CHAPTER 10

Configuring Parameter Maps

This chapter describes how to configure parameter maps on the Cisco Application Control Engine (ACE) using Cisco Application Networking Manager (ANM).

Note When naming ACE objects (such as a real server, virtual server, parameter map, class map, health probe, and so on), enter an alphanumeric string of 1 to 64 characters, which can include the following special characters: underscore (_), hyphen (-), and dot (.). Spaces are not allowed.

If you are using ANM with an ACE module or ACE appliance and you configure a named object at the ACE CLI, keep in mind that ANM does not support all of the special characters that the ACE CLI allows you to use when configuring a named object. If you use special characters that ANM does not support, you may not be able to import or manage the ACE using ANM.

This chapter includes the following sections:

Information About Parameter Maps

Parameter maps allow you to perform actions on traffic that ingresses 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 10-1 describes the parameter maps that you can configure using ANM and the ACE devices that support them.

Table 10-1 Parameter Map Types and ACE Support

Parameter Map	Description	ACE Device	
		ACE Module	ACE Appliance
Connection	Connection parameter maps combine all IP and TCP connection-related behaviors pertaining to: • TCP normalization, termination, and server reuse • IP normalization, fragmentation, and reassembly	X	X
DNS	Domain Name System (DNS) parameter maps configure DNS actions for DNS packet inspection.	X	X
Generic	Generic parameter maps combine related generic protocol actions for server load-balancing connections.	X	X
HTTP	HTTP parameter maps configure ACE behavior for HTTP load-balanced connections.	X	X
Optimization	Optimization parameter maps specify optimization-related commands that pertain to application acceleration and optimization functions performed by the ACE.		X
RDP	Remote Desktop Protocol (RDP) parameter maps configure routing-token-rebalance in which the ACE redirects a connection that contains RDP packets to another server when the real server that matches the token information in the client request is down. **Note** RDP parameter maps require ACE software Version A5(2.0) or later.	X	X
RTSP	Real Time Streaming Protocol (RTSP) parameter maps configure advanced RTSP behavior for server load-balancing connections.	X	X
SIP	Session Initiation Protocol (SIP) parameter maps configure SIP deep packet inspection on the ACE.	X	X
Skinny	Skinny Client Control Protocol (SCCP) parameter maps configure SCCP packet inspection on the ACE.	X	X

Related Topics

- Configuring Connection Parameter Maps, page 10-3
- Configuring Generic Parameter Maps, page 10-8
- Configuring HTTP Parameter Maps, page 10-9
- Configuring Optimization Parameter Maps, page 10-12
- Configuring RTSP Parameter Maps, page 10-21
- Configuring SIP Parameter Maps, page 10-22
- Configuring Skinny Parameter Maps, page 10-24
- Configuring Generic Parameter Maps, page 10-8
- Configuring Traffic Policies, page 14-1
- Configuring Parameter Maps, page 10-1
- Configuring Virtual Contexts, page 6-8

Configuring Connection Parameter Maps

You can configure a connection parameter map for use with a Layer 3/Layer 4 policy map. Connection parameter maps combine all IP and TCP connection-related behaviors pertaining to the following:

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

Procedure

Step 1 Choose **Config** > **Devices** > *context* > **Load Balancing** > **Parameter Maps** > **Connection Parameter Maps**.

The Connection Parameter Maps table appears.

Step 2 In the Connection Parameter Maps table, click **Add** to add a new parameter map, or choose an existing parameter map and click **Edit** to modify it.

The Connection Parameter Maps configuration window appears.

Step 3 In the Connection Parameter Maps configuration window, configure the parameter map using the information in Table 10-2.

Click **More Settings** to access the additional Connection Parameter Map configuration attributes. By default, ANM hides the default Connection Parameter Map configuration attributes and the attributes that are not commonly used.

Table 10-2 Connection Parameter Map Attributes

Field	Description
Parameter Name	Unique name for the parameter map. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters.
Description	Field that appears for ACE module A2(1.5), ACE appliance A3(2.3), and later releases of either device type. If you attempt to use the Description feature with an ACE that is running an earlier software version, ANM displays an invalid command detected error message and does not deploy the parameter map. Brief description of the parameter map. Enter a text string with a maximum of 240 alphanumeric characters (A–Z, a–z, 0–9). Spaces and special characters are allowed. Double quotes must be entered as matching pairs.
Inactivity Timeout (Seconds)	Number of seconds that the ACE is to wait before disconnecting idle connections. Valid entries are from 0 to 3217203. A value of 0 indicates that the ACE is never to time out a TCP connection.

Table 10-2 Connection Parameter Map Attributes (continued)

Field	Description
More Settings	
Exceeds MSS	Action that the ACE takes to handle segments that exceed the maximum segment size (MSS): • **Allow**—The ACE is to permit segments that exceed the configured MSS. • **Drop**—The ACE is to discard segments that exceed the configured MSS.
Full Proxy MSS	Allows the ACE to splice together the client front-end and the server back-end connections when the ACE is proxying Layer 7 traffic flow and the negotiated front-end and back-end TCP handshakes do not match. Uncheck the check box when you do not want the ACE to enable a connection when the TCP handshakes do not match.
Max. Connection Limit	Maximum number of concurrent connections to allow for the parameter map. Valid entries are from 0 to 4000000.
Nagle	Check box that enables the Nagle algorithm, which 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. Uncheck the check box to disable the Nagle algorithm. **Note** Disable the Nagle algorithm when you observe unacceptable delays in TCP connections.
Random Sequence Number	Check box that enables the use of random TCP sequence numbers, which 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. Uncheck the check box to disable the use of random TCP sequence numbers. This option is enabled by default.
Bandwidth Rate Limit	Option that appears for ACE modules only. Enter the bandwidth-rate limit in bytes per second for the parameter map. Valid entries are from 0 to 300000000 bytes.
Connection Rate Limit	Connection-rate limit in connections per second. Valid entries are from 0 to350000.
Reserved Bits	Action that the ACE takes to handle segments with the reserved bits set in the TCP header: • **Allow**—Segments with the reserved bits are to be permitted. • **Drop**—Segments with the reserved bits are to be discarded. • **Clear**—Reserved bits in TCP headers are to be cleared and segments are to be allowed.
Type-of-Service IP Header	Type of service for an IP packet that determines how the network handles the packet and balances its precedence, throughput, delay, reliability, and cost. Enter the type-of-service value to be applied to IP packets. Valid entries are from 0 to 255. For more information about type of service, refer to RFCs 791, 1122, 1349, and 3168.
ACK Delay Time (Milliseconds)	Number of milliseconds that the ACE is to wait before sending an acknowledgement from a client to a server. Valid entries are from 0 to 400.

Table 10-2 Connection Parameter Map Attributes (continued)

Field	Description
TCP Buffer Share (Bytes)	Option that appears for only ACE modules. 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. Enter the maximum size of the TCP buffer in bytes. Valid entries are from 8192 to 262143 bytes. Default is 32768. **Note** 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.
TCP Buffer Threshold (%)	Select the TCP buffer threshold, expressed as a percent, to indicate when the TCP connection is to be reset. This entry represents the maximum number of TCP connections that the hosts can open. This entry prevents the ACE from exhausting all available buffers due to the outage caused by DDoS attack. The options are 50, 75, 77, 88, 95, and 100. The default value is 100.
Smallest TCP MSS (Bytes)	Size of the smallest segment of TCP data that the ACE is to accept. Valid entries are from 0 to 65535 bytes. The value 0 indicates that the ACE is not to set a minimum limit.
Largest TCP MSS (Bytes)	Size of the largest segment of TCP data that the ACE is to accept. Valid entries are from 0 to 65535 bytes. The value 0 indicates that the ACE is not to set a maximum limit.
SYN Retries	Number of attempts that the ACE is to make to transmit a TCP segment when initiating a Layer 7 connection. Valid entries are from 1 to 15. The default is 4.

TCP WAN Optimization RTT	Option that 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.
	
	The choices are as follows:
	• An entry of 0 (zero) indicates that the ACE is to apply TCP optimizations to packets for the life of a connection.
	• An entry of 65535 (the default) indicates that the ACE is to perform normal operations (that is, without optimizations) for the life of a connection.
	• Entries from 1 to 65534 indicate that the ACE is to use the following guidelines:
	  • If the actual client RTT is less than the configured RTT, the ACE performs normal operations for the life of the connection.
	  • 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.
	
	Valid entries are from 0 to 65535.

Timeout For Embryonic Connections (Seconds)	Number of seconds that the ACE is to wait before timing out an embryonic connection, which is a TCP three-way handshake for a connection that does not complete for some reason. Valid entries are from 0 to 4294967295. The default is 5. A value of 0 indicates that the ACE is never to time out an embryonic connection.
Half Closed Timeout (Seconds)	Number of seconds the ACE is to wait before closing a half-closed connection, which is one in which the client or server sends a FIN and the server or client acknowledges the FIN without sending a FIN itself. Valid entries are from 0 to 4294967295. The default is 3600 (1 hour). A value of 0 indicates that the ACE is never to time out a half-closed connection.

Table 10-2 Connection Parameter Map Attributes (continued)

Field	Description
Slow Start Algorithm	Check box that enables the slow start algorithm. 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. Uncheck the check box to disable the slow start algorithm. This option is disabled by default.
SYN Segments With Data	Action that the ACE takes to handle TCP SYN segments that contain data: • **Allow**—The ACE is to permit SYN segments that contain data and mark them for processing. • **Drop**—The ACE is to discard SYN segments that contain data.
Urgent Pointer Policy	Action that the ACE takes to handle urgent data as identified by the Urgent data control bit. 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. The choices are as follows: • **Allow**—The ACE is to permit the status of the Urgent control bit. • **Clear**—The ACE is to set the Urgent control bit to 0 (zero) and thereby invalidate the Urgent Pointer which provides segment information.
TCP Window Scale Factor	TCP window scale factor. 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. Valid entries are from 0 to 14 (the maximum scale factor). For more information on TCP window scaling, refer to RFC 1323.
Action For TCP Options Range	Action that the ACE takes to handle the following TCP options: • Selective ACK • Timestamps • Action For TCP Window Scale Factor The choices are as follows: • **N/A**—This option is not set. • **Allow**—The ACE is to allow any segment with the specified option set. • **Drop**—The ACE is to discard any segment with the specified option set.
Lower TCP Options	Option that appears if you chose Allow or Drop for the Action For TCP Options Range. Enter the lower limit of the TCP option range. Valid entries are 6, 7, or a value from 9 to 255. See Table 10-3 for information on TCP options.
Upper TCP Options	Option that appears if you chose Allow or Drop for the Action For TCP Options Range. Enter the upper limit of the TCP option range. Valid entries are 6, 7, or a value from 9 to 255. See Table 10-3 for information on TCP options.

Table 10-2 Connection Parameter Map Attributes (continued)

Field	Description
Full Proxy MSS Mismatch	Allows the ACE to splice together the client front-end and the server back-end connections when the ACE is proxying Layer 7 traffic flow and the negotiated front-end and back-end TCP handshakes do not match. Uncheck the check box when you do not want the ACE to enable a connection when the TCP handshakes do not match. **Note** This field appears only for ACE software Version A5(2.0) or later.
Selective ACK	Action that the ACE takes to handle the selective ACK option that is specified in SYN segments: • **Allow**—The ACE allows any segment with the specified option set. • **Clear**—The ACE clears the specified option from any segment that has it set and allow the segment.
Timestamps	Action that the ACE takes to handle the time stamp option that is specified in SYN segments: • **Allow**—The ACE allows any segment with the specified option set. • **Clear**—The ACE clears the specified option from any segment that has it set and allow the segment.
Action For TCP Window Scale Factor	Action that the ACE takes to handle the TCP window scale factor option that is specified in SYN segments: • **Allow**—The ACE allows any segment with the specified option set. • **Clear**—The ACE clears the specified option from any segment that has it set and allow the segment. • **Drop**—The ACE discards any segment with the specified option set.

Table 10-3 lists the TCP options for connection parameter maps.

Table 10-3 TCP Options for Connection Parameter Maps[1]

Type	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

Table 10-3 TCP Options for Connection Parameter Maps[1] (continued)

Type	Length	Meaning
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 about TCP options, see the *Cisco 4700 Series Application Control Engine Appliance Security Configuration Guide*.

Step 4 Do one of the following:

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

Related Topics

- Configuring Parameter Maps, page 10-1
- Configuring Traffic Policies, page 14-1
- Configuring Virtual Contexts, page 6-8

Configuring Generic Parameter Maps

You configure a generic parameter map, which allows you to specify nonprotocol-specific behavior for data parsing. Generic parameter maps examine the payload and make decisions regardless of the protocol.

Procedure

Step 1 Choose **Config** > **Devices** > *context* > **Load Balancing** > **Parameter Maps** > **Generic Parameter Maps**.

The Generic Parameter Maps table appears.

Step 2 In the Generic Parameter Maps table, click **Add** to add a new parameter map, or choose an existing parameter map and click **Edit** to modify it.

The Parameter Maps configuration window appears.

Step 3 In the Parameter Maps configuration window, configure the parameter map using the information in Table 10-4.

Table 10-4 Generic Parameter Map Attributes

Field	Description
Parameter Name	Unique name for the parameter map. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters.
Description	Field that appears for ACE module A2(1.5), ACE appliance A3(2.3), and later releases of either device type. If you attempt to use the Description feature with an ACE that is running an earlier software version, ANM displays an invalid command detected error message and does not deploy the parameter map. Brief description of the parameter map. Enter a text string with a maximum of 240 alphanumeric characters (A–Z, a–z, 0–9). Spaces and special characters are allowed. Double quotes must be entered as matching pairs.
Case-Insensitive	Check box that instructs the ACE to be case insensitive for the parameter map. Uncheck this check box to instruct the ACE to be case sensitive for this parameter map.
Max. Parse Length (Bytes)	Number of bytes to parse for the total length of all generic headers. Valid entries are from 1 to 65535. The default is 2048 bytes.

Step 4 Do one of the following:

- Click **Deploy Now** to deploy this configuration on the ACE and save your entries to the running-configuration and startup-configuration files.
- Click **Cancel** to exit this procedure without saving your entries and to return to the Generic Parameter Maps table.
- Click **Next** to deploy your entries and to configure another generic parameter map.

Related Topics

- Configuring Parameter Maps, page 10-1
- Configuring Traffic Policies, page 14-1
- Configuring Parameter Maps, page 10-1
- Configuring Virtual Contexts, page 6-8

Configuring HTTP Parameter Maps

You can configure an HTTP parameter map for use with a Layer 3/Layer 4 policy map. HTTP parameter maps allow you to configure ACE behavior for HTTP load-balanced connections.

Procedure

Step 1 Choose **Config** > **Devices** > *context* > **Load Balancing** > **Parameter Maps** > **HTTP Parameter Maps**.

The HTTP Parameter Maps table appears.

Step 2 In the HTTP Parameter Maps table, click **Add** to add a new parameter map, or choose an existing parameter map and click **Edit** to modify it.

The HTTP Parameter Maps configuration window appears.

Step 3 In the HTTP Parameter Maps configuration window, configure the parameter map using the information in Table 10-5.

Table 10-5 HTTP Parameter Map Attributes

Field	Description
Parameter Name	Unique name for the parameter map. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters.
Description	Field that appears for ACE module A2(1.5), ACE appliance A3(2.3), and later releases of either device type. If you attempt to use the Description feature with an ACE that is running an earlier software version, ANM displays an invalid command detected error message and does not deploy the parameter map. Brief description of the parameter map. Enter a text string with a maximum of 240 alphanumeric characters (A–Z, a–z, 0–9). Spaces and special characters are allowed. Double quotes must be entered as matching pairs.
Case-Insensitive	Check box that instructs the ACE to be case insensitive. Uncheck this check box to indicate that the ACE is to be case sensitive. This check box is cleared by default.
Header Modify Per-Request	Check box to require that SSL information is inserted for every HTTP GET request. Current functionality only requires that the information be inserted at the first GET request.
Exceed Max. Parse Length	Action that the ACE takes to handle cookies, HTTP headers, and URLs that exceed the maximum parse length. The choices are as follows: • **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. • **Drop**—The ACE is to stop load balancing and to discard the packet.
HTTP Persistence Rebalance	Check box that instructs the ACE to do the following: • Separately load balance each subsequent HTTP request on the same TCP connection. • Insert the header and cookie for every request instead of only the first request. Uncheck this check box to indicate that this option is disabled. This option is enabled by default.
TCP Server Connection Reuse	Check box that instructs the ACE 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, perform the following tasks: • Ensure that the ACE maximum segment size (MSS) is the same as the server maximum segment size. • Configure port address translation (PAT) on the interface that is connected to the real server. • Configure on the ACE the same TCP options that exist on the TCP server. • Ensure that each server farm is homogeneous (all real servers within a server farm have identical configurations). Uncheck this check box to disable this option.

Table 10-5 HTTP Parameter Map Attributes (continued)

Field	Description
Enable Drop on Parsing Error	This field requires ACE software Version A5(2.0) or later. Check this check box to have the ACE drop a connection when it detects a parse error. Clear the check box to disable this option and configure the ACE maintain a connection even when it detects a parse error. This is the default setting.
Enable Non Strict on Parsing Error	This field requires ACE software Version A4(2.0) or later. Check this check box to configure the ACE to allow the presence of a CRLF in the header before the header name, which is inserted for header name continuation purposes. Normally, the ACE considers a CRLF in the header a parse error. When you enable this feature and the ACE encounters a CRLF in the header, the ACE ignores the parse error and allows the Layer 7 connection. Clear the check box to disable this feature and configure the ACE to not allow a CRLF in the header. When the ACE encounters a CRLF, it considers it a parsing error and reacts according to how you set the Enable Drop on Parsing Error field. This is the default setting.
Content Max. Parse Length (Bytes)	Maximum number of bytes to parse in HTTP content. Valid entries are from 1 to 65535. The default is 4096.
Header Max. Parse Length (Bytes)	Maximum number of bytes to parse for the total length of cookies, HTTP headers, and URLs. Valid entries are from 1 to 65535. The default is 4096.
Secondary Cookie Delimiters	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	Option that appears only for ACE appliances (all versions) and ACE modules version A4(1.0) and later. In the field on the left, enter the Multipurpose Internet Mail Extension (MIME) type to compress, and click **Add**. The MIME type appears in the column on the right. To remove or change a MIME type, choose it in the column on the right, and click **Remove**. The selected MIME type appears in the field on the left where you can modify or delete it. To specify the sequence in which compression is to be applied, choose MIME types in the column on the right, and click **Up** or **Down** to arrange the MIME types. The "Supported MIME Types" section on page 10-28 lists the supported MIME types. You can use an asterisk (*) to indicate a wildcard, such as text/*, which would include all text MIME types (text/html, text/plain, and so on).

Table 10-5 HTTP Parameter Map Attributes (continued)

Field	Description
User Agent Not To Compress	Option that appears only for ACE appliances (all versions) and ACE modules version A4(1.0) and later. 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. In the field on the left, enter the user agent string to be matched, and click **Add**. The string appears in the column on the right. To remove or change a user agent string, choose it in the column on the right, and click **Remove**. The selected string appears in the field on the left where you can modify or delete it. To specify the sequence in which strings are to be matched, choose strings in the column on the right, and click **Up** or **Down** to arrange the strings in the desired sequence. Valid entries are 64 characters.
Min. Size To Compress (Bytes)	Option that appears only for ACE appliances (all versions) and ACE modules version A4(1.0) and later. Enter the threshold at which compression is to occur. The ACE compresses files that are the minimum size or larger. Valid entries are from 1 to 4096 bytes.

Step 4 Do one of the following:

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

Related Topics

- Configuring Parameter Maps, page 10-1
- Configuring Traffic Policies, page 14-1
- Configuring Parameter Maps, page 10-1
- Configuring Virtual Contexts, page 6-8

Configuring Optimization Parameter Maps

Note Optimization parameter maps are available for ACE appliances only.

You can configure an optimization parameter map for use with a Layer 3/Layer 4 policy map. Optimization parameter maps specify optimization-related commands that pertain to application acceleration and optimization functions performed by the ACE.

See the "Configuring Application Acceleration and Optimization" section on page 15-1 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 Choose **Config** > **Devices** > *context* > **Load Balancing** > **Parameter Maps** > **Optimization Parameter Maps**.

The Optimization Parameter Maps table appears.

Step 2 In the Optimization Parameter Maps table, click **Add** to add a new parameter map, or choose an existing parameter map and click **Edit** to modify it.

The Optimization Parameter Maps configuration window appears.

Step 3 In the Optimization Parameter Maps configuration window, configure the parameter map using the information in Table 10-6.

Table 10-6 Optimization Parameter Map Attributes

Field	Description
Parameter Name	Unique name for the parameter map. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters.
Description	Field that appears for ACE module A2(1.5), ACE appliance A3(2.3), and later releases of either device type. If you attempt to use the Description feature with an ACE that is running an earlier software version, ANM displays an invalid command detected error message and does not deploy the parameter map. Brief description of the parameter map. Enter a text string with a maximum of 240 alphanumeric characters (A–Z, a–z, 0–9). Spaces and special characters are allowed. Double quotes must be entered as matching pairs.
Set Browser Freshness Period	Method that the ACE uses to determine the freshness of objects in the client's browser: • **N/A**—This option is not configured. • **Disable Browser Object Freshness Control**—Browser freshness control is not used. • **Set Freshness Similar To Flash Forward Objects**—The ACE sets freshness similar to that used for FlashForwarded objects and to use the values specified in the Maximum Time for Cache Time-To-Live and Minimum Time for Cache Time-To-Live fields.
Duration For Browser Freshness (Seconds)	Field that 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 (Comma Separated)	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 from 100 to 599, inclusive.
Appscope Optimize Rate (%)	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. The default is 10 percent. The sum of this value and the value entered in the Passthru Rate Percent field must not exceed 100.

Table 10-6 Optimization Parameter Map Attributes (continued)

Field	Description
Appscope Passthrough Rate (%)	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. The default is 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)	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 from 0 to 10,000 bytes.
Max. For Post Data to Scan for Logging (KBytes)	Maximum number of kilobytes of POST data that the ACE is to scan for parameters for the purpose of logging transaction parameters in the statistics log. Valid entries are from 0 to 1000 KB.
String For Grouping Requests	String that the ACE uses 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. For example, to define a string that is used to identify the URLs http://server/catalog.asp?region=asia and http://server/catalog.asp?region=america as two separate reporting categories, you would enter **http_query_param(region)**. Valid entries are from 1 to 255 characters and can contain the parameter expander functions listed in Table 10-7.
Base File Anonymous Level	Base file anonymous level. Information that is common to a large set of users is generally not confidential or user-specific. Conversely, information that is unique to a specific user or a small set of users is generally confidential or user-specific. The anonymous base file feature enables the ACE to create and deliver condensed base files that contain only information that is common to a large set of users. No information unique to a particular user, or across a very small subset of users, is included in anonymous base files. Enter the value for base file anonymity for the all-user condensation method. Valid entries are from 0 to 50. The default is 0, which disables the base file anonymity feature.
Cache-Key Modifier Expression	Cache key modifier expression. A cache object key is a unique identifier that is used to identify a cached object to be served to a client, replacing a trip to the origin server. The cache key modifier feature allows you to modify the canonical form of a URL; that is, the portion before “?” in a URL. For example, the canonical URL of http://www.xyz.com/somepage.asp?action=browse&level=2 is http://www.xyz.com/somepage.asp. Enter a regular expression containing embedded variables as described in Table 10-7. The ACE transforms URLs specified in class maps for this virtual server with the expression and variable entered here. Valid entries are unquoted text strings with no spaces and a maximum of 255 alphanumeric characters. If the string includes spaces, enclose the string with quotation marks (“).
Min. Time For Cache Time-To-Live (Seconds)	Minimum number of seconds that an object without an explicit expiration time should be considered fresh in the ACE cache. This value specifies the minimum time that content can be cached. If the ACE is configured for FlashForward optimization, this value should normally be 0. If the ACE is configured for dynamic caching, this value should indicate how long the ACE should cache the page. (See Table 7-17 for information about these configuration options.) Valid entries are from 0 to 2147483647 seconds.

Table 10-6 Optimization Parameter Map Attributes (continued)

Field	Description
Max. Time For Cache Time-To-Live (Seconds)	Maximum number of seconds that an object without an explicit expiration time should be considered fresh in the ACE cache. Valid entries are from 0 to 2147483647 seconds.
Cache Time-To-Live Duration (%)	Percentage of an object's age at which an embedded object without an explicit expiration time is considered fresh. Valid entries are from 0 to 100 percent.
Expression To Modify Cache Key Query Parameter	Regular expression that contains embedded variables as described in Table 10-7. The ACE transforms URLs specified in class maps for this virtual server with the expression and variable entered here. The cache parameter feature allows you to modify the query parameter of a URL; that is, the portion after "?" in a URL. For example, the query parameter portion of http://www.xyz.com/somepage.asp?action=browse&level=2 is action=browse&level=2. If no string is specified, the query parameter portion of the URL is used as the default value for this portion of the cache key. Valid entries are unquoted text strings with no spaces and a maximum of 255 alphanumeric characters.
Canonical URL Expressions (Comma Separated)	Comma-separated list of parameter expander functions as defined in Table 10-7 to identify the URLs to associate with this parameter map. 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. Valid entries are unquoted text strings with a maximum of 255 alphanumeric characters.
Enable Cacheable Content Optimization	Check box that enables delta optimization of content that can be cached. This feature allows the ACE to detect content that can be cached and perform delta optimization on it. Uncheck the check box to disable this feature.
Enable Delta Optimization On First Visit To Web Page	Check box that enables condensation on the first visit to a web page. Uncheck the check box to disable this feature.
Min. Page Size For Delta Optimization (Bytes)	Minimum page size, in bytes, that can be condensed. Valid entries are from 1 to 250000 bytes.
Max. Page Size For Delta Optimization (Bytes)	Maximum page size, in bytes, that can be condensed. Valid entries are from 1 to 250000 bytes.
Set Default Client Script	Scripting language that the ACE recognizes on condensed content pages: • **N/A**—This option is not configured. • **Javascript**—The default scripting language is JavaScript. • **Visual Basic Script**—The default scripting language is Visual Basic.
Exclude Iframes From Delta Optimization	Check box that specifies that delta optimization is not to be applied to IFrames (inline frames). Uncheck the check box to indicate that delta optimization is to be applied to IFrames.

Table 10-6 Optimization Parameter Map Attributes (continued)

Field	Description
Exclude Non-ASCII Data From Delta Optimization	Check box that specifies that delta optimization is not to be applied to non-ASCII data. Uncheck the check box to indicate that delta optimization is to be applied to non-ASCII data.
Exclude JavaScripts From Delta Optimization	Check box that specifies that delta optimization is not to be applied to JavaScript. Clear the check box to indicate that delta optimization is to be applied to JavaScript.
MIME Types To Exclude From Delta Optimization	Mime types to exclude from delta optimization. Do the following: 1. In the first field, enter a comma-separated list of the MIME (Multipurpose Internet Mail Extension) type messages that are not to have delta optimization applied, such as image/Jpeg, text/html, application/msword, or audio/mpeg. See the "Supported MIME Types" section on page 10-28 for a list of supported MIME types. 2. Click **Add** to add the entry to the list box on the right. You can position the entries in the list box by using the Up and Down buttons.
Remove HTML META Elements From Documents	Check box that specifies that HTML META elements are to be removed from documents to prevent them from being condensed. Uncheck the check box to indicate that HTML META elements are not to be removed from documents.
Set Flash Forward Refresh Policy	Method the ACE is to use to refresh stale embedded objects: • **N/A**—This option is not configured. • **Allow Flash Forward To Indirect Refresh Of Objects**—The ACE uses FlashForward to indirectly refresh embedded objects. • **Bypass Flash Forward To Direct Refresh Of Objects**—The ACE bypasses FlashForward for stale embedded objects so that they are refreshed directly.
Rebase Delta Optimization Threshold (%)	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 from 0 to 10000 percent.
Rebase Flash Forward Threshold (%)	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 from 0 to 10000 percent.
Rebase History Size (Pages)	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 from 10 to 2147483647.
Rebase Modify Cool-Off Period (Seconds)	Number of seconds after the last modification before performing a rebase. Valid entries are from 1 to 14400 seconds (4 hours).
Rebase Reset Period (Seconds)	Period of time, in seconds, for performing a meta data refresh. Valid entries are from 1 to 900 seconds (15 minutes).

Table 10-6 Optimization Parameter Map Attributes (continued)

Field	Description
Override Client Request Headers	Action that the ACE takes to handle client request headers (primarily for embedded objects): • **N/A**—This feature is not enabled. • **All Cache Request Headers Are Ignored**—The ACE ignores all cache request headers. • **Overrides The Cache Control: No Cache HTTP Header From A Request**—The ACE ignores cache control request headers that state *no cache*.
Override Server Response Headers	Action that the ACE takes to handle origin server response headers (primarily for embedded objects): • **N/A**—This feature is not enabled. • **All Cache Request Headers Are Ignored**—The ACE ignores all response headers. • **Overrides The Cache Control: Private HTTP Header From A Response**—The ACE ignores cache control response headers that state *private*.
UTF-8 Character Set Threshold	UTF-8 (8-bit Unicode Transformation Format) character set, which 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. 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 from 1 to 1,000,000.
Server Load Threshold Trigger (%)	Server load threshold trigger that 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. Enter the threshold, expressed as a percent, at which the TTL for cached objects is to be changed. Valid entries are from 0 to 100 percent.
Server Load Time-To-Live Change (%)	Option that 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. Enter the percent by which the cache TTL is to be increased or decreased when the server load threshold trigger is met. Valid entries are from 0 to 100 percent.

Table 10-6 Optimization Parameter Map Attributes (continued)

Field	Description
Delta Optimization Mode	Method by which delta optimization is to be implemented. The choices are as follows: • **N/A**—This option is not configured. • **Enable The 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. • **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.
String To Be Used For Server HTTP Header	Option that defines 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. Enter the string that is to appear in the server header. Valid entries are quoted text strings with a maximum of 64 alphanumeric characters.

Table 10-7 lists the parameter expander functions that you can use.

Table 10-7 Parameter Expander Functions

Variable	Description
$(*number*)	Expands to the corresponding matching subexpression (by *number*) in the URL pattern. Subexpressions are marked in a URL pattern using parentheses (). The numbering of the subexpressions begins with 1 and is the number of the left-parenthesis "(" counting from the left. You can specify any positive integer for the number. $(0) matches the entire URL. For example, if the URL pattern is ((http://server/.*)/(.*)/)a.jsp, and the URL that matches it is http://server/main/sub/a.jsp?category=shoes&session=99999, then the following are correct: $(0) = http://server/main/sub/a.jsp $(1) = http://server/main/sub/ $(2) = http://server/main $(3) = sub If the specified subexpression does not exist in the URL pattern, then the variable expands to the empty string.
$http_query_string()	Expands to the value of the whole query string in the URL. For example, if the URL is http://myhost/dothis?param1=value1&param2=value2, then the following is correct: $http_query_string() = param1=value1&param2=value2 This function applies to both GET and POST requests.
$http_query_param(*query-param-name*) The obsolete syntax is also supported: $param(*query-param-name*)	Expands to the value of the named query parameter (case sensitive). For example, if the URL is http://server/main/sub/a.jsp?category=shoes&session=99999, then the following are correct: $http_query_param(category) = shoes $http_query_param(session) = 99999 If the specified parameter does not exist in the query, then the variable expands to the empty string. This function applies to both GET and POST requests.
$http_cookie(*cookie-name*)	Evaluates to the value of the named cookie. For example, $http_cookie(cookiexyz). The cookie name is case sensitive.
$http_header(*request-header-name*)	Evaluates to the value of the specified HTTP request header. In the case of multivalued headers, it is the single representation as specified in the HTTP specification. For example, $http_header(user-agent). The HTTP header name is not case sensitive.
$http_method()	Evaluates to the HTTP method used for the request, such as GET or POST.

Table 10-7 Parameter Expander Functions (continued)

Variable	Description
Boolean Functions: $http_query_param_present(*query-param-name*) $http_query_param_notpresent(*query-param-name*) $http_cookie_present(*cookie-name*) $http_cookie_notpresent(*cookie-name*) $http_header_present(*request-header-name*) $http_header_notpresent(*request-header-name*) $http_method_present(*method-name*) $http_method_notpresent(*method-name*)	Evaluates to a Boolean value: True or False, depending on the presence or absence of the element in the request. The elements are a specific query parameter (*query-param-name*), a specific cookie (*cookie-name*), a specific request header (*request-header-name*), or a specific HTTP method (*method-name*). All identifiers are case sensitive except for the HTTP request header name.
$regex_match(*param1*, *param2*)	Evaluates to a Boolean value: True if the two parameters match and False if they do not match. The two parameters can be any two expressions, including regular expressions, that evaluate to two strings. For example, this function: `$regex_match($http_query_param(URL), .*Store\.asp.*)` compares the query URL with the regular expression string .*Store\.asp.* If the URL matches this regular expression, this function evaluates to True.

Step 4 Do one of the following:

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

Related Topics

- Configuring Parameter Maps, page 10-1
- Configuring Traffic Policies, page 14-1
- Configuring Parameter Maps, page 10-1
- Configuring Virtual Contexts, page 6-8

Configuring RTSP Parameter Maps

You can configure a Real Time Streaming protocol (RTSP) parameter map, which allows you to configure advanced RTSP behavior for server load-balancing connections.

Procedure

Step 1 Choose **Config > Devices >** *context* **> Load Balancing > Parameter Maps > RTSP Parameter Maps**.

The RTSP Parameter Maps table appears.

Step 2 In the RTSP Parameter Maps table, click **Add** to add a new parameter map, or choose an existing parameter map and click **Edit** to modify it.

The Parameter Maps configuration window appears.

Step 3 In the Parameter Maps configuration window, configure the parameter map using the information in Table 10-8.

Table 10-8 RTSP Parameter Map Attributes

Field	Description
Parameter Name	Unique name for the parameter map. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters.
Description	Field that appears for ACE module A2(1.5), ACE appliance A3(2.3), and later releases of either device type. If you attempt to use the Description feature with an ACE that is running an earlier software version, ANM displays an invalid command detected error message and does not deploy the parameter map. Brief description of the parameter map. Enter a text string with a maximum of 240 alphanumeric characters (A–Z, a–z, 0–9). Spaces and special characters are allowed. Double quotes must be entered as matching pairs.
Case-Insensitive	Check box that instructs the ACE to be case insensitive. Uncheck the check box to instruct the ACE is to be case sensitive.
Header Max. Parse Length (Bytes)	Number of bytes to parse for the total length of RTSP headers. Valid entries are from 1 to 65535. The default is 2048 bytes.

Step 4 Do one of the following:

- Click **Deploy Now** to deploy this configuration on the ACE and save your entries to the running-configuration and startup-configuration files.
- Click **Cancel** to exit this procedure without saving your entries and to return to the RTSP Parameter Maps table.
- Click **Next** to deploy your entries and to configure another RTSP parameter map.

Related Topics

- Configuring Parameter Maps, page 10-1
- Configuring Traffic Policies, page 14-1
- Configuring Parameter Maps, page 10-1

- Configuring Virtual Contexts, page 6-8

Configuring SIP Parameter Maps

You can configure Session Initiation Protocol (SIP) parameter maps, which allow you to configure SIP deep-packet inspection policy maps on the ACE.

Procedure

Step 1 Choose **Config** > **Devices** > *context* > **Load Balancing** > **Parameter Maps** > **SIP Parameter Maps**.

The SIP Parameter Maps table appears.

Step 2 In the SIP Parameter Maps table, click **Add** to add a new parameter map, or choose an existing parameter map and click **Edit** to modify it.

The Parameter Maps configuration window appears.

Step 3 In the Parameter Maps configuration window, configure the parameter map using the information in Table 10-9.

Table 10-9 SIP Parameter Map Attributes

Field	Description
Parameter Name	Unique name for the parameter map. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters.
Description	Field that appears for ACE module A2(1.5), ACE appliance A3(2.3), and later releases of either device type. If you attempt to use the Description feature with an ACE that is running an earlier software version, ANM displays an invalid command detected error message and does not deploy the parameter map. Brief description of the parameter map. Enter a text string with a maximum of 240 alphanumeric characters (A–Z, a–z, 0–9). Spaces and special characters are allowed. Double quotes must be entered as matching pairs.
Instant Messaging	Check box that enables instant messaging (IM) over SIP after it has been disabled. Uncheck this check box to disable this feature.
Logging All	Check box that appears only for ACE module and ACE appliance software Version A4(1.0) or later. Check this check box to enable logging of all received and transmitted SIP packets in the system log (syslog) in addition to the dropped packets, which by default are logged. The ACE allows all headers sent in the SIP packet, including proprietary headers. In the event of a failover for SIP sessions over UDP, the ACE continues to process SIP packets for established SIP sessions. Uncheck this check box to disable this feature.

Table 10-9 SIP Parameter Map Attributes (continued)

Field	Description
Max. Forward Validation	Option that 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. The choices are as follows: • **N/A**—The ACE is not to validate Max-Forward header fields. • **Drop**—The ACE is to drop the SIP message if it does not pass Max-Forward header validation. • **Deny**—The ACE is to reset the SIP connection if it does not pass Max-Forward header validation.
Log Max. Forward Validation Event	Check box that instructs the ACE to log Max-Forward validation events. Uncheck the check box to disable this feature.
Mask UA Software Version	Check box that instructs the ACE to mask the user agent 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. Uncheck the check box to disable this feature.
Log UA Software Version	Check box that instructs the ACE to log the user agent software version. Uncheck the check box to disable this feature.
Strict Header Validation	Action that the ACE is to take to handle 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: • From • To • Call-ID • CSeq • Via • Max-Forwards 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. The choices are as follows: • **N/A**—The ACE does not to perform header validation. • **Drop**—The ACE drops the SIP message if the SIP packet does not pass header validation. • **Reset**—The ACE resets the connection if the SIP packet does not pass header validation.
Log Strict Header Validation	Check box that instructs the ACE to log header validation events. Uncheck the check box to disable this feature.
Mask Non SIP URI	Check box that instructs the ACE to mask non-SIP URIs in SIP messages. This option and the next enable the detection of non-SIP URIs in SIP messages. Uncheck the check box to disable this feature.

Table 10-9 SIP Parameter Map Attributes (continued)

Field	Description
Log Non SIP URI	Check box that instructs the ACE to log non-SIP URIs in SIP messages. Uncheck the check box to disable this feature.
SIP Media Pinhole Timeout (Seconds)	Timeout period for SIP media pinhole (secure port) connections in seconds. Valid entries are from 1 to 65535 seconds. The default is 5.

Step 4 Do one of the following:

- Click **Deploy Now** to deploy this configuration on the ACE and save your entries to the running-configuration and startup-configuration files.
- Click **Cancel** to exit this procedure without saving your entries and to return to the SIP Parameter Maps table.
- Click **Next** to deploy your entries and to configure another SIP parameter map.

Related Topics

- Configuring Parameter Maps, page 10-1
- Configuring Traffic Policies, page 14-1
- Configuring Parameter Maps, page 10-1
- Configuring Virtual Contexts, page 6-8

Configuring Skinny Parameter Maps

You can configure Skinny Client Control Protocol (SCCP or Skinny) parameter maps, which allow you to configure SCCP packet inspection on the ACE.

Procedure

Step 1 Choose **Config** > **Devices** > *context* > **Load Balancing** > **Parameter Maps** > **Skinny Parameter Maps**.

The Skinny Parameter Maps table appears.

Step 2 In the Skinny Parameter Maps table, click **Add** to add a new parameter map, or choose an existing parameter map and click **Edit** to modify it.

The Parameter Maps configuration window appears.

Step 3 In the Parameter Maps configuration window, configure the parameter map using the information in Table 10-10.

Table 10-10 Skinny Parameter Map Attributes

Field	Description
Parameter Name	Unique name for the parameter map. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters.
Description	Field that appears for ACE module A2(1.5), ACE appliance A3(2.3), and later releases of either device type. If you attempt to use the Description feature with an ACE that is running an earlier software version, ANM displays an invalid command detected error message and does not deploy the parameter map. Brief description of the parameter map. Enter a text string with a maximum of 240 alphanumeric characters (A–Z, a–z, 0–9). Spaces and special characters are allowed. Double quotes must be entered as matching pairs.
Enforce Registration	Check box that enables Skinny registration enforcement. 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 CCM, the ACE opens a secure port (pinhole) to allow that client to make a call. Uncheck the check box to disable this feature.
Message Id Max	Maximum value for the station message ID in hexadecimal that the ACE is to accept. Valid entries are hexadecimal values from 0x0 to 0x4000 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. **Note** The Message Id Max. hexadecimal value should always start with 0x or 0X.
Min. SCCP Prefix Length (Bytes)	Minimum SCCP prefix length in bytes. 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. Valid entries are from 4 to 4000 bytes.
Max. SCCP Prefix Length (Bytes)	Maximum SCCP prefix length in bytes. 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. Valid entries are from 4 to 4000 bytes.

Step 4 Do one of the following:

- Click **Deploy Now** to deploy this configuration on the ACE and save your entries to the running-configuration and startup-configuration files.
- Click **Cancel** to exit this procedure without saving your entries and to return to the Skinny Parameter Maps table.
- Click **Next** to deploy your entries and to configure another Skinny parameter map.

Related Topics

- Configuring Parameter Maps, page 10-1

- Configuring Traffic Policies, page 14-1
- Configuring Virtual Contexts, page 6-8

Configuring DNS Parameter Maps

You can configure Domain Name System (DNS) parameter maps, which allow you to configure DNS actions for DNS packet inspection.

Procedure

Step 1 Choose **Config** > **Devices** > *context* > **Load Balancing** > **Parameter Maps** > **DNS Parameter Maps**.

The DNS Parameter Maps table appears.

Step 2 In the DNS Parameter Maps table, click **Add** to add a new parameter map, or choose an existing parameter map and click **Edit** to modify it.

The DNS Parameter Maps configuration window appears.

Step 3 In the DNS Parameter Maps configuration window, configure the parameter map using the information in Table 10-11.

Table 10-11 DNS Parameter Map Attributes

Field	Description
Parameter Name	Unique name for the parameter map. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters.
Description	Field that appears for ACE module A2(1.5), ACE appliance A3(2.3), and later releases of either device type. If you attempt to use the Description feature with an ACE that is running an earlier software version, ANM displays an invalid command detected error message and does not deploy the parameter map. Brief description of the parameter map. Enter a text string with a maximum of 240 alphanumeric characters (A–Z, a–z, 0–9). Spaces and special characters are allowed. Double quotes must be entered as matching pairs.
Timeout (Seconds)	Amount of time in seconds that the ACE keeps the query entries without answers in the hash table before timing them out. Configure the ACE to time out DNS queries that have no matching server response. Specify the Enter an integer from 2 to 120 seconds. The default is 10 seconds.

Step 4 Do one of the following:

- Click **Deploy Now** to deploy this configuration on the ACE and save your entries to the running-configuration and startup-configuration files.
- Click **Cancel** to exit this procedure without saving your entries and to return to the DNS Parameter Maps table.
- Click **Next** to deploy your entries and to configure another DNS parameter map.

Related Topics

- Configuring Parameter Maps, page 10-1

- Configuring Traffic Policies, page 14-1
- Configuring Virtual Contexts, page 6-1

Configuring RDP Parameter Maps

Note RDP parameter maps require ACE software Version A5(2.0) or later.

Remote Desktop Protocol (RDP) parameter maps configure routing-token-rebalance in which the ACE redirects connections that contain RDP packets to another server when the real server that matches the routing token information in the client request is down.

Use this procedure to configure a RDP parameter map.

Procedure

Step 1 Choose **Config > Virtual Contexts >** ***context*** **> Load Balancing > Parameter Maps > RDP Parameter Maps**. The RDP Parameter Maps table appears.

Step 2 From the RDP Parameter Maps table, click **Add** to add a new parameter map, or choose an existing parameter map, and then click **Edit** to modify it. The New Parameter Map configuration table appears.

Step 3 From the New Parameter Map table, configure the parameter map using the information in Table 10-12.

Table 10-12 RDP 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.
Description	Brief description of the parameter map. Enter a text string with a maximum of 240 alphanumeric characters (A–Z, a–z, 0–9). Spaces and special characters are allowed. Double quotes must be entered as matching pairs.
Routing Token Rebalance	Check this check box to enable routing-token-rebalance. Uncheck this check box to disable routing-token-rebalance and have the ACE drop the RDP packets when the real server that matches the routing token information is down.

Step 4 Do one of the following:

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

Related Topics

- Configuring Parameter Maps, page 10-1
- Configuring Traffic Policies, page 14-1

- Configuring Virtual Contexts, page 6-1

Supported MIME Types

The ACE supports the 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
- 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