URLs and other content in the data stream between the origin server and the client browser. Normally, URL mapping applies only to HTML files unless non-HTML file mapping is enabled. Select this check box to enable URL mapping on files other than HTML files. Clear this check box to indicate that the ACE is not to apply URL mapping to non-HTML files.
Appscope Optimize Rate (%)	Enter the percentage of all requests or sessions to be sampled for performance with acceleration (or optimization) applied. All applicable optimizations for the class will be performed. Valid entries are from 0 to 100 percent, with a default of 10 percent. The sum of this value and the value entered in the Passthru Rate Percent field must not exceed 100.
Appscope Passthrough Rate (%)	Enter the percentage of all requests or sessions to be sampled for performance without optimization. No optimizations for the class will be performed. Valid entries are from 0 to 100, with a default of 10 percent. The sum of this value and the value entered in the Optimize Rate Percent field must not exceed 100.
Max Number for Parameter Summary Log (bytes)	Enter the maximum number of bytes that are to be logged for each parameter value in the parameter summary of a transaction log entry in the statistics log. If a parameter value exceeds this limit, it is truncated at the specified limit. Valid entries are 0 to 10,000 bytes.
Max for POST Data to Scan for Logging (kBytes)	Enter the maximum number of kilobytes of POST data the ACE is to scan for parameters for the purpose of logging transaction parameters in the statistics log. Valid entries are 0 to 1000 KB.

**Draft - CISCO CONFIDENTIAL****Table 7-6 Optimization Parameter Map Attributes (continued)**

Field	Description
Specify String for Grouping Requests	<p>Enter the string the ACE is to use to sort requests for AppScope reporting. The string can contain a URL regular expression that defines a set of URLs in which URLs that differ only by their query parameters are to be treated as separate URLs in AppScope reports.</p> <p>For example, to define a string that is used to identify the URLs <code>http://server/catalog.asp?region=asia</code> and <code>http://server/catalog.asp?region=america</code> as two separate reporting categories, you would enter <code>http_query_param(region)</code>.</p> <p>Valid entries contain 1 to 255 characters and can contain the parameter expander functions listed in <a href="#">Table 12-4</a>.</p>
Specify Base File Anonymous Level	<p>Information that is common to a large set of users is generally not confidential or user-specific. Conversely, information that is unique to a specific user or a small set of users is generally confidential or user-specific. The anonymous base file feature enables the ACE to create and deliver condensed base files that contain only information that is common to a large set of users. No information unique to a particular user, or across a very small subset of users, is included in anonymous base files.</p> <p>Enter the value for base file anonymity for the all-user condensation method. Valid entries are integers from 0 to 50; the default value of 0 disables the base file anonymity feature.</p>
Specify Cache-Key Modifier Expression	<p>A cache object key is a unique identifier that is used to identify a cached object to be served to a client, replacing a trip to the origin server. The cache key modifier feature allows you to modify the canonical form of a URL; that is, the portion before “?” in a URL. For example, the canonical URL of “<code>http://www.xyz.com/somepage.asp?action=browse&amp;level=2</code>” is “<code>http://www.xyz.com/somepage.asp</code>”.</p> <p>Enter a regular expression containing embedded variables as described in <a href="#">Table 12-4</a>. The ACE transforms URLs specified in class maps for this virtual server with the expression and variable entered here.</p> <p>Valid entries are unquoted text strings with no spaces and a maximum of 255 alphanumeric characters. If the string includes spaces, enclose the string with quotation marks (“”).</p>
Maximum Time for Cache Time-to-Live (seconds)	<p>Enter the maximum number of seconds that an object without an explicit expiration time should be considered fresh in the ACE cache. Valid entries are 0 to 2147483647 seconds.</p>
Minimum Time for Cache Time-to-Live (seconds)	<p>Enter the minimum number of seconds that an object without an explicit expiration time should be considered fresh in the ACE cache. This value specifies the minimum time that content can be cached. If the ACE is configured for FlashForward optimization, this value should normally be 0. If the ACE is configured for dynamic caching, this value should indicate how long the ACE should cache the page. (See <a href="#">Table 4-16</a> for information about these configuration options.)</p> <p>Valid entries are 0 to 2147483647 seconds.</p>
Cache Time-to-Live Duration (%)	<p>Enter the percent of an object’s age at which an embedded object without an explicit expiration time is considered fresh.</p> <p>Valid entries are 0 to 100 percent.</p>

**Table 7-6 Optimization Parameter Map Attributes (continued)**

Field	Description
Expression to Modify Cache Key Query Parameter	<p>The cache parameter feature allows you to modify the query parameter of a URL; that is, the portion after “?” in a URL. For example, the query parameter portion of “http://www.xyz.com/somepage.asp?action=browse&amp;level=2” is “action=browse&amp;level=2”.</p> <p>Enter a regular expression containing embedded variables as described in <a href="#">Table 12-4</a>. The ACE transforms URLs specified in class maps for this virtual server with the expression and variable entered here. If no string is specified, the query parameter portion of the URL is used as the default value for this portion of the cache key.</p> <p>Valid entries are unquoted text strings with no spaces and a maximum of 255 alphanumeric characters.</p>
Canonical URL Expressions	<p>The ACE uses the canonical URL feature to eliminate the “?” and any characters that follow to identify the general part of the URL. This general URL is then used to create the base file. In this way, the ACE maps multiple URLs to a single canonical URL.</p> <p>Enter a comma-separated list of parameter expander functions as defined in <a href="#">Table 12-4</a> to identify the URLs to associate with this parameter map.</p> <p>Valid entries are unquoted text strings with a maximum of 255 alphanumeric characters.</p>
Enable Cacheable Content Optimization	<p>This feature allows the ACE to detect content that can be cached and perform delta optimization on it.</p> <p>Select the check box to enable delta optimization of content that can be cached. Clear the check box to disable this feature.</p>
Enable Delta Optimization on First Visit to Web Page	<p>Select the check box to enable condensation on the first visit to a Web page. Clear the check box to disable this feature.</p>
Minimum page size for Delta Optimization (bytes)	<p>Enter the minimum page size, in bytes, that can be condensed. Valid entries are integers from 1 to 250000 bytes.</p>
Maximum page size for Delta Optimization (bytes)	<p>Enter the maximum page size, in bytes, that can be condensed. Valid entries are integers from 1 to 250000 bytes.</p>
Set Default Client Script	<p>Indicate the scripting language that the ACE is to recognize on condensed content pages:</p> <ul style="list-style-type: none"> <li>• N/A—This option is not configured.</li> <li>• Javascript—The default scripting language is JavaScript.</li> <li>• Visual Basic Script—The default scripting language is Visual Basic.</li> </ul>
Exclude Iframes from Delta Optimization	<p>Select the check box to indicate that delta optimization is not to be applied to IFrames (inline frames). Clear the check box to indicate that delta optimization is to be applied to IFrames.</p>
Exclude Non-ASCII Data from Delta Optimization	<p>Select the check box to indicate that delta optimization is not to be applied to non-ASCII data. Clear the check box to indicate that delta optimization is to be applied to non-ASCII data.</p>
Exclude JavaScripts from Delta Optimization	<p>Select the check box to indicate that delta optimization is not to be applied to JavaScript. Clear the check box to indicate that delta optimization is to be applied to JavaScript.</p>

**Draft - CISCO CONFIDENTIAL****Table 7-6 Optimization Parameter Map Attributes (continued)**

Field	Description
MIME Types to Exclude from Delta Optimization	<ol style="list-style-type: none"> <li>In the first field, enter a comma-separated list of the MIME (Multipurpose Internet Mail Extension) type messages that are not to have delta optimization applied, such as image/Jpeg, text/html, application/msword, or audio/mpeg. See <a href="#">Supported MIME Types, page 7-21</a> for a list of supported MIME types.</li> <li>Click <b>Add</b> to add the entry to the list box on the right. You can position the entries in the list box by using the Up and Down buttons.</li> </ol>
Remove HTML META Elements from Documents	Select the check box to indicate that HTML META elements are to be removed from documents to prevent them from being condensed. Clear the check box to indicate that HTML META elements are not to be removed from documents.
Set FlashForward Refresh Policy	Select the method the ACE is to use to refresh stale embedded objects: <ul style="list-style-type: none"> <li>N/A—This option is not configured.</li> <li>Allow FlashForward to indirect refresh of objects—The ACE is to use FlashForward to indirectly refresh embedded objects.</li> <li>Bypass FlashForward to direct refresh of objects—The ACE is to bypass FlashForward for stale embedded objects so that they are refreshed directly.</li> </ul>
Rebase Delta Optimization Threshold (%)	Enter the delta threshold, expressed as a percent, when rebasing is to be triggered. This entry represents the size of a page delta relative to total page size, expressed as a percent. This entry triggers rebasing when the delta response size exceeds the threshold as a percentage of base file size.  Valid entries are 0 to 10000 percent.
Rebase FlashForward Threshold (%)	Enter the threshold, expressed as a percent, when rebasing is to be triggered based on the percent of FlashForwarded URLs in the response. This entry triggers rebasing when the difference between the percentages of FlashForwarded URLs in the delta response and the base file exceeds the threshold.  Valid entries are 0 to 10000 percent.
Rebase History Size (pages)	Enter the number of pages to be stored before the ACE resets all rebase control parameters to zero and starts over. This option prevents the base file from becoming too rigid.  Valid entries are 10 to 2147483647.
Rebase Modify Cool-off Period (seconds)	Enter the number of seconds after the last modification before performing a rebase.  Valid entries are 1 to 14400 seconds (4 hours).
Rebase Reset Period (seconds)	Enter the period of time, in seconds, for performing a meta data refresh.  Valid entries are 1 to 900 seconds (15 minutes).
Override Client Request Headers	Indicate how the ACE is to handle client request headers (primarily for embedded objects): <ul style="list-style-type: none"> <li>N/A—This feature is not enabled.</li> <li>All cache request headers are ignored—The ACE is to ignore all cache request headers.</li> <li>Overrides the Cache-Control: no cache HTTP header from a request—The ACE is to ignore cache control request headers that state <i>no cache</i>.</li> </ul>

Table 7-6 Optimization Parameter Map Attributes (continued)

Field	Description
Override Server Response Headers	<p>Indicate how the ACE is to handle origin server response headers (primarily for embedded objects):</p> <ul style="list-style-type: none"> <li>• N/A—This feature is not enabled.</li> <li>• All cache response headers are ignored—The ACE is to ignore all response headers.</li> <li>• Overrides the Cache-Control: private HTTP header from a response—The ACE is to ignore cache control response headers that state <i>private</i>.</li> </ul>
UTF-8 Character Set Threshold	<p>The UTF-8 (8-bit Unicode Transformation Format) character set is an international standard that allows Web pages to display non-ASCII or non-English multibyte characters. It can represent any universal character in the Unicode standard and is backwards compatible with ASCII.</p> <p>Enter the number of UTF-8 characters that need to appear on a page to constitute a UTF-8 character set page. Valid entries are integers from 1 to 1,000,000.</p>
Hosts Limit for FlashConnect	<p>FlashConnect dynamically renames embedded objects by adding a prefix and changing the hostname so that the objects appear to reside on different hosts. FlashConnect then has the browser open a separate connection to the origin server for each object and retrieve the objects in parallel instead of sequentially.</p> <p>Enter the maximum number of artificial hosts that FlashConnect can create for retrieving embedded objects.</p> <p>Valid entries are integers from 0 to 99.</p>
Server Load Threshold Trigger (%)	<p>The server load threshold trigger indicates that the time-to-live (TTL) period for cached objects is to be based dynamically on server load. With this method, TTL periods increase if the current response time from the origin sever is greater than the average response time and decrease if the current response time from the origin server is less than the average response time when the difference in response times exceeds a specified threshold amount.</p> <p>Enter the threshold, expressed as a percent, at which the TTL for cached objects is to be changed.</p> <p>Valid entries are from 0 to 100 percent.</p>
Server Load Time-to-Live Change (%)	<p>This option specifies the percentage by which the cache TTL is increased or decreased in response to a change in server load. For example, if this value is set to 20 and the current TTL for a response is 300 seconds, and if the current server response times exceeds the trigger threshold, the cache TTL for the response is raised to 360 seconds.</p> <p>Enter the percent by which the cache TTL is to be increased or decreased when the server load threshold trigger is met.</p> <p>Valid entries are from 0 to 100 percent.</p>
Enable XSLT Merge Debug	<p>Select the check box to enable the XSLT merge debug function. Clear the check box to disable the XSLT merge debug function.</p>
Specify XSLT Stylesheet for PreTransform	<p>Enter the URL of an XSLT style sheet to indicate that the ACE is to perform a pretransformation of the style sheet.</p>
Specify XSLT Stylesheet for XSLT Merge	<p>Enter the URL of an XSLT style sheet to force the use of this style sheet, regardless of any XSL specified in the XML source file.</p>

**Draft - CISCO CONFIDENTIAL****Table 7-6 Optimization Parameter Map Attributes (continued)**

Field	Description
Specify Delta Optimization Mode	<p>Select the method by which delta optimization is to be implemented:</p> <ul style="list-style-type: none"> <li>• N/A—This option is not configured.</li> <li>• Enable all-user mode for delta optimization—The ACE is to generate the delta against a single base file that is shared by all users of the URL. This option is usable in most cases if the structure of a page is common across all users, and the disk space overhead is minimal.</li> <li>• Enable the per-user mode for delta optimization—The ACE is to generate the delta against a base file that is created specifically for that user. This option is useful when page contents, including layout elements, are different for each user, and delivers the highest level of condensation. However, this increases disk space requirements because a copy of the base page that is delivered to each user is cached. This option is useful when privacy is required because base pages are not shared among users.</li> </ul>
Smooth Transform of Image	Select the check box to indicate that the ACE is to apply a smoothing transformation to images, if needed. Clear the check box to indicate that the ACE is not to apply a smoothing transformation to images.
Ignore Thumbnail Images	Select the check box to indicate that the ACE is to ignore small thumbnail images without transforming them in any way. Clear the check box to indicate that the ACE is not to ignore thumbnail images.
Progressive Rendering of Image	<p>Select the check box to indicate that the ACE is to transform images so that they are rendered progressively by the browser. When enabled, this feature results in slightly larger image sizes. Because images render progressively, this feature might not be useful in fast networking environments, such as LANs.</p> <p>Clear the check box to indicate that the ACE is not to transform images so that they are rendered progressively by the browser.</p>
High Quality Transform of Image	<p>Select the check box to indicate that the ACE is to apply higher quality transformation with less compression to images. When enabled, this option results in images that are larger than those compressed without this option, but they have less visual deterioration. Image size is smaller with this option than for uncompressed images.</p> <p>Clear the check box to indicate that the ACE is not to apply higher quality transformation to images.</p>
Grayscale Transform of Image	<p>Select the check box to indicate that the ACE is to optimize images by transforming JPEG and PNG images to grayscale images.</p> <p>Clear the check box to indicate that the ACE is not to optimize images by transforming JPEG and PNG images to grayscale images.</p>
String To Be Used for Server HTTP Header	<p>Use this option to define a string that is to be sent in the server header for an HTTP response. This option provides you with a method for uniquely tagging the context or URL match statement by setting the server header value to a particular string. The server header string can be used when a particular URL is not being transmitted to the correct target context or match statement.</p> <p>Enter the string that is to appear in the server header. Valid entries are quoted text strings with a maximum of 64 alphanumeric characters.</p>

**Step 4** Click:

- **Deploy Now** to save your entries. The ACE validates the parameter map configuration and deploys it.
- **Cancel** to exit this procedure without accepting your entries and to return to the Parameter Map table.
- **Next** to accept your entries and to add another parameter map.

**Related Topics**

- [Configuring Parameter Maps, page 7-1](#)
- [Configuring Traffic Policies, page 11-1](#)
- [Configuring Parameter Maps, page 7-1](#)
- [Configuring Virtual Contexts, page 3-5](#)

## Configuring RTSP Parameter Maps

RTSP parameter maps are available for ACE 2.0 modules and the ACE 4710 A3(1.0) release only.

RTSP parameter maps allow you to configure advanced RTSP behavior for server load-balancing connections.

Use this procedure to configure an [RTSP](#) parameter map.

**Procedure**

- 
- Step 1** Select **Config > Devices > context > Load Balancing > Parameter Maps > RTSP Parameter Map**. The RTSP Parameter Map table appears.
- Step 2** Click **Add** to add a new parameter map, or select an existing parameter map, then click **Edit** to modify it. The Parameter Maps configuration screen appears.
- Step 3** Configure the parameter map using the information in [Table 7-7](#).

**Table 7-7** RTSP Parameter Map Attributes

Field	Description
Parameter Name	Enter a unique name for the parameter map. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters.
Case-insensitive	Select this check box to indicate that the ACE is to be case insensitive. Clear this check box to indicate that the ACE is to be case sensitive.
Header Max Parse Length	Enter the number of bytes to parse for the total length of RTSP headers. Valid entries are integers from 1 to 65535 with a default of 2048 bytes.

**Draft - CISCO CONFIDENTIAL****Step 4** Click:

- **Deploy Now** to deploy this configuration.
- **Cancel** to exit this procedure without saving your entries and to return to the RTSP Parameter Map table.
- **Next** to deploy your entries and to configure another RTSP parameter map.

**Related Topics**

- [Configuring Parameter Maps, page 7-1](#)
- [Configuring Traffic Policies, page 11-1](#)
- [Configuring Parameter Maps, page 7-1](#)
- [Configuring Virtual Contexts, page 3-5](#)

## Configuring SIP Parameter Maps

SIP parameter maps are available for ACE 2.0 modules and the ACE 4710 A3(1.0) release only.

[SIP](#) parameter maps allow you to configure SIP deep-packet inspection policy maps on the ACE.

Use this procedure to configure a SIP parameter map.

**Procedure**

- 
- Step 1** Select **Config > Devices > context > Load Balancing > Parameter Maps > SIP Parameter Map**. The SIP Parameter Map table appears.
- Step 2** Click **Add** to add a new parameter map, or select an existing parameter map, then click **Edit** to modify it. The Parameter Maps configuration screen appears.
- Step 3** Configure the parameter map using the information in [Table 7-8](#).

**Table 7-8** *SIP Parameter Map Attributes*

Field	Description
Parameter Name	Enter a unique name for the parameter map. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters.
Instant Messaging	Select the check box to enable instant messaging (IM) over SIP after it has been disabled. Clear this check box to disable this feature.
Max Forward Validation	This option allows you to configure the ACE to validate the value of the Max-Forward header field. Specify how the ACE is to handle the validation of Max-Forward header fields: <ul style="list-style-type: none"> <li>• N/A—The ACE is not to validate Max-Forward header fields.</li> <li>• Drop—The ACE is to drop the SIP message if it does not pass Max-Forward header validation.</li> <li>• Reset—The ACE is to reset the SIP connection if it does not pass Max-Forward header validation.</li> </ul>

**Table 7-8 SIP Parameter Map Attributes (continued)**

Field	Description
Log Max Forward Validation Event	Select the check box to indicate that the ACE is to log Max-Forward validation events. Clear the check box to disable this feature.
Mask UA Software Version	If the software version of a user agent is exposed, that user agent might be vulnerable to attacks from hackers who exploit the security holes present in that particular software version. This option allows you to mask or log the user agent software version so that it is not exposed. Select the check box to indicate that the ACE is to mask the user agent software version. Clear the check box to disable this feature.
Log UA Software Version	Select the check box to indicate that the ACE is to log the user agent software version. Clear the check box to disable this feature.
Strict Header Validation	You can ensure the validity of SIP packet headers by configuring the ACE to check for the presence of the following mandatory SIP header fields: <ul style="list-style-type: none"> <li>• From</li> <li>• To</li> <li>• Call-ID</li> <li>• CSeq</li> <li>• Via</li> <li>• Max-Forwards</li> </ul> If one of the header fields is missing in a SIP packet, the ACE considers that packet invalid. The ACE also checks for forbidden header fields, according to RFC 3261. Specify how the ACE is to handle header validation. <ul style="list-style-type: none"> <li>• N/A—The ACE is not to perform header validation.</li> <li>• Drop—The ACE is to drop the SIP message if the SIP packet does not pass header validation.</li> <li>• Reset—The ACE is to reset the connection if the SIP packet does not pass header validation.</li> </ul>
Log Strict Header Validation	Select the check box to indicate that the ACE is to log header validation events. Clear the check box to disable this feature.
Mask non-SIP URI	This option and the next enable the detection of non-SIP URIs in SIP messages. Select the check box to indicate that the ACE is to mask non-SIP URIs in SIP messages. Clear the check box to disable this feature.
Log non-SIP URI	Select the check box to indicate that the ACE is to log non-SIP URIs in SIP messages. Clear the check box to disable this feature.
SIP Media Pinhole Timeout	Specify the timeout period for SIP media pinhole (secure port) connections in seconds. Valid entries are integers from 1 to 65535 seconds. Default is 5.

**Draft - CISCO CONFIDENTIAL****Step 4** Click:

- **Deploy Now** to deploy this configuration.
- **Cancel** to exit this procedure without saving your entries and to return to the SIP Parameter Map table.
- **Next** to deploy your entries and to configure another SIP parameter map.

**Related Topics**

- [Configuring Parameter Maps, page 7-1](#)
- [Configuring Traffic Policies, page 11-1](#)
- [Configuring Parameter Maps, page 7-1](#)
- [Configuring Virtual Contexts, page 3-5](#)

## Configuring Skinny Parameter Maps

Skinny parameter maps are available for ACE 2.0 modules and the ACE 4710 A3(1.0) release only.

Skinny Client Control Protocol ([SCCP](#) or [Skinny](#)) parameter maps allow you to configure SCCP packet inspection on the ACE.

Use this procedure to configure a Skinny parameter map.

**Procedure**

- 
- Step 1** Select **Config > Devices > context > Load Balancing > Parameter Maps > Skinny Parameter Map**. The Skinny Parameter Map table appears.
- Step 2** Click **Add** to add a new parameter map, or select an existing parameter map, then click **Edit** to modify it. The Parameter Maps configuration screen appears.
- Step 3** Configure the parameter map using the information in [Table 7-9](#).

**Table 7-9** *Skinny Parameter Map Attributes*

Field	Description
Parameter Name	Enter a unique name for the parameter map. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters.
Enforce Registration	You can configure the ACE to allow only registered Skinny clients to make calls. To accomplish this task, the ACE maintains the state of each Skinny client. After a client registers with <a href="#">CCM</a> , the ACE opens a secure port (pinhole) to allow that client to make a call. Select the check box to enable Skinny registration enforcement. Clear the check box to disable this feature.
Message Id Max	Enter the largest value for the station message ID in hexadecimal that the ACE is to accept. Valid entries are hexadecimal values from 0 to 4000 with a default value of 0x181. If a packet arrives with a station message ID greater than the specified value, the ACE drops the packet and generates a syslog message.

**Table 7-9** Skinny Parameter Map Attributes (continued)

Field	Description
SCCP Prefix Length Max	This feature allows you to configure the ACE so that it checks the maximum SCCP prefix length. The ACE drops Skinny message packets that fail this check and generates a syslog message.  Enter the maximum SCCP prefix length in bytes. Valid entries are integers from 4 to 4000 bytes.
SCCP Prefix Length Min	By default, the ACE drops SCCP messages that have an SCCP Prefix length that is less than the message ID. The ACE drops Skinny message packets that fail this check and generates a syslog message.  Enter the minimum SCCP prefix length in bytes. Valid entries are integers from 4 to 4000 bytes.

**Step 4** Click:

- **Deploy Now** to deploy this configuration.
- **Cancel** to exit this procedure without saving your entries and to return to the Skinny Parameter Map table.
- **Next** to deploy your entries and to configure another Skinny parameter map.

**Related Topics**

- [Configuring Parameter Maps, page 7-1](#)
- [Configuring Traffic Policies, page 11-1](#)
- [Configuring Parameter Maps, page 7-1](#)
- [Configuring Virtual Contexts, page 3-5](#)

## Supported MIME Types

The ACE supports following MIME types:

- application/msexcel
- application/mspowerpoint
- application/msword
- application/octet-stream
- application/pdf
- application/postscript
- application/x-gzip
- application/x-java-archive
- application/x-java-vm
- application/x-messenger
- application/zip

***Draft - CISCO CONFIDENTIAL***

- audio/\*
- audio/basic
- audio/midi
- audio/mpeg
- audio/x-adpcm
- audio/x-aiff
- audio/x-ogg
- audio/x-wav
- image/\*
- image/gif
- image/jpeg
- image/png
- image/tiff
- image/x-3ds
- image/x-bitmap
- image/x-niff
- image/x-portable-bitmap
- image/x-portable-greymap
- image/x-xpm
- text/\*
- text/css
- text/html
- text/plain
- text/richtext
- text/sgml
- text/xmcd
- text/xml
- video/\*
- video/flc
- video/mpeg
- video/quicktime
- video/sgi
- video/x-fli