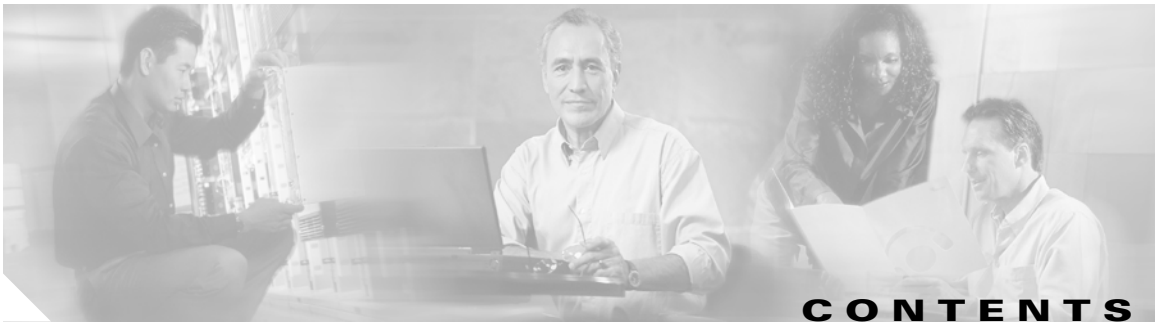
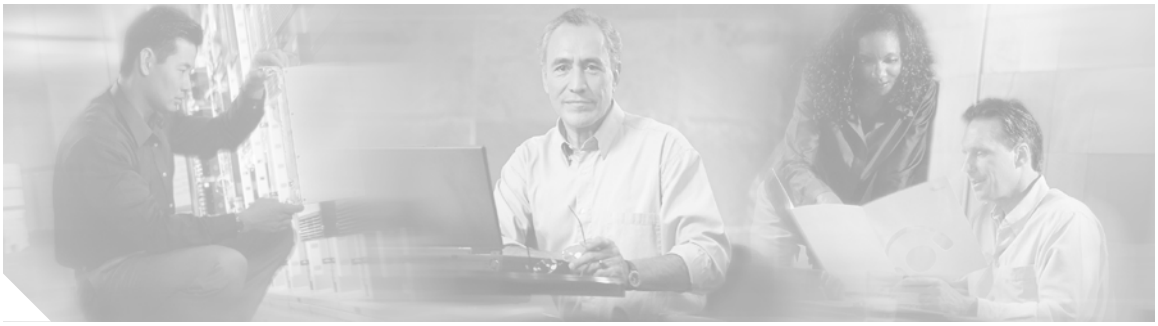
Catalyst 6500 Series Switch SSL Services Module Command Reference

Release 2.1

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Text Part Number: OL-4779-01





Preface

This preface describes the audience, organization, and conventions of this publication, and provides information on how to obtain related documentation.

Audience

This publication is for experienced network administrators who are responsible for configuring and maintaining Catalyst 6500 series switches.

Organization

This publication is organized as follows:

Chapter	Title	Description
Chapter 1	Command-Line Interface	Describes the Catalyst 6500 series switch CLI.
Chapter 2	Commands for the Catalyst 6500 Series Switch SSL Services Module	Lists alphabetically and provides detailed information for commands specific to the Catalyst 6500 series switch SSL Services Module.
Appendix A	Acronyms	Defines the acronyms used in this publication.

Related Documentation

The Catalyst 6500 series switch Cisco IOS documentation set includes these documents:

- *Catalyst 6500 Series Switch SSL Services Module Configuration Note*
- *Catalyst 6500 Series Switch Cisco IOS Software Configuration Guide*
- *Catalyst 6500 Series Switch SSL Services Module System Message Guide*
- *Catalyst 6500 Series Switch SSL Services Module Installation and Verification Note*
- *Release Notes for Catalyst 6500 Series Switch SSL Services Module Release 2.1*

The Cisco IOS documentation set includes these documents:

- *Configuration Fundamentals Configuration Guide*
- *Command Reference*

For information about MIBs, refer to this URL:

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

Conventions

This document uses the following conventions:

Convention	Description
boldface font	Commands, command options, and keywords are in **boldface**.
italic font	Arguments for which you supply values are in *italics*.
[ ]	Elements in square brackets are optional.
{ x | y | z }	Alternative keywords are grouped in braces and separated by vertical bars. Braces can also be used to group keywords and/or aguments; for example, {**interface** *interface* **type**}.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
`screen` font	Terminal sessions and information the system displays are in `screen` font.
`boldface screen` font	Information you must enter is in **`boldface screen`** font.
italic screen font	Arguments for which you supply values are in *italic screen* font.
^	The symbol ^ represents the key labeled Control—for example, the key combination ^D in a screen display means hold down the Control key while you press the D key.
< >	Nonprinting characters, such as passwords are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Notes use the following conventions:

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the publication.

Cautions use the following conventions:

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Obtaining Documentation

Cisco provides several ways to obtain documentation, technical assistance, and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation on the World Wide Web at this URL:

http://www.cisco.com/cisco/web/psa/default.html?mode=prod

You can access the Cisco website at this URL:

http://www.cisco.com

International Cisco websites can be accessed from this URL:

http://www.cisco.com/web/siteassets/locator/index.html

Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which may have shipped with your product. The Documentation CD-ROM is updated regularly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual or quarterly subscription.

Registered Cisco.com users can order a single Documentation CD-ROM (product number DOC-CONDOCCD=) through the Cisco Ordering tool:

http://www.cisco.com/en/US/ordering/index.shtml

All users can order annual or quarterly subscriptions through the online Subscription Store:

http://www.cisco.com/go/subscription

Click Subscriptions & Promotional Materials in the left navigation bar.

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/en/US/ordering/index.shtml

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/en/US/ordering/index.shtml

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can submit e-mail comments about technical documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, the Cisco Technical Assistance Center (TAC) provides 24-hour-a-day, award-winning technical support services, online and over the phone. Cisco.com features the Cisco TAC website as an online starting point for technical assistance. If you do not hold a valid Cisco service contract, please contact your reseller.

Cisco TAC Website

The Cisco TAC website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The Cisco TAC website is available 24 hours a day, 365 days a year. The Cisco TAC website is located at this URL:

http://www.cisco.com/tac

Accessing all the tools on the Cisco TAC website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a login ID or password, register at this URL:

http://tools.cisco.com/RPF/register/register.do

Opening a TAC Case

Using the online TAC Case Open Tool is the fastest way to open P3 and P4 cases. (P3 and P4 cases are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Case Open Tool automatically recommends resources for an immediate solution. If your issue is not resolved using the recommended resources, your case will be assigned to a Cisco TAC engineer. The online TAC Case Open Tool is located at this URL:

https://tools.cisco.com/RPF/register/register.do

For P1 or P2 cases (P1 and P2 cases are those in which your production network is down or severely degraded) or if you do not have Internet access, contact Cisco TAC by telephone. Cisco TAC engineers are assigned immediately to P1 and P2 cases to help keep your business operations running smoothly.

To open a case by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553-2447

For a complete listing of Cisco TAC contacts, go to this URL:

http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html

TAC Case Priority Definitions

To ensure that all cases are reported in a standard format, Cisco has established case priority definitions.

Priority 1 (P1)—Your network is “down” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Priority 2 (P2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Priority 3 (P3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Priority 4 (P4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The Cisco Product Catalog describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the Cisco Product Catalog at this URL:

  http://www.cisco.com/en/US/products/index.html

- Cisco Press publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press online at this URL:

  http://www.ciscopress.com

- Packet magazine is the Cisco quarterly publication that provides the latest networking trends, technology breakthroughs, and Cisco products and solutions to help industry professionals get the most from their networking investment. Included are networking deployment and troubleshooting tips, configuration examples, customer case studies, tutorials and training, certification information, and links to numerous in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/web/about/ac123/ac114/about_cisco_packet_magazine.html

- iQ Magazine is the Cisco bimonthly publication that delivers the latest information about Internet business strategies for executives.

- Internet Protocol Journal is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/web/about/ac123/ac147/about_cisco_the_internet_protocol_journal.html

- Training—Cisco offers world-class networking training. Current offerings in network training are listed at this URL:

  http://www.cisco.com/web/learning/index.html

Command-Line Interface

This chapter provides information for understanding and using the Catalyst 6500 series switch SSL Services Module software using the command-line interface (CLI). The command line interface (CLI) for the Catalyst 6500 series switch SSL Services Module is based on the Cisco IOS CLI. For information about Cisco IOS commands that are not contained in this publication, refer to the current Cisco IOS documentation including:

- *Cisco IOS Release 12.2 Configuration Fundamentals Configuration Guide*
- *Cisco IOS Release 12.2 Command Reference*

This chapter includes the following sections:

Getting Help

To obtain a list of commands that are available for each command mode, enter a question mark (**?**) at the system prompt. You also can obtain a list of any command's associated keywords and arguments with the context-sensitive help feature.

Table 1-1 lists commands that you can enter to get help that is specific to a command mode, a command, a keyword, or an argument.

Table 1-1 Getting Help

Command	Purpose
*abbreviated-command-entry***?**	Obtain a list of commands that begin with a particular character string. (Do not leave a space between the command and question mark.)
abbreviated-command-entry<**Tab**>	Complete a partial command name.
?	List all commands available for a particular command mode.

Table 1-1 Getting Help (continued)

Command	Purpose
command **?**	List a command's associated keywords. Leave a space between the command and question mark.
command keyword **?**	List a keyword's associated arguments. Leave a space between the keyword and question mark.

This example shows how to obtain a list of commands that begin with a particular character string or complete a partial command name:

```
ssl-proxy# tu?
tunnel

simpson1-2# tu
```

This example shows how to list all commands available for a particular command mode:

```
ssl-proxy(config)# ?
Configure commands:
  aaa                         Authentication, Authorization and
                              Accountin
  access-list                 Add an access list entry
  alias                       Create command alias
  arp                         Set a static ARP entry
  async-bootp                 Modify system bootp parameters
  banner                      Define a login banner
  boot                        Modify system boot parameters
  bridge                      Bridge Group.
  buffers                     Adjust system buffer pool parameters
  cdp                         Global CDP configuration subcommands
  class-map                   Configure QoS Class Map
.
.
.
Output is truncated.
```

This example shows how to list a keyword's associated arguments:

```
ssl-proxy(config-if)# channel-group 1 mode ?
  auto       Enable PAgP only if a PAgP device is detected
  desirable  Enable PAgP unconditionally
  on         Enable Etherchannel only

ssl-proxy(config-if)#
```

How to Find Command Options

This section provides an example of how to display syntax for a command. The syntax can consist of optional or required keywords. To display keywords for a command, enter a question mark (**?**) at the configuration prompt or after entering part of a command followed by a space. The Catalyst 6500 series SSL Services Module software displays a list of available keywords along with a brief description of the keywords. For example, if you are in global configuration mode and want to see all the keywords for the **ssl-proxy** command, you enter **ssl-proxy ?**.

Table 1-2 shows examples of how you can use the question mark (**?**) to assist you in entering commands.

Table 1-2 How to Find Command Options

Command	Comment

`ssl-proxy> enable`
`Password: <password>`
`ssl-proxy#`
	Enter the **enable** command and password to access privileged EXEC commands.
	You are in privileged EXEC mode when the prompt changes to `ssl-proxy#`.

`ssl-proxy# configure terminal`
`Enter configuration commands, one per line. End with CNTL/Z.`
`ssl-proxy(config)#`
	Enter global configuration mode.
	You are in global configuration mode when the prompt changes to `ssl-proxy(config)#`.

`ssl-proxy(config)# crypto ca trustpoint trustpoint-label` `ssl-proxy(ca-trustpoint)#`	Enter the configuration submode. You are in the configuration submode when the prompt displays the submode, for example: `ssl-proxy(ca-trustpoint)#`.
`ssl-proxy(config)# interface` *type mod/port* `ssl-proxy(config-if)#`	From the global configuration mode, you can also enter the interface configuration mode by entering the **interface** global configuration command. You are in interface configuration mode when the prompt changes to `ssl-proxy(config-if)#`.

`ssl-proxy(config-if)# channel-group ?`
`  group  channel-group of the interface`
 	
`ssl-proxy(config-if)#channel-group`
	Enter the command that you want to configure for the controller. In this example, the **channel-group** command is used.
	Enter a **?** to display what you must enter next on the command line. In this example, you must enter the **group** keyword.
	Because a `<cr>` is not displayed, it indicates that you must enter more information to complete the command.

Table 1-2 How to Find Command Options (continued)

Command	Comment

`ssl-proxy(config-if)# channel-group group ?`
`  <1-256>  Channel group number`
 	
`ssl-proxy(config-if)#channel-group group`
	After you enter the **group** keyword, enter a **?** to display what you must enter next on the command line. In this example, you must enter a channel group number from 1 to 256.
	
	Because a <cr> is not displayed, it indicates that you must enter more information to complete the command.

`ssl-proxy(config-if)# channel-group 1 ?`
`  mode  Etherchannel Mode of the interface`
 	
`ssl-proxy(config-if)#`
	After you enter the channel group number, enter a **?** to display what you must enter next on the command line. In this example, you must enter the **mode** keyword.
	
	Because a <cr> is not displayed, it indicates that you must enter more information to complete the command.

`ssl-proxy(config-if)# channel-group 1 mode ?`
`  auto       Enable PAgP only if a PAgP device is detected`
`  desirable  Enable PAgP unconditionally`
`  on         Enable Etherchannel only`
 	
`ssl-proxy(config-if)#`
	After you enter the **mode** keyword, enter a **?** to display what you must enter next on the command line. In this example, you must enter the **auto**, **desirable**, or **on** keyword.
	
	Because a <cr> is not displayed, it indicates that you must enter more information to complete the command.

`ssl-proxy(config-if)# channel-group 1 mode auto ?`
`  <cr>`
 	
`ssl-proxy(config-if)#`
	In this example, the **auto** keyword is entered. After you enter the **auto** keyword, enter a **?** to display what you must enter next on the command line.
	
	Because a <cr> is displayed, it indicates that you can press **Return** to complete the command. If additional keywords are listed, you can enter more keywords or press **Return** to complete the command.

`ssl-proxy(config-if)# channel-group 1 mode auto` `ssl-proxy(config-if)#`	In this example, press **Return** to complete the command.

Understanding Command Modes

This section contains descriptions of the command modes for the Cisco IOS user interface.

Cisco IOS User Interface

The Cisco IOS user interface is divided into many different modes. The commands that are available to you depend on which mode you are currently in. You can obtain a list of commands that are available for each command mode by entering a question mark (**?**) at the system prompt.

When you start a session on the Catalyst 6500 series switch, you begin in user mode, often called EXEC mode. Only a limited subset of the commands are available in EXEC mode. In order to have access to all commands, you must enter privileged EXEC mode. Normally, you must enter a password to enter privileged EXEC mode. From privileged EXEC mode, you can enter any EXEC command or enter global configuration mode. Most EXEC commands are one-time commands, such as **show** commands, which show the current status of a given item, and **clear** commands, which clear counters or interfaces. The EXEC commands are not saved across reboots of the Catalyst 6500 series switch.

The configuration modes allow you to make changes to the running configuration. If you later save the configuration, these commands are stored across Catalyst 6500 series switch reboots. In order to get to the various configuration modes, you must start at global configuration mode where you can enter interface configuration mode, subinterface configuration mode, and a variety of protocol-specific modes.

ROM-monitor mode is a separate mode that is used when the Catalyst 6500 series switch cannot boot properly. If your Catalyst 6500 series switch or access server does not find a valid system image when it is booting, or if its configuration file is corrupted at startup, the system might enter ROM-monitor mode.

Table 1-3 provides a summary of the main command modes.

Table 1-3 Summary of Main Command Modes

Command Mode	Access Method	Prompt	Exit Method
User EXEC	Log in.	`ssl-proxy>`	Use the **logout** command.
Privileged EXEC	From user EXEC mode, enter the **enable** EXEC command.	`ssl-proxy#`	To exit to user EXEC mode, enter the **disable** command. To enter global configuration mode, enter the **configure terminal** privileged EXEC command.
Global configuration	From privileged EXEC mode, enter the **configure terminal** privileged EXEC command.	`ssl-proxy(config)#`	To exit to privileged EXEC mode, enter the **exit** or **end** command or press **Ctrl-Z**. To enter interface configuration mode, enter an **interface** configuration command.
Global configuration submode	From global configuration mode, enter a submode command.	`ssl-proxy(config-submode)#`	To exit to global configuration submode, enter the **exit** command.

Table 1-3 Summary of Main Command Modes (continued)

Command Mode	Access Method	Prompt	Exit Method
Interface configuration	From global configuration mode, enter by specifying an interface with an **interface** command.	`ssl-proxy(config-if)#`	To exit to global configuration mode, enter the **exit** command. To exit to privileged EXEC mode, enter the **exit** command or press **Ctrl-Z**. To enter subinterface configuration mode, specify a subinterface with the **interface** command.
Subinterface configuration	From interface configuration mode, specify a subinterface with an **interface** command.	`ssl-proxy(config-subinterface)#`	To exit to global configuration mode, enter the **exit** command. To enter privileged EXEC mode, enter the **end** command or press **Ctrl-Z**.
ROM monitor	From privileged EXEC mode, enter the **reload** EXEC command. Press the Break key during the first 60 seconds while the system is booting.	`Rommon>`	To exit ROM-monitor mode, you must reload the image by entering the **boot** command. If you use the **boot** command without specifying a file or any other boot instructions, the system boots from the default Flash image (the first image in onboard Flash memory). Otherwise, you can instruct the system to boot from a specific Flash image (using the **boot system flash** *filename* command).

For more information on command modes, refer to the "Using the Command Line Interface" chapter of the *Configuration Fundamentals Configuration Guide*.

Note You can issue EXEC-level Cisco IOS commands (such as **show**, **clear**, and **debug** commands) from within global configuration mode or other modes by issuing the **do** command followed by the EXEC command. See the **do** command for information on how to use this command.

Using the No and Default Forms of Commands

Almost every configuration command has a **no** form. In general, enter the **no** form to disable a function. Use the command without the keyword **no** to reenable a disabled function or to enable a function that is disabled by default. For example, IP routing is enabled by default. To disable IP routing, specify the **no ip routing** command and specify the **ip routing** command to reenable it. This publication provides the complete syntax for the configuration commands and describes what the **no** form of a command does.

Configuration commands can have a **default** form. The **default** form of a command returns the command setting to its default. Most commands are disabled by default, so the **default** form is the same as the **no** form. However, some commands are enabled by default and have variables set to certain default values. In these cases, the **default** form of the command enables the command and sets variables to their default values. This publication describes what the **default** form of a command does if the command is not the same as the **no** form.

Using the CLI String Search

The pattern in the command output is referred to as a string. The CLI string search feature allows you to search or filter any **show** or **more** command output and allows you to search and filter at --More-- prompts. This feature is useful when you need to sort though large amounts of output, or if you want to exclude output that you do not need to see.

With the search function, you can begin unfiltered output at the first line that contains a regular expression that you specify. You can then specify a maximum of one filter per command or start a new search from the --More-- prompt.

A regular expression is a pattern (a phrase, number, or more complex pattern) that software uses to match against **show** or **more** command output. Regular expressions are case sensitive and allow for complex matching requirements. Examples of simple regular expressions are Serial, misses, and 138. Examples of complex regular expressions are 00210..., (is), and [Oo]utput.

You can perform three types of filtering:

- Use the **begin** keyword to begin output with the line that contains a specified regular expression.
- Use the **include** keyword to include output lines that contain a specified regular expression.
- Use the **exclude** keyword to exclude output lines that contain a specified regular expression.

You can then search this filtered output at the --More-- prompts.

Note The CLI string search function does not allow you to search or filter backward through previous output; filtering cannot be specified using HTTP access to the CLI.

Regular Expressions

A regular expression can be a single character that matches the same single character in the command output or multiple characters that match the same multiple characters in the command output. This section describes how to create both single-character patterns and multiple-character patterns and how to create more complex regular expressions using multipliers, alternation, anchoring, and parentheses.

Single-Character Patterns

The simplest regular expression is a single character that matches the same single character in the command output. You can use any letter (A-Z, a-z) or digit (0-9) as a single-character pattern. You can also use other keyboard characters (such as ! or ~) as single-character patterns, but certain keyboard characters have special meaning when used in regular expressions. Table 1-4 lists the keyboard characters with special meaning.

Table 1-4 Characters with Special Meaning

Character	Special Meaning
.	Matches any single character, including white space.
*	Matches 0 or more sequences of the pattern.
+	Matches 1 or more sequences of the pattern.
?	Matches 0 or 1 occurrences of the pattern.

Table 1-4 Characters with Special Meaning (continued)

Character	Special Meaning
^	Matches the beginning of the string.
$	Matches the end of the string.
_ (underscore)	Matches a comma (,), left brace ({), right brace (}), left parenthesis (( ), right parenthesis ( )), the beginning of the string, the end of the string, or a space.

To enter these special characters as single-character patterns, remove the special meaning by preceding each character with a backslash (\). These examples are single-character patterns matching a dollar sign, an underscore, and a plus sign, respectively.

\$ _ \+

You can specify a range of single-character patterns to match against command output. For example, you can create a regular expression that matches a string containing one of the following letters: a, e, i, o, or u. One and only one of these characters must exist in the string for pattern matching to succeed. To specify a range of single-character patterns, enclose the single-character patterns in square brackets ([ ]). For example,

[aeiou]

matches any one of the five vowels of the lowercase alphabet, while

[abcdABCD]

matches any one of the first four letters of the lower- or uppercase alphabet.

You can simplify ranges by entering only the end points of the range separated by a dash (-). Simplify the previous range as follows:

[a-dA-D]

To add a dash as a single-character pattern in your range, include another dash and precede it with a backslash:

[a-dA-D\-]

You can also include a right square bracket (]) as a single-character pattern in your range. To do so, enter the following:

[a-dA-D\-\]]

The previous example matches any one of the first four letters of the lower- or uppercase alphabet, a dash, or a right square bracket.

You can reverse the matching of the range by including a caret (^) at the start of the range. This example matches any letter except the ones listed:

[^a-dqsv]

This example matches anything except a right square bracket (]) or the letter d:

[^\]d]

Multiple-Character Patterns

When creating regular expressions, you can also specify a pattern containing multiple characters. You create multiple-character regular expressions by joining letters, digits, or keyboard characters that do not have special meaning. For example, a4% is a multiple-character regular expression. Put a backslash in front of the keyboard characters that have special meaning when you want to remove their special meaning.

With multiple-character patterns, order is important. The regular expression a4% matches the character a followed by a 4 followed by a % sign. If the string does not have a4%, in that order, pattern matching fails. This multiple-character regular expression

a.

uses the special meaning of the period character to match the letter a followed by any single character. With this example, the strings ab, a!, or a2 are all valid matches for the regular expression.

You can remove the special meaning of the period character by putting a backslash in front of it. In the following expression

a\.

only the string a. matches this regular expression.

You can create a multiple-character regular expression containing all letters, all digits, all keyboard characters, or a combination of letters, digits, and other keyboard characters. These examples are all valid regular expressions:

telebit 3107 v32bis

Multipliers

You can create more complex regular expressions to match multiple occurrences of a specified regular expression by using some special characters with your single- and multiple-character patterns. Table 1-5 lists the special characters that specify “multiples” of a regular expression.

Table 1-5 Special Characters Used as Multipliers

Character	Description
*	Matches 0 or more single- or multiple-character patterns.
+	Matches 1 or more single- or multiple-character patterns.
?	Matches 0 or 1 occurrences of the single- or multiple-character patterns.

This example matches any number of occurrences of the letter a, including none:

a*

This pattern requires that at least one letter a in the string is matched:

a+

This pattern matches the string bb or bab:

ba?b

This string matches any number of asterisks (*):

******

To use multipliers with multiple-character patterns, you enclose the pattern in parentheses. In the following example, the pattern matches any number of the multiple-character string ab:

(ab)*

As a more complex example, this pattern matches one or more instances of alphanumeric pairs (but not none; that is, an empty string is not a match):

([A-Za-z][0-9])+

The order for matches using multipliers (*, +, or ?) is to put the longest construct first. Nested constructs are matched from outside to inside. Concatenated constructs are matched beginning at the left side of the construct. The regular expression matches A9b3, but not 9Ab3 because the letters are specified before the numbers.

Alternation

Alternation allows you to specify alternative patterns to match against a string. You separate the alternative patterns with a vertical bar (|). Exactly one of the alternatives can match the string. For example, the regular expression

codex | telebit

matches the string codex or the string telebit, but not both codex and telebit.

Anchoring

You can match a regular expression pattern against the beginning or the end of the string. That is, you can specify that the beginning or end of a string contains a specific pattern. You "anchor" these regular expressions to a portion of the string using the special characters shown in Table 1-6.

Table 1-6 Special Characters Used for Anchoring

Character	Description
^	Matches the beginning of the string.
$	Matches the end of the string.

This regular expression matches a string only if the string starts with abcd:

^abcd

In contrast, this expression is in a range that matches any single letter, as long as it is not the letters a, b, c, or d:

[^abcd]

With this example, the regular expression matches a string that ends with .12:

$\.12

Contrast these anchoring characters with the special character underscore (_). The underscore matches the beginning of a string (^), the end of a string ($), parentheses ( ), space ( ), braces { }, comma (,), or underscore (_). With the underscore character, you can specify that a pattern exist anywhere in the string.

For example,

_1300_

matches any string that has 1300 somewhere in the string. The string's 1300 can be preceded by or end with a space, brace, comma, or underscore. For example,

{1300_

matches the regular expression, but 21300 and 13000 do not.

Using the underscore character, you can replace long regular expression lists, such as the following:

^1300$ ^1300(space) (space)1300 {1300, ,1300, {1300} ,1300, (1300

with

_1300_

Parentheses for Recall

As shown in the "Multipliers" section on page 1-9, you use parentheses with multiple-character regular expressions to multiply the occurrence of a pattern. You can also use parentheses around a single- or multiple-character pattern to remember a pattern for use elsewhere in the regular expression.

To create a regular expression that recalls a previous pattern, you use parentheses to indicate a remembered specific pattern and a backslash (\) followed by an integer to reuse the remembered pattern. The integer specifies the occurrence of the parentheses in the regular expression pattern. If you have more than one remembered pattern in your regular expression, then \1 indicates the first remembered pattern, \2 indicates the second remembered pattern, and so on.

This regular expression uses parentheses for recall:

a(.)bc(.)\1\2

This regular expression matches an a followed by any character (call it character 1), followed by bc, followed by any character (character 2), followed by character 1 again, and then followed by character 2 again. The regular expression can match aZbcTZT. The software remembers that character 1 is Z and character 2 is T and then uses Z and T again later in the regular expression.

CHAPTER 2

Commands for the Catalyst 6500 Series Switch SSL Services Module

This chapter contains an alphabetical listing of commands for the Catalyst 6500 series switch SSL Services Module.

For additional SSL Services Module information, refer to the following documentation:

- *Catalyst 6500 Series Switch SSL Services Module Configuration Note*
- *Catalyst 6500 Series Switch SSL Services Module Installation and Verification Note*

clear ssl-proxy conn

To clear all TCP connections on the entire system, use the **clear ssl-proxy conn** command.

clear ssl-proxy conn [**service** *name*]

Syntax Description

service *name*	(Optional) Clears the connections for the specified service.

Defaults

This command has no default settings.

Command Modes

EXEC

Command History

Release	Modification
Cisco IOS Release 12.1(13)E and SSL Services Module Release 1.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.

Usage Guidelines

To reset all the statistics counters that the SSL Services Module maintains, use the **clear ssl-proxy connection** command without options.

Examples

This example shows how to clear the connections for the specified service:

```
ssl-proxy# clear ssl-proxy conn service S6
```

This example shows how to clear all TCP connections on the entire system:

```
ssl-proxy# clear ssl-proxy conn
ssl-proxy#
```

clear ssl-proxy session

To clear all entries from the session cache, use the **clear ssl-proxy session** command.

clear ssl-proxy session [**service** *name*]

Syntax Description

service *name*	(Optional) Clears the session cache for the specified service.

Defaults

This command has no default settings.

Command Modes

EXEC

Command History

Release	Modification
SSL Services Module Release 1.2(1)	Support for this command was introduced on the Catalyst 6500 series switches.

Usage Guidelines

To clear all entries from the session cache for all services, use the **clear ssl-proxy session** command without options.

Examples

This example shows how to clear the entries from the session cache for the specified service on the SSL Services Module:

```
ssl-proxy# clear ssl-proxy session service S6
```

This example shows how to clear all entries in the session cache that are maintained on the SSL Services Module:

```
ssl-proxy# clear ssl-proxy session
ssl-proxy#
```

clear ssl-proxy stats

To reset the statistics counters that are maintained in the different system components on the SSL Services Module, use the **clear ssl-proxy stats** command.

clear ssl-proxy stats [**crypto** | **fdu** | **ipc** | **pki** | **service** | **ssl** | **tcp**]

Syntax Description

crypto	(Optional) Clears statistics information about the crypto.
fdu	(Optional) Clears statistics information about the F6DU.
ipc	(Optional) Clears statistics information about the inter-process communications (IPC).
pki	(Optional) Clears information about the public key infrastruture (PKI).
service *name*	(Optional) Clears statistics information for a specific service.
ssl	(Optional) Clears statistics information about the SSL.
tcp	(Optional) Clears statistics information about the TCP.

Defaults

This command has no default settings.

Command Modes

EXEC

Command History

Release	Modification
Cisco IOS Release 12.1(13)E and SSL Services Module Release 1.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.

Usage Guidelines

To reset all the statistics counters that the SSL Services Module maintains, use the **clear ssl-proxy stats** command without options.

Examples

This example shows how to reset the statistics counters that are maintained in the different system components on the SSL Services Module:

```
ssl-proxy# clear ssl-proxy stats crypto
ssl-proxy# clear ssl-proxy stats ipc
ssl-proxy# clear ssl-proxy stats pki
ssl-proxy# clear ssl-proxy stats service S6
```

This example shows how to clear all the statistic counters that the SSL Services Module maintains:

```
ssl-proxy# clear ssl-proxy stats
ssl-proxy#
```

crypto ca export pem

To export privacy-enhanced mail (PEM) files from the SSL Services Module, use the **crypto ca export pem** command.

crypto ca export *trustpoint_label* **pem** {**terminal** {**des** | **3des**} {**url** *url*}} *pass_phrase*

Syntax Description

trustpoint-label	Name of the trustpoint.
terminal	Displays the request on the terminal.
des	Specifies the 56-bit DES-CBC encryption algorithm.
3des	Specifies the 168-bit DES (3DES) encryption algorithm.
url *url*	Specifies the URL location. Valid values are as follows: • **ftp:**—Exports to the FTP: file system • **null:**—Exports to the NULL: file system • **nvram:**—Exports to the NVRAM: file system • **rcp:**—Exports to the RCP: file system • **scp:**—Exports to the SCP: file system • **system:**—Exports to the system: file system • **tftp:**—Exports to the TFTP: file system
pass-phrase	Pass phrase that is used to protect the private key.

Defaults

This command has no default settings.

Command Modes

Global configuration

Command History

Release	Modification
SSL Services Module Release 1.2(1)	Support for this command was introduced on the Catalyst 6500 series switches.

Usage Guidelines

The *pass_phrase* can be any phrase including spaces and punctuation except for "**?**", which has special meaning to the Cisco IOS parser.

Pass-phrase protection associates a pass phrase with the key. The pass phrase is used to encrypt the key when it is exported. When this key is imported, you must enter the same pass phrase to decrypt it.

A key that is marked as unexportable cannot be exported.

You can change the default file extensions when prompted. The default file extensions are as follows:

- public key (.pub)
- private key (.prv)
- certificate (.crt)
- CA certificate (.ca)
- signature key (-sign)
- encryption key (-encr)

Note In SSL software release 1.2, only the private key (.prv), the server certificate (.crt), and the issuer CA certificate (.ca) of the server certificate are exported. To export the whole certificate chain, including all the CA certificates, use a PKCS12 file instead of PEM files.

Examples

This example shows how to export a PEM-formatted file on the SSL Services Module:

```
ssl-proxy(config)# crypto ca import TP5 pem url tftp://10.1.1.1/TP5 password
% Importing CA certificate...
Address or name of remote host [10.1.1.1]?
Destination filename [TP5.ca]?
Reading file from tftp://10.1.1.1/TP5.ca
Loading TP5.ca from 10.1.1.1 (via Ethernet0/0.168): !
[OK - 1976 bytes]

% Importing private key PEM file...
Address or name of remote host [10.1.1.1]?
Destination filename [TP5.prv]?
Reading file from tftp://10.1.1.1/TP5.prv
Loading TP5.prv from 10.1.1.1 (via Ethernet0/0.168): !
[OK - 963 bytes]

% Importing certificate PEM file...
Address or name of remote host [10.1.1.1]?
Destination filename [TP5.crt]?
Reading file from tftp://10.1.1.1/TP5.crt
Loading TP5.crt from 10.1.1.1 (via Ethernet0/0.168): !
[OK - 1692 bytes]
% PEM files import succeeded.
ssl-proxy(config)# end
ssl-proxy#
*Apr 11 15:11:29.901: %SYS-5-CONFIG_I: Configured from console by console
```

Related Commands

crypto ca import pem

crypto ca import pem

To import a PEM-formatted file to the SSL Services Module, use the **crypto ca import pem** command.

crypto ca import *trustpoint_label* **pem** [**exportable**] {**terminal** | **url** *url* | **usage-keys**} *pass_phrase*

Syntax Description

trustpoint-label	Name of the trustpoint.
exportable	(Optional) Specifies the key that can be exported.
terminal	Displays the request on the terminal.
url *url*	Specifies the URL location. Valid values are as follows: • **ftp:**—Exports to the FTP: file system • **null:**—Exports to the null: file system • **nvram:**—Exports to the NVRAM: file system • **rcp:**—Exports to the RCP: file system • **scp:**—Exports to the SCP: file system • **system:**—Exports to the system: file system • **tftp:**—Exports to the TFTP: file system
pass_phrase	Pass phrase.
usage-keys	Specifies that two special-usage key pairs should be generated, instead of one general-purpose key pair.

Defaults

This command has no default settings.

Command History

Global configuration

Command History

Release	Modification
SSL Services Module Release 1.2(1)	Support for this command was introduced on the Catalyst 6500 series switches.

Usage Guidelines

You will receive an error if you enter the pass phrase incorrectly.The *pass_phrase* can be any phrase including spaces and punctuation except for "**?**", which has special meaning to the Cisco IOS parser.

Pass-phrase protection associates a pass phrase with the key. The pass phrase is used to encrypt the key when it is exported. When this key is imported, you must enter the same pass phrase to decrypt it.

When importing RSA keys, you can use a public key or its corresponding certificate.

The **crypto ca import pem** command imports only the private key (.prv), the server certificate (.crt), and the issuer CA certificate (.ca). If you have more than one level of CA in the certificate chain, you need to import the root and subordinate CA certificates before this command is issued for authentication. Use cut-and-paste or TFTP to import the root and subordinate CA certificates.

Examples

This example shows how to import a PEM-formatted file from the SSL Services Module:

```
ssl-proxy(config)# crypto ca import TP5 pem url tftp://10.1.1.1/TP5 password
% Importing CA certificate...
Address or name of remote host [10.1.1.1]?
Destination filename [TP5.ca]?
Reading file from tftp://10.1.1.1/TP5.ca
Loading TP5.ca from 10.1.1.1 (via Ethernet0/0.168): !
[OK - 1976 bytes]

% Importing private key PEM file...
Address or name of remote host [10.1.1.1]?
Destination filename [TP5.prv]?
Reading file from tftp://10.1.1.1/TP5.prv
Loading TP5.prv from 10.1.1.1 (via Ethernet0/0.168): !
[OK - 963 bytes]

% Importing certificate PEM file...
Address or name of remote host [10.1.1.1]?
Destination filename [TP5.crt]?
Reading file from tftp://10.1.1.1/TP5.crt
Loading TP5.crt from 10.1.1.1 (via Ethernet0/0.168): !
[OK - 1692 bytes]
% PEM files import succeeded.
ssl-proxy(config)# end
ssl-proxy#
*Apr 11 15:11:29.901: %SYS-5-CONFIG_I: Configured from console by console
```

Related Commands

crypto ca export pem

crypto ca export pkcs12

To export a PKCS12 file from the SSL Services Module, use the **crypto ca export pkcs12** command.

crypto ca export *trustpoint_label* **pkcs12** *file_system* [*pkcs12_filename*] *pass_phrase*

Syntax Description

trustpoint_label	Specifies the trustpoint label.
file_system	Specifies the file system. Valid values are **scp:, ftp:**, **nvram:**, **rcp:**, and **tftp:**
pkcs12_filename	(Optional) Specifies the name of the PKCS12 file to import.
pass_phrase	Specifies the pass phrase of the PKCS12 file.

Defaults

This command has no default settings.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS Release 12.1(13)E and SSL Services Module Release 1.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.

Usage Guidelines

Imported key pairs cannot be exported.

If you are using SSH, we recommend using SCP (secure file transfer) when exporting a PKCS12 file. SCP authenticates the host and encrypts the transfer session.

If you do not specify *pkcs12_filename*, you will be prompted to accept the default filename (the default filename is the *trustpoint_label*) or enter the filename. For the **ftp:** or **tftp:** value, include the full path in the *pkcs12_filename*.

You will receive an error if you enter the pass phrase incorrectly.

If there is more than one level of CA, the root CA and all the subordinate CA certificates are exported in the PKCS12 file.

Examples

This example shows how to export a PKCS12 file using SCP:

```
ssl-proxy(config)# crypto ca export TP1 pkcs12 scp: sky is blue
Address or name of remote host []? 10.1.1.1
Destination username [ssl-proxy]? admin-1
Destination filename [TP1]? TP1.p12

Password:

Writing TP1.p12 Writing pkcs12 file to scp://admin-1@10.1.1.1/TP1.p12

Password:
!
CRYPTO_PKI:Exported PKCS12 file successfully.
ssl-proxy(config)#
```

crypto ca import pkcs12

To import a PKCS12 file to the SSL Services Module, use the **crypto ca import** command.

crypto ca import *trustpoint_label* **pkcs12** *file_system* [*pkcs12_filename*] *pass_phrase*

Syntax Description

trustpoint_label	Specifies the trustpoint label.
file_system	Specifies the file system. Valid values are as follows: • **ftp:**—Imports from the FTP: file system • **nvram:**—Imports from the NVRAM: file system • **rcp:**—Imports from the RCP: file system • **scp:**—Imports from the SCP: file system • **tftp:**—Imports from the TFTP: file system
pkcs12_filename	(Optional) Specifies the name of the PKCS12 file to import.
pass_phrase	Specifies the pass phrase of the PKCS12 file.

Defaults

This command has no default settings.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS Release 12.1(13)E and SSL Services Module Release 1.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.

Command Modes

If you are using SSH, we recommend using SCP (secure file transfer) when importing a PKCS12 file. SCP authenticates the host and encrypts the transfer session.

If you do not specify *pkcs12_filename*, you will be prompted to accept the default filename (the default filename is the *trustpoint_label*) or to enter the filename. For the **ftp:** or **tftp:** value, include the full path in the *pkcs12_filename*.

You will receive an error if you enter the pass phrase incorrectly.

If there is more than one level of CA, the root CA and all the subordinate CA certificates are exported in the PKCS12 file.

Examples

This example shows how to import a PKCS12 file using SCP:

```
ssl-proxy(config)# crypto ca import TP2 pkcs12 scp: sky is blue
Address or name of remote host []? 10.1.1.1
Source username [ssl-proxy]? admin-1
Source filename [TP2]? /users/admin-1/pkcs12/TP2.p12

Password:password
Sending file modes:C0644 4379 TP2.p12
!
ssl-proxy(config)#
*Aug 22 12:30:00.531:%CRYPTO-6-PKCS12IMPORT_SUCCESS:PKCS #12 Successfully Imported.
ssl-proxy(config)#
```

crypto key export rsa pem

To export a PEM-formatted RSA key to the SSL Services Module, use the **crypto key export rsa pem** command.

crypto key export rsa *keylabel* **pem** {**terminal** | **url** *url*} {{**3des** | **des**} [**exportable**] *pass_phrase*}

Syntax Description

keylabel	Name of the key.
terminal	Displays the request on the terminal.
url *url*	Specifies the URL location. Valid values are as follows: • **ftp:**—Exports to the FTP: file system • **null:**—Exports to the null: file system • **nvram:**—Exports to the NVRAM: file system • **rcp:**—Exports to the RCP: file system • **scp:**—Exports to the SCP: file system • **system:**—Exports to the system: file system • **tftp:**—Exports to the TFTP: file system
des	Specifies the 56-bit DES-CBC encryption algorithm.
3des	Specifies the 168-bit DES (3DES) encryption algorithm.
exportable	(Optional) Specifies that the key can be exported.
pass_phrase	Pass phrase.

Defaults

This command has no default settings.

Command Modes

Global configuration

Command History

Release	Modification
SSL Services Module Release 1.2(1)	Support for this command was introduced on the Catalyst 6500 series switches.

Usage Guidelines

The pass phrase can be any phrase including spaces and punctuation except for "**?**", which has special meaning to the Cisco IOS parser.

Pass-phrase protection associates a pass phrase with the key. The pass phrase is used to encrypt the key when it is exported. When this key is imported, you must enter the same pass phrase to decrypt it.

Examples

This example shows how to export a key from the SSL Services Module:

```
ssl-proxy(config)# crypto key export rsa test-keys pem url scp: 3des password
% Key name:test-keys
   Usage:General Purpose Key
Exporting public key...
Address or name of remote host []? 7.0.0.7
Destination username [ssl-proxy]? lab
Destination filename [test-keys.pub]?

Password:

Writing test-keys.pub Writing file to scp://lab@7.0.0.7/test-keys.pub
Password:
!
Exporting private key...
Address or name of remote host []? 7.0.0.7
Destination username [ssl-proxy]? lab
Destination filename [test-keys.prv]?

Password:

Writing test-keys.prv Writing file to scp://lab@7.0.0.7/test-keys.prv
Password:
ssl-proxy(config)#
```

crypto key import rsa pem

To import a PEM-formatted RSA key from an external system, use the **crypto key import rsa pem** command.

crypto key import rsa *keylabel* **pem** [**usage-keys**] {**terminal** | **url** *url*} [**exportable**] *passphrase*}

Syntax Description

keylabel	Name of the key.
usage-keys	(Optional) Specifies that two special-usage key pairs should be generated, instead of one general-purpose key pair.
terminal	Displays the request on the terminal.
url *url*	Specifies the URL location. Valid values are as follows: • **ftp:**—Imports from the FTP: file system • **null:**—Imports from the null: file system • **nvram:**—Imports from the NVRAM: file system • **rcp:**—Imports from the RCP: file system • **scp:**—Imports from the SCP: file system • **system:**—Imports from the system: file system • **tftp:**—Imports from the TFTP: file system
exportable	(Optional) Specifies that the key can be exported.
passphrase	Pass phrase.

Defaults

This command has no default settings.

Command Modes

Global configuration

Command History

Release	Modification
SSL Services Module Release 1.2(1)	Support for this command was introduced on the Catalyst 6500 series switches.

Usage Guidelines

The pass phrase can be any phrase including spaces and punctuation except for "**?**", which has special meaning to the Cisco IOS parser.

Pass-phrase protection associates a pass phrase with the key. The pass phrase is used to encrypt the key when it is exported. When this key is imported, you must enter the same pass phrase to decrypt it.

Examples

This example shows how to import a PEM-formatted RSA key from an external system and export the PEM-formatted RSA key to the SSL Services Module:

```
ssl-proxy(config)# crypto key import rsa newkeys pem url scp: password
% Importing public key or certificate PEM file...
Address or name of remote host []? 7.0.0.7
Source username [ssl-proxy]? lab
Source filename [newkeys.pub]? test-keys.pub

Password:
Sending file modes:C0644 272 test-keys.pub
Reading file from scp://lab@7.0.0.7/test-keys.pub!
% Importing private key PEM file...
Address or name of remote host []? 7.0.0.7
Source username [ssl-proxy]? lab
Source filename [newkeys.prv]? test-keys.prv

Password:
Sending file modes:C0644 963 test-keys.prv
Reading file from scp://lab@7.0.0.7/test-keys.prv!% Key pair import succeeded.

ssl-proxy(config)#
```

debug ssl-proxy

To turn on the debug flags in different system components, use the **debug ssl-proxy** command. Use the **no** form of this command to turn off the debug flags.

debug ssl-proxy {**app** | **fdu** [*type*] | **ipc** | **pki** [*type*] | **ssl** [*type*] | **tcp** [*type*]}

Syntax Description

app	Turns on App debugging.
fdu *type*	Turns on FDU debugging; (optional) *type* valid values are **cli**, **hash**, **ipc**, and **trace**. See the "Usage Guidelines" section for additional information.
ipc	Turns on IPC debugging.
pki *type*	Turns on PKI debugging; (optional) *type* valid values are **cert**, **events**, **history**, **ipc**, and **key**. See the "Usage Guidelines" section for additional information.
ssl *type*	Turns on SSL debugging; (optional) *type* valid values are **alert**, **error**, **handshake**, and **pkt**. See the "Usage Guidelines" section for additional information.
tcp *type*	Turns on TCP debugging; (optional) *type* valid values are **event**, **packet**, **state**, and **timers**. See the "Usage Guidelines" section for additional information.

Defaults

This command has no default settings.

Command Modes

EXEC

Command History

Release	Modification
Cisco IOS Release 12.1(13)E and SSL Services Module Release 1.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.

Usage Guidelines

The **fdu** *type* includes the following values:

- **cli**—Debugs the FDU CLI.
- **hash**—Debugs the FDU hash.
- **ipc** —Debugs the FDU IPC.
- **trace**—Debugs the FDU trace.

The **pki** *type* includes the following values:

- **certs**—Debugs the certificate management.
- **events**—Debugs events.
- **history**—Debugs the certificate history.
- **ipc**—Debugs the IPC messages and buffers.
- **key**—Debugs key management.

The **ssl** *type* includes the following values:

- **alert**—Debugs the SSL alert events.
- **error**—Debugs the SSL error events.
- **handshake**—Debugs the SSL handshake events.
- **pkt**—Debugs the received and transmitted SSL packets.

Note Use the TCP debug commands only to troubleshoot basic connectivity issues under little or no load conditions (for instance, when no connection is being established to the virtual server or real server).

If you run TCP debug commands, the TCP module displays large amounts of debug information on the console, which can significantly slow down module performance. Slow module performance can lead to delayed processing of TCP connection timers, packets, and state transitions.

The **tcp** *type* includes the following values:

- **events**—Debugs the TCP events.
- **pkt**—Debugs the received and transmitted TCP packets.
- **state**—Debugs the TCP states.
- **timers**—Debugs the TCP timers.

Examples

This example shows how to turn on App debugging:

```
ssl-proxy# debug ssl-proxy app
ssl-proxy#
```

This example shows how to turn on FDU debugging:

```
ssl-proxy# debug ssl-proxy fdu
ssl-proxy#
```

This example shows how to turn on IPC debugging:

```
ssl-proxy# debug ssl-proxy ipc
ssl-proxy#
```

This example shows how to turn on PKI debugging:

```
ssl-proxy# debug ssl-proxy pki
ssl-proxy#
```

This example shows how to turn on SSL debugging:

```
ssl-proxy# debug ssl-proxy ssl
ssl-proxy#
```

This example shows how to turn on TCP debugging:

```
ssl-proxy# debug ssl-proxy tcp
ssl-proxy#
```

This example shows how to turn off TCP debugging:

```
ssl-proxy# no debug ssl-proxy tcp
ssl-proxy#
```

do

To execute EXEC-level commands from global configuration mode or other configuration modes or submodes, use the **do** command.

do *command*

Syntax Description

command	EXEC-level command to be executed.

Defaults

This command has no default settings.

Command Modes

Global configuration or any other configuration mode or submode from which you are executing the EXEC-level command.

Command History

Release	Modification
Cisco IOS Release 12.1(13)E and SSL Services Module Release 1.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.

Usage Guidelines

Caution Do not enter the **do** command in EXEC mode. Interruption of service may occur.

You cannot use the **do** command to execute the **configure terminal** command because entering the **configure terminal** command changes the mode to configuration mode.

You cannot use the **do** command to execute the **copy** or **write** command in the global configuration or any other configuration mode or submode.

Examples

This example shows how to execute the EXEC-level **show interfaces** command from within global configuration mode:

```
ssl-proxy(config)# do show interfaces serial 3/0

Serial3/0 is up, line protocol is up
  Hardware is M8T-RS232
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255, load 1/255
  Encapsulation HDLC, loopback not set, keepalive set (10 sec)
  Last input never, output 1d17h, output hang never
  Last clearing of "show interface" counters never
.
.
.
ssl-proxy(config)#
```

show ssl-proxy admin-info

To display the administration VLAN and related IP and gateway addresses, use the **show ssl-proxy admin-info** command.

show ssl-proxy admin-info

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

EXEC

Command History

Release	Modification
Cisco IOS Release 12.1(13)E and SSL Services Module Release 1.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.

Examples

This example shows how to display the administration VLAN and related IP and gateway addresses:

```
ssl-proxy# show ssl-proxy admin-info
STE administration VLAN: 2
STE administration IP address: 207.57.100.18
STE administration gateway: 207.0.207.5
ssl-proxy#
```

Related Commands

ssl-proxy vlan

show ssl-proxy buffers

To display information about TCP buffer usage, use the **show ssl-proxy buffers** command.

show ssl-proxy buffers

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

EXEC

Command History

Release	Modification
Cisco IOS Release 12.1(13)E and SSL Services Module Release 1.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.

Examples

This example shows how to display the buffer usage and other information in the TCP subsystem:

```
ssl-proxy# show ssl-proxy buffers
Buffers info for TCP module 1
TCP data buffers used 2816 limit 112640
TCP ingress buffer pool size 56320 egress buffer pool size 56320
TCP ingress data buffers min-thresh 7208960 max-thresh 21626880
TCP ingress data buffers used Current 0 Max 0
TCP ingress buffer RED shift 9 max drop prob 10
Conns consuming ingress data buffers 0
Buffers with App 0
TCP egress data buffers used Current 0 Max 0
Conns consuming egress data buffers 0
In-sequence queue bufs 0 OOO bufs 0
ssl-proxy#
```

Related Commands

ssl-proxy policy tcp

show ssl-proxy certificate-history

To display information about the event history of the certificate, use the **show ssl-proxy certificate-history** command.

show ssl-proxy certificate-history [**service** [*name*]]

Syntax Description

service *name*	Displays all certificate records of a proxy service and (optionally) for a specific proxy service.

Defaults

This command has no default settings.

Command Modes

EXEC

Command History

Release	Modification
Cisco IOS Release 12.1(13)E and SSL Services Module Release 1.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.

Usage Guidelines

The **show ssl-proxy certificate-history** command displays these records:

- Service name
- Key pair name
- Generation or import time
- Trustpoint name
- Certificate subject name
- Certificate issuer name
- Serial number
- Date

A syslog message is generated for each record. The oldest records are deleted after the limit of 512 records is reached.

Examples

This example shows how to display the event history of all the certificate processing:

```
ssl-proxy# show ssl-proxy certificate-history
Record 1, Timestamp:00:00:51, 16:36:34 UTC Oct 31 2002
    Installed Server Certificate, Index 5
    Proxy Service:s1,  Trust Point:t3
    Key Pair Name:k3,  Key Usage:RSA General Purpose, Exportable
    Time of Key Generation:12:27:58 UTC Oct 30 2002
    Subject Name:OID.1.2.840.113549.1.9.2 = simpson5-2-ste.cisco.com,
OID.1.2.840.113549.1.9.8 = 207.79.1.9, OID.2.5.4.5 = B0FFF235
    Issuer Name:CN = SimpsonTestCA, OU = Simpson Lab, O = Cisco Systems, L = San Jose, ST
= CA, C = US, EA =<16> simpson-pki@cisco.com
    Serial Number:5D3D1931000100000D99
    Validity Start Time:21:58:12 UTC Oct 30 2002
    End Time:22:08:12 UTC Oct 30 2003
    Renew Time:00:00:00 UTC Jan 1 1970
  End of Certificate Record

  Record 2, Timestamp:00:01:06, 16:36:49 UTC Oct 31 2002
    Installed Server Certificate, Index 6
    Proxy Service:s5,  Trust Point:t10
    Key Pair Name:k10,  Key Usage:RSA General Purpose, Exportable
    Time of Key Generation:07:56:43 UTC Oct 11 2002
    Subject Name:CN = host1.cisco.com, OID.1.2.840.113549.1.9.2 =
simpson5-2-ste.cisco.com, OID.1.2.840.113549.1.9.8 = 207.79.1.9, OID.2.5.4.5 = B0FFF235
    Issuer Name:CN = SimpsonTestCA, OU = Simpson Lab, O = Cisco Systems, L = San Jose, ST
= CA, C = US, EA =<16> simpson-pki@cisco.com
    Serial Number:24BC81B7000100000D85
    Validity Start Time:22:38:00 UTC Oct 19 2002
    End Time:22:48:00 UTC Oct 19 2003
    Renew Time:00:00:00 UTC Jan 1 1970
  End of Certificate Record

  Record 3, Timestamp:00:01:34, 16:37:18 UTC Oct 31 2002
    Installed Server Certificate, Index 7
    Proxy Service:s6,  Trust Point:t10
    Key Pair Name:k10,  Key Usage:RSA General Purpose, Exportable
    Time of Key Generation:07:56:43 UTC Oct 11 2002
    Subject Name:CN = host1.cisco.com, OID.1.2.840.113549.1.9.2 =
simpson5-2-ste.cisco.com, OID.1.2.840.113549.1.9.8 = 207.79.1.9, OID.2.5.4.5 = B0FFF235
    Issuer Name:CN = SimpsonTestCA, OU = Simpson Lab, O = Cisco Systems, L = San Jose, ST
= CA, C = US, EA =<16> simpson-pki@cisco.com
    Serial Number:24BC81B7000100000D85
    Validity Start Time:22:38:00 UTC Oct 19 2002
    End Time:22:48:00 UTC Oct 19 2003
    Renew Time:00:00:00 UTC Jan 1 1970
  End of Certificate Record

  Record 4, Timestamp:00:01:40, 16:37:23 UTC Oct 31 2002
    Deleted Server Certificate, Index 0
    Proxy Service:s6,  Trust Point:t6
    Key Pair Name:k6,  Key Usage:RSA General Purpose, Not Exportable
    Time of Key Generation:00:28:28 UTC Mar 1 1993
    Subject Name:CN = host1.cisco.com, OID.1.2.840.113549.1.9.2 =
simpson5-2-ste.cisco.com, OID.1.2.840.113549.1.9.8 = 207.79.1.8, OID.2.5.4.5 = B0FFF235
    Issuer Name:CN = SimpsonTestCA, OU = Simpson Lab, O = Cisco Systems, L = San Jose, ST
= CA, C = US, EA =<16> simpson-pki@cisco.com
    Serial Number:5CB5CFD6000100000D97
    Validity Start Time:19:30:26 UTC Oct 30 2002
    End Time:19:40:26 UTC Oct 30 2003
    Renew Time:00:00:00 UTC Jan 1 1970
  End of Certificate Record
% Total number of certificate history records displayed = 4
ssl-proxy#
```

This example shows how to display the certificate record for a specific proxy service:

```
ssl-proxy# show ssl-proxy certificate-history service s6
Record 3, Timestamp:00:01:34, 16:37:18 UTC Oct 31 2002
    Installed Server Certificate, Index 7
    Proxy Service:s6,  Trust Point:t10
    Key Pair Name:k10,  Key Usage:RSA General Purpose, Exportable
    Time of Key Generation:07:56:43 UTC Oct 11 2002
    Subject Name:CN = host1.cisco.com, OID.1.2.840.113549.1.9.2 =
simpson5-2-ste.cisco.com, OID.1.2.840.113549.1.9.8 = 207.79.1.9, OID.2.5.4.5 = B0FFF235
    Issuer Name:CN = SimpsonTestCA, OU = Simpson Lab, O = Cisco Systems, L = San Jose, ST
= CA, C = US, EA =<16> simpson-pki@cisco.com
    Serial Number:24BC81B7000100000D85
    Validity Start Time:22:38:00 UTC Oct 19 2002
    End Time:22:48:00 UTC Oct 19 2003
    Renew Time:00:00:00 UTC Jan 1 1970
  End of Certificate Record

  Record 4, Timestamp:00:01:40, 16:37:23 UTC Oct 31 2002
    Deleted Server Certificate, Index 0
    Proxy Service:s6,  Trust Point:t6
    Key Pair Name:k6,  Key Usage:RSA General Purpose, Not Exportable
    Time of Key Generation:00:28:28 UTC Mar 1 1993
    Subject Name:CN = host1.cisco.com, OID.1.2.840.113549.1.9.2 =
simpson5-2-ste.cisco.com, OID.1.2.840.113549.1.9.8 = 207.79.1.8, OID.2.5.4.5 = B0FFF235
    Issuer Name:CN = SimpsonTestCA, OU = Simpson Lab, O = Cisco Systems, L = San Jose, ST
= CA, C = US, EA =<16> simpson-pki@cisco.com
    Serial Number:5CB5CFD6000100000D97
    Validity Start Time:19:30:26 UTC Oct 30 2002
    End Time:19:40:26 UTC Oct 30 2003
    Renew Time:00:00:00 UTC Jan 1 1970
  End of Certificate Record
Total number of certificate history records displayed = 2
```

Related Commands

ssl-proxy service

show ssl-proxy conn

To display the TCP connections from the SSL Services Module, use the **show ssl-proxy conn** command.

show ssl-proxy conn 4tuple [**local** {**ip** *local-ip-addr local-port*} [**remote** [{**ip** *remote-ip-addr* [**port** *remote-port*]} | {**port** *remote-port* [**ip** *remote-ip-addr*]}]]]

show ssl-proxy conn 4tuple [**local** {**port** *local-port*} [**remote** [{**ip** *remote-ip-addr* [**port** *remote-port*]} | {**port** *remote-port* [**ip** *remote-ip-addr*]}]]]

show ssl-proxy conn 4tuple [**local** {**remote** [{**ip** *remote-ip-addr* [**port** *remote-port*]} | {**port** *remote-port* [**ip** *remote-ip-addr*]}]]

show ssl-proxy conn service *name*

Syntax Description

4tuple	Displays the TCP connections for a specific address.
local	(Optional) Displays the TCP connections for a specific local device.
ip *local-ip-addr*	IP address of a local device.
local-port	Port number of a local device.
remote	(Optional) Displays the TCP connections for a specific remote device.
ip *remote-ip-addr*	IP address of a remote device.
port *remote-port*	Port number of a remote device.
port *local-port*	(Optional) Displays the TCP connections for a specific local port.
service *name*	Displays the TCP connections for a specific proxy service.

Defaults

This command has no default settings.

Command Modes

EXEC

Command History

Release	Modification
Cisco IOS Release 12.1(13)E and SSL Services Module Release 1.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.

Usage Guidelines

The **show ssl-proxy conn** commanddisplays these records:

- Local Address
- Remote Address
- VLAN
- Conid
- Send-Q
- Recv-Q
- State

  The State record indicates the TCP state of the connection between the SSL Services Module and a remote device. The TCP states are described in the following table:

Table 2-1 TCP Connection State Descriptions

LISTEN	This module is wating for a request to initiate a TCP connection.
SYN_SEND	This module has sent a SYN packet to another device in order to initiate the opening of a TCP connection.
SYN_RECEIVED	This module has received a SYN packet from another device that is requesting to open a TCP connection.
ESTABLISHED or ESTAB	The three-way TCP handshake (SYN, SYN/ACK, ACK) has been completed and a TCP connection is now established between this module and another device.
FIN_WAIT_1	This module has sent a FIN packet to a connected device in order to close the TCP connection.
TIME_WAIT or TWAIT	This module has successfully completed a FIN sequence to close a TCP connection with a connected device. The connection will be held in this state for 30-120 seconds to receive any late packets.
CLOSE_WAIT	This module has received a FIN packet from a connected device that is requesting to close the TCP connection.
FIN_WAIT_2	After sending a FIN packet to a connected device in order to close the TCP connection, this module has received an ACK packet and is wating for a FIN packet.
LAST_ACK	At the request of a connected device, this module has closed the TCP connection and is waiting for a final ACK from the other device.
CLOSING	This module has actively closed the TCP connection and is waiting for a final ACK from the other device before entering the TIME_WAIT state.
CLOSED	A TCP connection has been closed with all wait times and acknowledgments completed.

Examples

These examples show different ways to display the TCP connection that is established from the SSL Services Module:

```
ssl-proxy# show ssl-proxy conn
Connections for TCP module 1
Local Address         Remote Address        VLAN Conid  Send-Q Recv-Q State
--------------------- --------------------- ---- ------ ------ ------ ------
2.0.0.10:4430         1.200.200.14:48582    2    0      0      0      ESTAB
1.200.200.14:48582    2.100.100.72:80       2    1      0      0      ESTAB

2.0.0.10:4430         1.200.200.14:48583    2    2      0      0      ESTAB
1.200.200.14:48583    2.100.100.72:80       2    3      0      0      ESTAB

2.0.0.10:4430         1.200.200.14:48584    2    4      0      0      ESTAB
1.200.200.14:48584    2.100.100.72:80       2    5      0      0      ESTAB

2.0.0.10:4430         1.200.200.14:48585    2    6      0      0      ESTAB
1.200.200.14:48585    2.100.100.72:80       2    7      0      0      ESTAB

2.0.0.10:4430         1.200.200.14:48586    2    8      0      0      ESTAB
1.200.200.14:48586    2.100.100.72:80       2    9      0      0      ESTAB

ssl-proxy# show ssl-proxy conn 4tuple local port 443
Connections for TCP module 1
Local Address         Remote Address        VLAN Conid  Send-Q Recv-Q State
--------------------- --------------------- ---- ------ ------ ------ ------
2.50.50.133:443       1.200.200.12:39728    2    113676 0      0      TWAIT
No Bound Connection

2.50.50.133:443       1.200.200.12:39729    2    113680 0      0      TWAIT
No Bound Connection

2.50.50.131:443       1.200.200.14:40599    2    113684 0      0      TWAIT
No Bound Connection

2.50.50.132:443       1.200.200.13:48031    2    114046 0      0      TWAIT
No Bound Connection

2.50.50.132:443       1.200.200.13:48032    2    114048 0      0      TWAIT
No Bound Connection

2.50.50.132:443       1.200.200.13:48034    2    114092 0      0      TWAIT
No Bound Connection

2.50.50.132:443       1.200.200.13:48035    2    114100 0      0      TWAIT
No Bound Connection

ssl-proxy# show ssl-proxy conn 4tuple remote ip 1.200.200.14
Connections for TCP module 1
Local Address         Remote Address        VLAN Conid  Send-Q Recv-Q State
--------------------- --------------------- ---- ------ ------ ------ ------
2.50.50.131:443       1.200.200.14:38814    2    58796  0      0      TWAIT
No Bound Connection

2.50.50.131:443       1.200.200.14:38815    2    58800  0      0      TWAIT
No Bound Connection

2.50.50.131:443       1.200.200.14:38817    2    58802  0      0      TWAIT
No Bound Connection

2.50.50.131:443       1.200.200.14:38818    2    58806  0      0      TWAIT
No Bound Connection
```

```
2.50.50.131:443       1.200.200.14:38819    2    58810  0      0      TWAIT
No Bound Connection

2.50.50.131:443       1.200.200.14:38820    2    58814  0      0      TWAIT
No Bound Connection

2.50.50.131:443       1.200.200.14:38821    2    58818  0      0      TWAIT
No Bound Connection

ssl-proxy# show ssl-proxy conn service iis1
Connections for TCP module 1
Local Address         Remote Address        VLAN Conid  Send-Q Recv-Q State
--------------------- --------------------- ---- ------ ------ ------ ------
2.50.50.131:443       1.200.200.14:41217    2    121718 0      0      TWAIT
No Bound Connection

2.50.50.131:443       1.200.200.14:41218    2    121722 0      0      TWAIT
No Bound Connection

2.50.50.131:443       1.200.200.14:41219    2    121726 0      0      TWAIT
No Bound Connection

2.50.50.131:443       1.200.200.14:41220    2    121794 0      0      TWAIT
No Bound Connection

2.50.50.131:443       1.200.200.14:41221    2    121808 0      0      TWAIT
No Bound Connection

2.50.50.131:443       1.200.200.14:41222    2    121940 0      0      TWAIT
No Bound Connection

2.50.50.131:443       1.200.200.14:41223    2    122048 0      0      TWAIT
No Bound Connection
```

show ssl-proxy crash-info

To collect information about the software-forced reset from the SSL Services Module, use the **show ssl-proxy crash-info** command.

show ssl-proxy crash-info [**brief** | **details**]

Syntax Description

brief	(Optional) Collects a small subset of software-forced reset information, limited to processor registers.
details	(Optional) Collects the full set of software-forced reset information, including exception and interrupt stacks dump (this can take up to 10 minutes to complete printing).

Defaults

This command has no default settings.

Command Modes

EXEC

Command History

Release	Modification
Cisco IOS Release 12.1(13)E and SSL Services Module Release 1.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.

Examples

This example shows how to collect information about the software-forced reset:

```
ssl-proxy# show ssl-proxy crash-info

===== SSL SERVICE MODULE - START OF CRASHINFO COLLECTION =====


------------- COMPLEX 0 [FDU_IOS] ----------------------

NVRAM CHKSUM:0xEB28
NVRAM MAGIC:0xC8A514F0
NVRAM VERSION:1

++++++++++ CORE 0 (FDU) ++++++++++++++++++++++

   CID:0
   APPLICATION VERSION:2003.04.15 14:50:20 built for cantuc
   APPROXIMATE TIME WHEN CRASH HAPPENED:14:06:04 UTC Apr 16 2003
   THIS CORE DIDN'T CRASH
   TRACEBACK:222D48 216894
   CPU CONTEXT  ----------------------------

$0 :00000000, AT :00240008, v0 :5A27E637, v1 :000F2BB1
a0 :00000001, a1 :0000003C, a2 :002331B0, a3 :00000000
t0 :00247834, t1 :02BFAAA0, t2 :02BF8BB0, t3 :02BF8BA0
t4 :02BF8BB0, t5 :00247834, t6 :00000000, t7 :00000001
```

```
s0 :00000000, s1 :0024783C, s2 :00000000, s3 :00000000
s4 :00000001, s5 :0000003C, s6 :00000019, s7 :0000000F
t8 :00000001, t9 :00000001, k0 :00400001, k1 :00000000
gp :0023AE80, sp :031FFF58, s8 :00000019, ra :00216894
LO :00000000, HI :0000000A, BADVADDR :828D641C
EPC :00222D48, ErrorEPC :BFC02308, SREG :34007E03
Cause 0000C000 (Code 0x0):Interrupt exception

CACHE ERROR registers  -------------------

CacheErrI:00000000, CacheErrD:00000000
ErrCtl:00000000, CacheErrDPA:0000000000000000

   PROCESS STACK -----------------------------
      stack top:0x3200000

   Process stack in use:

   sp is close to stack top;

   printing 1024 bytes from stack top:

031FFC00:06405DE0 002706E0 0000002D 00000001  .@]`.'.`...-....
031FFC10:06405DE0 002706E0 00000001 0020B800  .@]`.'.`..... 8.
031FFC20:031FFC30 8FBF005C 14620010 24020004  ..|0.?.\.b..$...
...........
...........
...........
FFFFFFD0:00000000 00000000 00000000 00000000 ................
FFFFFFE0:00627E34 00000000 00000000 00000000 .b~4............
FFFFFFF0:00000000 00000000 00000000 00000006 ................


===== SSL SERVICE MODULE - END OF CRASHINFO COLLECTION =======
```

This example shows how to collect a small subset of software-forced reset information:

```
ssl-proxy# show ssl-proxy crash-info brief


===== SSL SERVICE MODULE - START OF CRASHINFO COLLECTION =====


------------- COMPLEX 0 [FDU_IOS] ----------------------

SKE CRASH INFO Error: wrong MAGIC # 0

CLI detected an error in FDU_IOS crash-info; wrong magic.

------------- COMPLEX 1 [TCP_SSL] ----------------------


Crashinfo fragment #0 from core 2 at offset 0 error:
Remote system reports wrong crashinfo magic.
Bad fragment received. Reception abort.

CLI detected an error in TCP_SSL crash-info;


===== SSL SERVICE MODULE - END OF CRASHINFO COLLECTION =======
```

show ssl-proxy mac address

To display the current MAC address, use the **show ssl-proxy mac address** command.

show ssl-proxy mac address

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

EXEC

Command History

Release	Modification
Cisco IOS Release 12.1(13)E and SSL Services Module Release 1.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.

Examples

This example shows how to display the current MAC address that is used in the SSL Services Module:

```
ssl-proxy# show ssl-proxy mac address
STE MAC address: 00e0.b0ff.f232
ssl-proxy#
```

show ssl-proxy natpool

To display information about the NAT pool, use the **show ssl-proxy natpool** command.

show ssl-proxy natpool [*name*]

Syntax Description

name	(Optional) NAT pool name.

Defaults

This command has no default settings.

Command Modes

EXEC

Command History

Release	Modification
Cisco IOS Release 12.1(13)E and SSL Services Module Release 1.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.

Examples

This example shows how to display information for a specific NAT address pool that is configured on the SSL Services Module:

```
ssl-proxy# show ssl-proxy natpool NP1
Start ip: 207.57.110.1
End ip: 207.57.110.8
netmask: 255.0.0.0
vlan associated with natpool: 2
SSL proxy services using this natpool:
S2
S3
S1
S6
Num of proxies using this natpool: 4
ssl-proxy#
```

Related Commands

ssl-proxy natpool

show ssl-proxy policy

To display the configured SSL proxy policies, use the **show ssl-proxy policy** command.

show ssl-proxy policy {**http-header** | **ssl** | **tcp** | **url-rewrite**} [*name*]

Syntax Description

http-header	Displays the configured HTTP header policies.
ssl	Displays the configured SSL policies.
tcp	Displays the configured TCP policies.
url-rewrite	Displays the configured URL rewrite policies.
name	(Optional) Policy name.

Defaults

This command has no default settings.

Command Modes

EXEC

Command History

Release	Modification
Cisco IOS Release 12.1(13)E and SSL Services Module Release 1.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.
SSL Services Module Release 2.1(1)	This command was changed to include the **http-header** and **url-rewrite** keywords.

Examples

This example shows how to display information about the HTTP header policy:

```
ssl-proxy# show ssl-proxy policy http-header httphdr-policy
 Client Certificate Insertion Header Only
 Session Header Insertion All
 Client IP/Port Insertion Client IP and Port
 Hdr # Custom Header
  0 SSL-Frontend:Enable

>Usage count of this policy: 0
ssl-proxy#
```

This example shows how to display policy information about a specific SSL policy that is configured on the SSL Services Module:

```
ssl-proxy# show ssl-proxy policy ssl ssl-policy1
Cipher suites: (None configured, default ciphers included)
     rsa-with-rc4-128-md5
     rsa-with-rc4-128-sha
     rsa-with-des-cbc-sha
     rsa-with-3des-ede-cbc-sha
SSL Versions enabled:SSL3.0, TLS1.0
strict close protocol:disabled
```

```
Session Cache:enabled
Handshake timeout not configured (never times out)
Num of proxies using this policy:0
```

This example shows how to display policy information about a specific TCP policy that is configured on the SSL Services Module:

```
ssl-proxy# show ssl-proxy policy tcp tcp-policy1
 MSS                 1250
 SYN timeout         75
 Idle timeout        600
 FIN wait timeout    75
 Reassembly timeout  60
 Rx Buffer Share     32768
 Tx Buffer Share     32768
 TOS Carryover       Enabled

 Usage count of this policy:0
ssl-proxy#
```

This example shows how to display information about the URL rewrite policy:

```
ssl-proxy# show ssl-proxy policy url-rewrite urlrw-policy
 >Rule URL Clearport SSLport
  1 wwwin.cisco.com 80 443
  2 www.cisco.com 8080 444
>
>Usage count of this policy: 0
ssl-proxy#
```

Related Commands

ssl-proxy policy http-header
ssl-proxy policy ssl
ssl-proxy policy tcp
ssl-proxy policy url-rewrite

show ssl-proxy service

To display information about the configured SSL virtual service, use the **show ssl-proxy service** command.

show ssl-proxy service [*name*]

Syntax Description

name	(Optional) Service name.

Defaults

This command has no default settings.

Command Modes

EXEC

Command History

Release	Modification
Cisco IOS Release 12.1(13)E and SSL Services Module Release 1.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.

Examples

This example shows how to display all SSL virtual services that are configured on the SSL Services Module:

```
ssl-proxy# show ssl-proxy service
Proxy Service Name Admin Operation Events
status status
S2 up up
S3 up up
S1 up up
S6 down down
ssl-proxy#
```

This example shows how to display a specific SSL virtual service that is configured on the SSL Services Module:

```
ssl-proxy# show ssl-proxy service S6
Service id: 0, bound_service_id: 256
Virtual IP: 10.10.1.104, port: 443
Server IP: 10.10.1.100, port: 80
Virtual SSL Policy: SSL1_PLC
rsa-general-purpose certificate trustpoint: tptest
  Certificate chain for new connections:
    Server Certificate:
       Key Label: tptest
       Serial Number: 01
    Root CA Certificate:
       Serial Number: 00
  Certificate chain complete
Admin Status: up
Operation Status: down
Proxy status: No Client VLAN, No Server VLAN
ssl-proxy#
```

show ssl-proxy stats

To display information about the statistics counter, use the **show ssl-proxy stats** command.

show ssl-proxy stats [*type*]

Syntax Description

type	(Optional) Information type; valid values are **crypto**, **ipc**, **pki**, **service**, **ssl**, and **tcp**. See the "Usage Guidelines" section for additional information.

Defaults

This command has no default settings.

Command Modes

EXEC

Command History

Release	Modification
Cisco IOS Release 12.1(13)E and SSL Services Module Release 1.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.
SSL Services Module Release 1.2(1)	The output of the **show ssl-proxy stats** command was changed to include information about the session allocation failure and session limit-exceed table.

Usage Guidelines

The *type* values are defined as follows:

- **crypto**—Displays crypto statistics.
- **ipc**—Displays IPC statistics.
- **pki**—Displays PKI statistics.
- **service**—Displays proxy service statistics.
- **ssl**—Displays SSL detailed statistics.
- **tcp**—Displays TCP detailed statistics.

Examples

This example shows how to display all the statistics counters that are collected on the SSL Services Module:

```
ssl-proxy# show ssl-proxy stats
TCP Statistics:
    Conns initiated     : 1970288       Conns accepted       : 1970288
    Conns established   : 3797817       Conns dropped        : 2481867
    Conns Allocated     : 1970288       Conns Deallocated    : 1970288
    Conns closed        : 3940576       SYN timeouts         : 141865
    Idle timeouts       : 0             Total pkts sent      : 2499818678
    Data packets sent   : 2034445802    Data bytes sent      : 2837513871
    Total Pkts rcvd     : 2055992562    Pkts rcvd in seq     : 1365961238
```

```
    Bytes rcvd in seq   : 464953685

SSL Statistics:
    conns attempted     : 1970288       conns completed     : 1970288
    full handshakes     : 1968370       resumed handshakes  : 0
    active conns        : 0             active sessions     : 0
    renegs attempted    : 0             conns in reneg      : 0
    handshake failures  : 1918          data failures       : 0
    fatal alerts rcvd   : 0             fatal alerts sent   : 1918
    no-cipher alerts    : 0             ver mismatch alerts : 0
    no-compress alerts  : 0             bad macs received   : 0
    pad errors          : 0             session fails       : 0

FDU Statistics:
    IP Frag Drops       : 0             IP Version Drops    : 0
    IP Addr Discards    : 0             Serv_Id Drops       : 27
    Conn Id Drops       : 0             Bound Conn Drops    : 0
    Vlan Id Drops       : 0             TCP Checksum Drops  : 0
    Hash Full Drops     : 0             Hash Alloc Fails    : 0
    Flow Creates        : 3940576       Flow Deletes        : 3940576
    Conn Id allocs      : 1970288       Conn Id deallocs    : 1970288
    Tagged Pkts Drops   : 0             Non-Tagg Pkts Drops : 0
    Add ipcs            : 3             Delete ipcs         : 0
    Disable ipcs        : 0             Enable ipcs         : 0
    Unsolicited ipcs    : 0             Duplicate Add ipcs  : 0
    IOS Broadcast Pkts  : 82820         IOS Unicast Pkts    : 1360
    IOS Multicast Pkts  : 0             IOS Total Pkts      : 84180
    IOS Congest Drops   : 0             SYN Discards        : 0
    TCP 5-tuple reuse   : 0

ssl-proxy#
```

This example shows how to display ssl statistics:

```
ssl-proxy# show ssl-proxy stats ssl
SSL Statistics:
    conns attempted     : 1970288       conns completed     : 1970288
    conns in handshake  : 0             conns in data       : 0
    renegs attempted    : 0             conns in reneg      : 0
    active sessions     : 0             max handshake conns : 472
    rand bufs allocated : 114801        cached rand buf miss: 0
    current device q len: 0             max device q len    : 144
    sslv2 forwards      : 0             cert reqs processed : 1897
    fatal alerts rcvd   : 0             fatal alerts sent   : 1918
    stale packet drops  : 0             service_id discards : 0
    session reuses      : 0             hs handle in use    : 0
    bad clnt session id : 0             expired session id  : 0
    available ctx count : 64            ctx cleanup count   : 22
    device reset count  : 22

    SSL3 Statistics:
      full handshakes    : 0             resumed handshakes : 0
      handshake failures : 0             data failures      : 0
      bad macs received  : 0             pad errors         : 0
      conns established with cipher rsa-with-rc4-128-md5       : 0
      conns established with cipher rsa-with-rc4-128-sha       : 0
      conns established with cipher rsa-with-des-cbc-sha       : 0
      conns established with cipher rsa-with-3des-ede-cbc-sha  : 0

    TLS1 Statistics:
      full handshakes    : 1968370       resumed handshakes : 0
      handshake failures : 1918          data failures      : 0
      bad macs received  : 0             pad errors         : 0
      conns established with cipher rsa-with-rc4-128-md5       : 1968369
```

```
      conns established with cipher rsa-with-rc4-128-sha        : 0
      conns established with cipher rsa-with-des-cbc-sha        : 0
      conns established with cipher rsa-with-3des-ede-cbc-sha   : 1

SSL error statistics:
    session alloc fails : 0             session limit exceed: 0
    handshake init fails: 0             renegotiation fails : 0
    no-cipher alerts    : 0             ver mismatch alerts : 0
    no-compress alerts  : 0             multi buf rec errors: 0
    ssl peer closes     : 0             non-ssl peer closes : 0
    unexpected record   : 0             rec formatting error: 0
    rsa pkcs pad errors : 0             premaster errors    : 0
    failed rsa reqs     : 0             failed random reqs  : 0
    failed key-material : 0             failed master-secret: 0
    failed update hash  : 0             failed finish hash  : 0
    failed encrypts     : 0             failed decrypts     : 0
    bad record version  : 0             bad record size     : 0
    cert verify errors  : 1896          unsupported certs   : 0
    conn aborted        : 0
    overload drops      : 0             hs limit exceeded   : 0
    hs handle mem fails : 0             conn reuse error    : 0
    dev invalid params  : 0             dev failed requests : 0
    dev timeout         : 0             dev busy            : 0
    dev cancelled       : 0             no dev fails        : 0
    dev resource fails  : 0             dev unknown errors  : 0
    dev conn ctx fails  : 0             dev cmd ctx fails   : 0
    mem alloc fails     : 0             buf alloc fails     : 0
    invalid cipher algo : 0             invalid hash algo   : 0
    unaligned buf addr  : 0             unaligned buf len   : 0
    internal error      : 0             unknown ipcs        : 0
    double free attempts: 0             alert-send fails    : 0

SSL Crypto Statistics:
    blocks encrypted    : 89226334      blocks decrypted    : 4864649
    bytes encrypted     : 1500039492    bytes decrypted     : 314938656
    crypto failures     : 0
    IKECount            : 128270        IKEFailedCount      : 0
    DHPublicCount       : 0             DHSharedCount       : 0
    rsa public key ops  : 1             rsa private key ops : 128269
    dsa_signs           : 0             dsa_verifies        : 0
    device dma errors   : 0
    PushMCR_nopkts      : 472328917     PushMCR_pushed      : 0
    PushMCR1_full       : 160504926     PushMCR2_full       : 0
    PushMCR_push        : 13277229
    GetFreeMCR_busy     : 0             GetFreeMCR_dma_error: 0
    GetFreeMCR_no_rsrc  : 0             GetFreeMCR_success  : 103511789

SSL last 5 sec average Statistics:
    full handshakes     : 0             resumed handshakes  : 0
    handshake failures  : 0             data failures       : 0
    bytes encrypted     : 0             bytes decrypted     : 0

SSL last 1 min average Statistics:
    full handshakes     : 0             resumed handshakes  : 0
    handshake failures  : 0             data failures       : 0
    bytes encrypted     : 0             bytes decrypted     : 0

SSL last 5 min average Statistics:
    full handshakes     : 0             resumed handshakes  : 0
    handshake failures  : 0             data failures       : 0
    bytes encrypted     : 0             bytes decrypted     : 0

SSL PKI Statistics:
    number of malloc    : 245           number of free      : 202
```

```
    ssl buf allocated   : 8             ssl buf freed       : 1

    Peer Certificate Verify Statistics:
    cert approved       : 1             cert disapproved    : 0
    peer cert empty     : 1896          total num of request: 1897
    req being processed : 0             req pending         : 0
    longest queue       : 1             longest pending     : 0
    verify congestion   : 0             req dropped, q full : 0
    no memory for verify: 0             verify data error   : 0
    verify context error: 0             context delete error: 0
    timer expired error : 0             timer expired count : 0
    late verify result  : 0             timer turned on     : 1
    timer turned off    : 1             context created     : 1
    context deleted     : 1

    High Priority IPC:
    ipc request received: 18            ipc request dropped : 0
    ipc req duplicated  : 0             ipc req fragment err: 0
    ipc req parm len err: 0             ipc req op code err : 0
    ipc req cert len err: 0             ipc response sent   : 18
    ipc resp no memory  : 0             ipc resp no ssl buf : 0
    ipc buffer allocated: 0             ipc buffer freed    : 0
    ipc buf alloc failed: 0             ipc send msg failed : 0

    Normal Priority IPC:
    ipc buffer allocated: 1             ipc buffer freed    : 1
    ipc request sent    : 1             ipc request received: 3
    ipc buf alloc failed: 0             ipc send msg failed : 0
    ipc requests dropped: 0

SSL Queue Sizes:
    bcm_cmd_ctx_pool_size   : 64            bcm_asym_cmd_ctx_pool_sz: 9000
    bcm_info_pool_size      : 65538         buf_desc_free_q_size    : 94709
    cert_result_free_q_size : 11048         delete_conn_q_size      : 0
    event_q_size            : 0             free_conn_q_size        : 65536
    free_sess_q_size        : 262144        free_sess_active_tmr_qsz: 0
    global_pending_q_size   : 0             to_app_ctx_pool_size    : 512
    ste_asym_req_q_size     : 0             ste_free_req_ctx_pool_sz: 20480
    ste_sym_req_q_size      : 0

SSL Random Buffer Info:
    psuedo_rand_req_pending : 0             rand_req_pending        : 0
    pseudo_rand_req_count   : 71
    curr_psuedo_rand_buf    : 0x0ACB5264    curr_rand_buf           : 0x0ACB520C
    psuedo_rand_buf_a       : 0x0ACB5238    psuedo_rand_buf_a_rx_sz : 2984
    psuedo_rand_buf_b       : 0x0ACB5264    psuedo_rand_buf_b_rx_sz : 3464
    rand_buf_a              : 0x0ACB51E0    rand_buf_a_rx_size      : 4064
    rand_buf_b              : 0x0ACB520C    rand_buf_b_rx_size      : 4064
```

This example shows how to display the TCP statistics:

```
ssl-proxy# show ssl-proxy stats tcp
TCP Statistics:
 Connection related :
    Initiated             : 1970288    Accepted            : 1970288
    Established           : 3797817    Dropped             : 2481867
    Dropped before est    : 142324     Closed              : 3940576
    Persist timeout drops : 0          Rxmt timeout drops  : 0
    Current TIME-WAIT     : 0          Current ESTABLISHED : 0
    Maximum TIME-WAIT     : 1027       Maximum ESTABLISHED : 1961
    Conns Allocated       : 1970288    Conns Deallocated   : 1970288
    Conn Deletes sent     : 3940576    Probe resets        : 0
 Timer related :
    RTT estimates         : 684903022  RTT est. updates    : 684060502
```

```
    delayed acks sent     : 1760943    FIN-WAIT2 timeouts   : 0
    Retransmit timeouts   : 1855840    Persist Timeouts     : 0
    SYN timeouts          : 141865     Idle Timeouts        : 0
    Reassembly timeouts   : 0
 Packet Transmit related :
    Total packets         : 2499818678 Data packets         : 2034445802
    Data bytes sent       : 2837513871 Retransmitted pkts   : 1283476
    Retransmitted bytes   : 311746077  Ack only pkts        : 5444907
    Window probes         : 0          URG only pkts        : 0
    Window Update pkts    : 452160292  Cntrl pkts (S/F/R)   : 6482745
    Tx TOS - normal       : 2499817222 Tx TOS - Min. Cost   : 0
    Tx TOS - max. rel.    : 0          Tx TOS - Max. thru.  : 0
    Tx TOS - min. delay   : 0          Tx TOS - invalid     : 0
 Packet Receive related :
    Total packets         : 2055992562 In seq data pkts     : 1365961238
    In seq data bytes     : 464953685  Bad Offset           : 0
    Too short             : 0          Dup-only data pkts   : 540520
    Dup-only data bytes   : 37642208   Part. dup. data pkts : 0
    Part. Dup. data bytes : 0          OOO data pkts        : 0
    OOO data bytes rcvd   : 0          Pkts after rx win    : 0
    Bytes after rx window : 0          Pkts after close     : 0
    Window Probes         : 0          Duplicate ACKs       : 1197303
    ACKs for unsent data  : 0          ACK-only pkts        : 690294070
    Bytes acked by acks   : 1974287219 Window Update pkts   : 0
    PAWS dropped pkts     : 0          Hdr pred. ACKs       : 664831275
    Hdr pred. data pkts   : 1360706633 TCB cache misses     : 1322565191
    3 dup-only pkts       : 35         Partial Acks         : 0
    Rx TOS - normal       : 2055337650 Rx TOS - Min. Cost   : 0
    Rx TOS - max. rel.    : 0          Rx TOS - Max. thru.  : 0
    Rx TOS - min. delay   : 0          Rx TOS - invalid     : 0
    Unrecognized Options  : 0          Unaligned MSS        : 0
    Unaligned Timestamp   : 0          Unaligned SACK       : 0
    RST ACK's sent        : 0

 Packet Drop statistics :
    Per-flow limit drops  : 0          Aggregate tail drops : 0
    Aggregate random drps : 0          Egress Bufpool drops : 0

 Connection Drop/Close statistics :
    Active                : 659122     Passive              : 656828
    App closed early      : 435        Client Reuse         : 0
    RST Rcvd              : 1169301    Unexp. Data Rcvd     : 0
    Server Reuse          : 0          App initiated abort  : 1313025
    Unexp. SYNs           : 0          Server Refused       : 0
    Other Drops           : 0          Conn Pool Fails      : 0
    Conn Bufpool Drops    : 0          Invalid MSS Drops    : 0
    User clear Drops      : 0          Conn Init Failures   : 0

 Debug Statistics :
    Unaccounted Buffers   : 0          Invalid Conns        : 0
    Output Failures       : 0          Header Bufpool Fails : 0
    MAC channel Fails     : 0          DM Channel Fails     : 0
    Invalid App Opcodes   : 0          MAC Bufpool Fails    : 0
    MAC BufDesc Fails     : 0          Recycle Conn Fails   : 0
    DM chan congested     : 0          MAC chan congested   : 0

ssl-proxy#
```

This example shows how to display the PKI statistics:

```
ssl-proxy# show ssl-proxy stats pki
Authentication request timeout: 180 seconds
Max in process: 50 (requests)
Max queued before dropping: 500 (requests)
```

```
Certificate Authentication & Authorization Statistics:
  Requests started: 1
  Requests finished: 1
  Requests pending to be processed: 0
  Requests waiting for CRL: 0
  Signature only requests: 1
  Valid signature: 0
  Invalid signature: 0
  Total number of invalid certificates: 0
  Approved with warning (no crl check): 1
  Number of times polling CRL: 0
  No certificates present: 0
  Failed to get CRL: 0
  Not authorized (e.g. denied by ACL): 0
  Root certificates not self-signed: 0
  Verify requests failed (e.g. expired or CRL operation failed): 0
  Unknown failure: 0
  Empty certificate chain: 0
  No memory to process requests: 0
  DER encoded certificates missing: 0
  Bad DER certificate length: 0
  Failed to get key from certificate: 0
  Issuer CA not in trusted CA pool: 0
  Issuer CA certificates not valid yet: 0
  Expired issuer CA certificates: 0
  Peer certificates not valid yet: 0
  Expired peer certificates: 0
Peer certificate cache size: 0 (entries), aging timeout: 15 (minutes)
Peer certificate cache statistics:
  In use: 0 (entries)
  Cache hit: 0
  Cache miss: 0
  Cache allocated: 0
  Cache freed: 0
  Cache entries expired: 0
  Cache error: 0
  Cache full (wrapped around): 0
  No memory for caching: 0
Certificate Expiration Warning statistics:
  Proxy service certificates expiring: 0
  CA certificates expiring: 0
  CA pool certificates expiring: 0
  Proxy service certificates expiring SNMP traps sent: 0
Certificate headers statistics:
  Certificate headers formed: 1
  Errors in forming headers: 0
  Prefix error: 0
Key Certificate Table Current Usage (cannot be cleared):
  Total number of entries in table: 8192
  Entries in use: 6
  Free entries: 8186
  Complete service entries: 4
  Incomplete new/renew service entries: 0
  Retiring service entries: 0
  Obsolete service entries: 0
  Complete intermediate CA cert: 1
  Complete root CA cert: 1
  Obsolete intermediate CA cert: 0
  Obsolete root CA cert: 0
PKI Accumulative Counters (cannot be cleared):
  Proxy service trustpoint added: 4
  Proxy service trustpoint deleted: 0
  Proxy service trustpoint modified: 0
  Keypair added: 4
```

```
  Keypair deleted: 0
  Wrong key type: 0
  Service certificate added: 4
  Service certificate deleted: 0
  Service certificate rolled over: 0
  Service certificate completed: 4
  Intermediate CA certificate added: 1
  Intermediate CA certificate deleted: 0
  Root CA certificate added: 1
  Root CA certificate deleted: 0
  Certificate overwritten: 0
  No free table entries: 0
  Rollover failed: 0
Certificate History Statistics (cannot be cleared):
  History records written: 0
  History records deleted: 0
  History records malloc: 0
  History records free: 0
  History records errors: 0
  History records currently kept in memory: 0
  History records have been cleared: 0 times
PKI IPC Counters for normal priority messages:
  Request buffer sent: 3
  Request buffer received: 1
  Request duplicated: 0
  Request send failed: 0
  Response buffer sent: 0
  Response buffer received: 0
  Response timeout: 0
  Response failed: 0
  Response with error reported by SSL Processor: 0
  Response with no request: 0
  Response duplicated: 0
  Message type error: 0
  Message length error: 0
PKI IPC Counters for high priority messages:
  Request buffer sent: 18
  Request buffer received: 0
  Request duplicated: 0
  Request send failed: 0
  Response buffer sent: 0
  Response buffer received: 18
  Response timeout: 0
  Response failed: 0
  Response with error reported by SSL Processor: 0
  Response with no request: 0
  Response duplicated: 0
  Message type error: 0
  Message length error: 0
PKI Memory Usage Counters:
  Malloc count: 237
  Free count: 178
  Malloc failed: 0
  High Priority IPC:
  Ipc alloc count: 36
  Ipc free count: 54
  Ipc alloc failed: 0
  Normal Priority IPC:
  Ipc alloc count: 3
  Ipc free count: 1
  Ipc alloc failed: 0
ssl-proxy#
```

This example shows how to display FDU statistics:

```
ssl-proxy# show ssl-proxy stats fdu
FDU Statistics:
    IP Frag Drops       : 0             IP Version Drops    : 0
    IP Addr Discards    : 0             Serv_Id Drops       : 27
    Conn Id Drops       : 0             Bound Conn Drops    : 0
    Vlan Id Drops       : 0             TCP Checksum Drops  : 0
    Hash Full Drops     : 0             Hash Alloc Fails    : 0
    Flow Creates        : 3940576       Flow Deletes        : 3940576
    Conn Id allocs      : 1970288       Conn Id deallocs    : 1970288
    Tagged Pkts Drops   : 0             Non-Tagg Pkts Drops : 0
    Add ipcs            : 3             Delete ipcs         : 0
    Disable ipcs        : 0             Enable ipcs         : 0
    Unsolicited ipcs    : 0             Duplicate Add ipcs  : 0
    IOS Broadcast Pkts  : 83551         IOS Unicast Pkts    : 1562
    IOS Multicast Pkts  : 0             IOS Total Pkts      : 85113
    IOS Congest Drops   : 0             SYN Discards        : 0
    TCP 5-tuple reuse   : 0


FDU Debug Counters:
    Inv. Conn Drops     : 0             Inv. Conn Pkt Drops : 0
    Inv. TCP opcodes    : 0

ssl-proxy#
```

This example shows how to display the HTTP header insertion statistics:

```
ssl-proxy# show ssl-proxy stats hdr
Header Insert Statistics:
    Session Headers Inserted : 0          Custom Headers Inserted : 1826046
    Session Id's Inserted    : 1826046    Client Cert. Inserted   : 1
    Client IP/Port Inserted  : 0          Req. boundry found      : 1826046
    Content Length Headers   : 0          Chunked Headers         : 0
    Content Length Splt Bufs : 0          Content Length Read Errs: 0
    Buffers allocated        : 0          Buffers Scanned         : 1826049
    Insertion Points Found   : 1826046    Header Overflow         : 3
    End of Header Found      : 1826046    Buffers Accumulated     : 1826049
    Multi-buffer IP Port     : 0          Multi-buffer Session Id : 0
    Multi-buffer Session Hdr : 0          Multi-buffer Custom Hdr : 0
    HTTP Struct Allocs       : 1826046    HTTP Struct Frees       : 1826046
    No End of Hdr Detected   : 0          Payload no HTTP header  : 0
    Desc Alloc Failed        : 0          Buffer Alloc Failed     : 0
    Client Cert Errors       : 1826045    Malloc failed           : 0
    Service Errors           : 0          Conn Entry Invalid      : 0
    Scan Internal Error      : 0          Database Not Initialized: 0
    Unsupported headers      : 0          Chunk Parse Errors      : 0
    Http headers removed     : 0          Http header removal errs: 0
```

This example shows how to display the URL rewrite statistics:

```
ssl-proxy# show ssl-proxy stats url
ssl-proxy#show ssl-pro stats url
URL Rewrite Statistics:
    Rewrites Succeeded   : 0          Rewrites Failed      : 0
    Rsp Scan Incomplete  : 0          URL Scan Incomplete  : 0
    Invalid Conn Entry   : 0          URL Mismatch         : 0
    URL Object Error     : 0          Dbase not initialized: 0
    Scan Internal Error  : 0          Scan Dbase not Init. : 0
    Slash Delim not found: 0
```

This example shows how to display content statistics:

```
ssl-proxy# show ssl-proxy stats content
```

```
Scan object statistics in CPU: SSL1
    Objects in use       : 0
    Obj alloc failures   : 0
    Max obj in use       : 5
```

show ssl-proxy status

To display information about the SSL Services Module proxy status, use the **show ssl-proxy status** command.

show ssl-proxy status

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

EXEC

Command History

Release	Modification
Cisco IOS Release 12.1(13)E and SSL Services Module Release 1.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.
SSL Services Module Release 1.2(1)	The output of the **show ssl-proxy status** command was changed to include statistics that are displayed at a 1-second, 1-minute, and 5-minute traffic rate for CPU utilization.

Examples

This example shows how to display the status of the SSL Services Module:

```
ssl-proxy# show ssl-proxy status
FDU cpu is alive!
FDU cpu utilization:
    % process util   : 0             % interrupt util : 0

    proc cycles : 0x4D52D1B7         int cycles  : 0x6B6C9937
    total cycles: 0xB954D5BEB6FA
    % process util (5 sec)   : 0             % interrupt util (5 sec) : 0

    % process util (1 min)  : 0             % interrupt util (1 min): 0
    % process util (5 min)  : 0             % interrupt util (5 min) : 0


TCP cpu is alive!
TCP cpu utilization:
    % process util   : 0             % interrupt util : 0

    proc cycles : 0xA973D74D         int cycles  : 0xAA03E1D89A
    total cycles: 0xB958C8FF0E73
    % process util (5 sec)   : 0             % interrupt util (5 sec) : 0

    % process util (1 min)  : 0             % interrupt util (1 min): 0
    % process util (5 min)  : 0             % interrupt util (5 min) : 0
```

```
SSL cpu is alive!
SSL cpu utilization:
    % process util   : 0             % interrupt util : 0

    proc cycles : 0xD475444          int cycles  : 0x21865088E
    total cycles: 0xB958CCEB8059
    % process util (5 sec)   : 0             % interrupt util (5 sec) : 0

    % process util (1 min)  : 0             % interrupt util (1 min): 0
    % process util (5 min)  : 0             % interrupt util (5 min) : 0
```

show ssl-proxy version

To display the current image version, use the **show ssl-proxy version** command.

show ssl-proxy version

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

EXEC

Command History

Release	Modification
Cisco IOS Release 12.1(13)E and SSL Services Module Release 1.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.

Examples

This example shows how to display the image version that is currently running on the SSL Services Module:

```
ssl-proxy# show ssl-proxy version
Cisco Internetwork Operating System Software
IOS (tm) SVCSSL Software (SVCSSL-K9Y9-M), Version 12.2(14.6)SSL(0.19)  INTERIM TEST
SOFTWARE
Copyright (c) 1986-2003 by cisco Systems, Inc.
Compiled Thu 10-Apr-03 03:03 by integ
Image text-base: 0x00400078, data-base: 0x00ABE000

ROM: System Bootstrap, Version 12.2(11)YS1 RELEASE SOFTWARE

ssl-proxy uptime is 3 days, 22 hours, 22 minutes
System returned to ROM by power-on
System image file is "tftp://10.1.1.1/unknown"
AP Version 1.2(1)

ssl-proxy#
```

show ssl-proxy vlan

To display VLAN information, use the **show ssl-proxy vlan** command.

show ssl-proxy vlan [*vlan-id* | **debug**]

Syntax Description

vlan-id	(Optional) VLAN ID. Displays information for a specific VLAN; valid values are from 1 to 1005.
debug	(Optional) Displays debug information.

Defaults

This command has no default settings.

Command Modes

EXEC

Command History

Release	Modification
Cisco IOS Release 12.1(13)E and SSL Services Module Release 1.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.

Examples

This example shows how to display all the VLANs that are configured on the SSL Services Module:

```
ssl-proxy# show ssl-proxy vlan
VLAN index 2 (admin VLAN)
   IP addr 10.1.1.1 NetMask 255.0.0.0 Gateway 10.1.1.5
   Network 10.1.1.2 Mask 255.0.0.0 Gateway 10.1.1.6
VLAN index 3
   IP addr 10.1.1.3 NetMask 255.0.0.0 Gateway 10.1.1.6
VLAN index 6
   IP addr 10.1.1.4 NetMask 255.0.0.0

ssl-proxy#
```

Related Commands

ssl-proxy vlan

snmp-server enable

To configure the SNMP traps and informs, use the **snmp-server enable** command. Use the **no** form of this command to disable SNMP traps and informs.

snmp-server enable {**informs** | **traps** {**ipsec** | **isakmp** | **snmp** | {**ssl-proxy** [**cert-expiring**] [**oper-status**]}}}

no snmp-server enable {**informs** | **traps** {**ipsec** | **isakmp** | **snmp** | {**ssl-proxy** [**cert-expiring**] [**oper-status**]}}}

Syntax Description

informs	Enables SNMP informs.
traps	Enables SNMP traps.
ipsec	Enables IPSec traps.
isakmp	Enables ISAKMP traps.
snmp	Enables SNMP traps.
ssl-proxy	Enables SNMP SSL proxy notification traps.
cert-expiring	(Optional) Enables SSL proxy certificate-expiring notification traps.
oper-status	(Optional) Enables SSL proxy operation-status notification traps.

Defaults

This command has no default setting.

Command Modes

Global configuration

Command History

Release	Modification
SSL Services Module Release 2.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.

Examples

This example shows how to enable SNMP informs:

```
ssl-proxy (config)# snmp-server enable informs
ssl-proxy (config)#
```

This example shows how to enable SSL-proxy traps:

```
ssl-proxy (config)# snmp-server enable traps ssl-proxy
ssl-proxy (config)#
```

This example shows how to enable SSL-proxy notification traps:

```
ssl-proxy (config)# snmp-server enable traps ssl-proxy cert-expiring oper-status
ssl-proxy (config)#
```

ssl pre-remove-http-hdr

To remove existing headers prior to inserting a new header, use the **ssl pre-remove-http-hdr** command. Use the **no** form of this command to ignore headers before insertion.

ssl pre-remove-http-hdr

no ssl pre-remove-http-hdr

Defaults

The default behavior for this command is to ignore the existing headers before inserting a new header.

Command Modes

Global configuration

Command History

Release	Modification
SSL Services Module Release 2.1(13)	Support for this command was introduced on the Catalyst 6500 series switches.

Usage Guidelines

This command requests that the SSLM search HTTP messages for all http headers that the SSLM can insert except for custom headers. If any headers are found, they are removed. The command does not search for header prefixes or aliases. This command might impact SSLM performance based on the number of headers present.

Examples

This example shows how to remove existing headers:

```
ssl-proxy (config)# policy http-header example
ssl-proxy (config)# pre-remove-http-hdr
!
```

ssl-proxy crypto selftest

To initiate a cryptographic self-test, use the **ssl-proxy crypto selftest** command. Use the **no** form of this command to disable the testing.

ssl-proxy crypto selftest [**time-interval** *seconds*]

no ssl-proxy crypto selftest

Syntax Description

time-interval *seconds*	(Optional) Sets the time interval between test cases; valid values are from 1 to 8 seconds.

Defaults

3 seconds

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS Release 12.1(13)E and SSL Services Module Release 1.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.

Usage Guidelines

The **ssl-proxy crypto selftest** command enables a set of crypto algorithm tests to be run on the SSL processor in the background. Random number generation, hashing, encryption and decryption, and MAC generation are tested with a time interval between test cases.

This test is run only for troubleshooting purposes. Running this test will impact run-time performance.

To display the results of the self-test, enter the **show ssl-proxy stats crypto** command.

Examples

This example shows how to start a cryptographic self-test:

```
ssl-proxy (config)# ssl-proxy crypto selftest
ssl-proxy (config)#
```

ssl-proxy device-check

To check the health of the crypto device, use the **ssl-proxy device-check** command.

ssl-proxy device-check interval *milliseconds* **reset-limit** *number*

Syntax Description

interval *milliseconds*	Device check interval in milliseconds. The range is from 10 to 60000. 0 = device check disabled.
reset-limit *number*	Number of consecutive resets before rebooting. The range is from 0 to 60. 0 = unlimited.

Defaults

The device check is disabled.

Command Modes

Global configuration

Command History

Release	Modification
SSL Services Module Release 2.1(13)	Support for this command was introduced on the Catalyst 6500 series switches.

Usage Guidelines

This command is normally disabled (device check interval is 0). If the command is enabled, the SSLM checks the crypto device at every interval for proper operation. If there are outstanding requests older than the request interval, the crypto device is reset to return to operational status. A reset limit can also be configured. If the reset limit is set to default (zero), there is no limit. If the reset limit is non zero, the SSLM reboots if the device is reset for more than the reset-limit number of consecutive poll intervals.

Examples

This example shows how to set the device-check interval to 20 milliseconds, and reset-limit to 0:

```
ssl-proxy (config)# ssl-proxy device-check interval 20 reset-limit 0
```

This example shows how to check the number of resets that have occurred using the **show ssl-proxy stats ssl** command. Note the ‘device reset count’ in the output.

```
ssl-proxy# show ssl-proxy stats ssl
SSL Queue Sizes:
    bcm_cmd_ctx_pool_size   : 64           bcm_asym_cmd_ctx_pool_sz: 9000
    bcm_info_pool_size      : 65538        buf_desc_free_q_size    : 94710
    cert_result_free_q_size : 11048        delete_conn_q_size      : 0
    event_q_size            : 0            free_conn_q_size        : 65536
    free_sess_q_size        : 262144       free_sess_active_tmr_qsz: 0
    global_pending_q_size   : 0            to_app_ctx_pool_size    : 512
    ste_asym_req_q_size     : 0            ste_free_req_ctx_pool_sz: 20480
    ste_sym_req_q_size      : 0            available ctx count     : 64
    ctx cleanup count       : 0            device reset count      : 0
```

ssl-proxy mac address

To configure a MAC address, use the **ssl-proxy mac address** command.

ssl-proxy mac address *mac-addr*

Syntax Description

mac-addr	MAC address; see the "Usage Guidelines" section for additional information.

Defaults

This command has no default settings.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS Release 12.1(13)E and SSL Services Module Release 1.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.

Usage Guidelines

Enter the MAC address in this format: H.H.H.

Examples

This example shows how to configure a MAC address:

```
ssl-proxy (config)# ssl-proxy mac address 00e0.b0ff.f232
ssl-proxy (config)#
```

Related Commands

show ssl-proxy mac address

ssl-proxy natpool

To define a pool of IP addresses, which the SSL Services Module uses for implementing the client NAT, use the **ssl-proxy natpool** command.

ssl-proxy natpool *nat-pool-name start-ip-addr* {**netmask** *netmask*}

Syntax Description

nat-pool-name	NAT pool name.
start-ip-addr	Specifies the first IP address in the pool.
netmask *netmask*	Netmask; see the "Usage Guidelines" section for additional information.

Defaults

This command has no default settings.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS Release 12.1(13)E and SSL Services Module Release 1.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.

Examples

This example shows how to define a pool of IP addresses:

```
ssl-proxy (config)# ssl-proxy natpool NP2 207.59.10.01 207.59.10.08 netmask 255.0.0.0
ssl-proxy (config)#
```

Related Commands

show ssl-proxy natpool

ssl-proxy pki

To configure and define the PKI implementation on the SSL Services Module, use the **ssl-proxy pki** command. Use the **no** form of this command to disable the logging and clear the memory.

ssl-proxy pki {{**authenticate** {**timeout** *seconds*}} | {**cache** {{**size** *entries*} | {**timeout** *minutes*}}} | {**certificate** {**check-expiring** {**interval** *hours*}}} | **history**}

no ssl-proxy pki {**authenticate | cache | certificate | history**}

Syntax Description

authenticate	Configures the certificate authentication and authorization.
timeout *seconds*	Specifies the timeout in seconds for each request; valid values are from 1 to 600 seconds.
cache	Configures the peer-certificate cache.
size *entries*	Specifies the maximum number of cache entries; valid values are from 0 to 5000 entries.
timeout *minutes*	Specifies the aging timeout value of entries; valid values are from 1 to 600 minutes.
certificate	Configures the check-expiring interval.
check-expiring interval *hours*	Specifies the check-expiring interval; valid values are from 0 to 720 hours.
history	Key and certificate history.

Defaults

The default settings are as follows:

- **timeout** *seconds*—**180** seconds
- **size** *entries*—**0** entries
- **timeout** *minutes*—**15** minutes
- **interval** *hours*—**0** hours, do not check

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS Release 12.1(13)E and SSL Services Module Release 1.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.
SSL Services Module Release 2.1(1)	This command was changed to add the following keywords: • **authenticate** • **cache** • **certificate**

Usage Guidelines

The **ssl-proxy pki history** command enables logging of certificate history records per-proxy service into memory and generates a syslog message per record. Each record tracks the addition or deletion of a key pair or certificate into the proxy services key and the certificate table.

When the index of the table changes, this command logs the following information:

- Key pair name
- Trustpoint label
- Service name
- Subject name
- Serial number of the certificate

Up to 512 records can be stored in the memory at one time.

Examples

This example shows how to specify the timeout in seconds for each request:

```
ssl-proxy (config)# ssl-proxy pki authenticate timeout 200
ssl-proxy (config)#
```

This example shows how to specify the cache size:

```
ssl-proxy (config)# ssl-proxy pki cache size 50
ssl-proxy (config)#
```

This example shows how to specify the aging timeout value of entries:

```
ssl-proxy (config)# ssl-proxy pki cache timeout 20
ssl-proxy (config)#
```

This example shows how to specify the check-expiring interval:

```
ssl-proxy (config)# ssl-proxy pki certificate check-expiring interval 100
ssl-proxy (config)#
```

This example shows how to enable PKI event-history:

```
ssl-proxy (config)# ssl-proxy pki history
ssl-proxy (config)#
```

Related Commands

show ssl-proxy stats

ssl-proxy policy http-header

To enter the HTTP header insertion configuration submode, use the **ssl-proxy policy http-header** command.

ssl-proxy policy http-header *http-header-policy-name*

Syntax Description

http-header-policy-name	HTTP header policy name.

Defaults

This command has no default settings.

Command Modes

Global configuration

Command History

Release	Modification
SSL Services Module Release 2.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.

Usage Guidelines

In HTTP header insertion configuration submode, you can define the HTTP header insertion content policy that is applied to the payload.

HTTP header insertion allows you to insert additional HTTP headers to indicate to the real server that the connection is actually an SSL connection. These headers allows server applications to collect correct information for each SSL session and/or client.

You can insert these header types:

- Client Certificate—Client certificate header insertion allows the back-end server to see the attributes of the client certificate that the SSL module has authenticated and approved. When you specify **client-cert**, the SSL module passes the following headers to the back-end server:
  - Client IP and Port Address—Network address translation (NAT) removes the client IP address and port information. When you specify **client-ip-port**, the SSL module inserts the client IP address and information about the client port into the HTTP header, allowing the server to see the client IP address and port.
  - Custom—When you specify **custom** *custom-string*, the SSL module inserts the user-defined header into the HTTP header.
  - Prefix—When you specify **prefix** *prefix-string*, the SSL module adds the specified prefix into the HTTP header to enable the server to identify that the connections are coming from the SSL module, not from other appliances.
- SSL Session—Session headers, including the session ID, are used to cache client certificates that are based on the session ID. The session headers are also cached on a session basis if the server wants to track connections that are based on a particular cipher suite. When you specify **session**, the SSL module passes information that is specific to an SSL connection to the back-end server as session headers.

Table 2-2 lists the commands available in HTTP header insertion configuration submode.

Table 2-2 HTTP Header Insertion Configuration Submode Command Descriptions

client-cert	Allows the back-end server to see the attributes of the client certificate that the SSL module has authenticated and approved.
client-ip-port	Inserts the client IP address and information about the client port into the HTTP header, allowing the server to see the client IP address and port.
custom *custom-string*	Inserts the *custom-string* header into the HTTP header. The maximum *custom-string* length is 239 characters. If this length is exceeded, an "Incomplete command" error will display. If the string includes spaces, you must enclose it in quotes ("").
prefix	Adds the *prefix-string* to the HTTP header to enable the server to identify the connections that come from the SSL module, not from other appliances
session	Passes information that is specific to an SSL connection to the back-end server as session headers.

Examples

This example shows how to enter the HTTP header insertion configuration submode:

```
ssl-proxy (config)# ssl-proxy policy http-header test1
ssl-proxy (config-http-header-policy)#
```

This example shows how to allow the back-end server to see the attributes of the client certificate that the SSL module has authenticated and approved:

```
ssl-proxy (config-http-header-policy)# client-cert
ssl-proxy (config-http-header-policy)#
```

This example shows how to insert the client IP address and information about the client port into the HTTP header, allowing the server to see the client IP address and port:

```
ssl-proxy (config-http-header-policy)# client-ip-cert
ssl-proxy (config-http-header-policy)#
```

This example shows how to insert the custom-string header into the HTTP header:

```
ssl-proxy (config-http-header-policy)# custom SSL-Frontend:Enable
ssl-proxy (config-http-header-policy)#
```

This example shows how to add the prefix-string into the HTTP header:

```
ssl-proxy (config-http-header-policy)# prefix
ssl-proxy (config-http-header-policy)#
```

This example shows how to pass information that is specific to an SSL connection to the back-end server as session headers:

```
ssl-proxy (config-http-header-policy)# session
ssl-proxy (config-http-header-policy)#
```

Related Commands

show ssl-proxy policy

ssl-proxy policy ssl

To enter the SSL-policy configuration submode, use the **ssl-proxy policy ssl** command. In the SSL-policy configuration submode, you can define the SSL policy for one or more SSL-proxy services.

ssl-proxy policy ssl *ssl-policy-name*

Syntax Description

ssl-policy-name	SSL policy name.

Defaults

The defaults are as follows:

- **cipher** is all.
- **close-protocol** is enabled.
- **session-caching** is enabled.
- **version** is all.
- **session-cache size** *size* is 262143 entries.
- **timeout session** *timeout* is 0 seconds.
- **timeout handshake** *timeout* is 0 seconds.
- **cert-req empty** is disabled.
- **tls-rollback** is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS Release 12.1(13)E and SSL Services Module Release 1.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.
SSL Services Module Release 1.2(1)	This command was changed to add the following subcommands: • **session-cache size** *size* • **timeout session** *timeout* [**absolute**]
SSL Services Module Release 2.1(5)	This command was changed to add the following subcommands: • **cert-req empty** • **tls-rollback** [**current** | **any**]

Usage Guidelines

Each SSL-policy configuration submode command is entered on its own line.

Table 2-3 lists the commands available in SSL-policy configuration submode.

Table 2-3 SSL-Policy Configuration Submode Command Descriptions

cert-req empty	Allows you to specify that the SSL Services Module backend service always returns the certificate associated with the trustpoint and does not look for a CA-name match.
cipher-suite {**RSA_WITH_3DES_EDE_CBC_SHA** | **RSA_WITH_DES_CBC_SHA** | **RSA_WITH_RC4_128_MD5** | **RSA_WITH_RC4_128_SHA** | **all**}	Allows you to configure a list of cipher-suites acceptable to the proxy-server; see the "Usage Guidelines" section for information about the cipher suites.
[**no**] **close-protocol enable**	Allows you to configure the SSL close-protocol behavior. Use the **no** form of this command to disable close protocol.
default {**cipher** | **close-protocol** | **session-cache** | **version**}	Sets a command to its default settings.
exit	Exits from SSL-policy configuration submode.
help	Provides a description of the interactive help system.
[**no**] **session-cache enable**	Allows you to enable the session-caching feature. Use the **no** form of this command to disable session-caching.
session-cache size *size*	Specifies the maximum number of session entries to be allocated for a given service; valid values are from 1 to 262143 entries.
timeout handshake *timeout*	Allows you to configure how long the module keeps the connection in handshake phase; valid values are from 0 to 65535 seconds.
timeout session *timeout* [**absolute**]	Allows you to configure the session timeout. The syntax description is as follows: • *timeout*—Session timeout; valid values are from 0 to 72000 seconds. • **absolute—**(Optional) The session entry is not removed until the configured timeout has completed.
tls-rollback [**current** | **any**]	Allows you to specify if the SSL protocol version number in the TLS/SSL premaster secret message is either the maximum version or the negotiated version (**current**), or if the version is not checked (**any**).
version {**all** | **ssl3** | **tls1**}	Allows you to set the version of SSL to one of the following: • **all**—Both SSL3 and TLS1 versions are used. • **ssl3**—SSL version 3 is used. • **tls1**—TLS version 1 is used.

You can define the SSL policy templates using the **ssl-proxy policy ssl** *ssl-policy-name* command and associate a SSL policy with a particular proxy server using the proxy server configuration CLI. The SSL policy template allows you to define various parameters that are associated with the SSL handshake stack.

When you enable **close-notify**, a close-notify alert message is sent to the client and a close-notify alert message is expected from the client as well. When disabled, the server sends a close-notify alert message to the client; however, the server does not expect or wait for a close-notify message from the client before tearing down the session.

The cipher-suite names follow the same convention as the existing SSL stacks.

The cipher-suites that are acceptable to the proxy-server are as follows:

- RSA_WITH_3DES_EDE_CBC_SHA— RSA with 3des-sha
- RSA_WITH_DES_CBC_SHA—RSA with des-sha
- RSA_WITH_RC4_128_MD5—RSA with rc4-md5
- RSA_WITH_RC4_128_SHA—RSA with rc4-sha
- all—All supported ciphers

If you enter the **timeout session** *timeout* **absolute** command, the session entry is kept in the session cache for the configured timeout before it is cleaned up. If the session cache is full, the timers are active for all the entries, the **absolute** keyword is configured, and all further new sessions are rejected.

If you enter the **timeout session** *timeout* command without the **absolute** keyword, the specified timeout is treated as the maximum timeout and a best-effort is made to keep the session entry in the session cache. If the session cache runs out of session entries, the session entry that is currently being used is removed for incoming new connections.

When you enter the **cert-req empty** command, the SSL Services Module backend service always returns the certificate associated with the trustpoint and does not look for CA-name match. By default, the SSL Services Module always looks for the CA-name match before returning the certificate. If the SSL server does not include a CA-name list in the certificate request during client authentication, the handshake fails.

By default, the SSL Services Module uses the maximum supported SSL protocol version (SSL2.0, SSL3.0, TLS1.0) in the ClientHello message. Enter the **tls-rollback** [**current** | **any**] command if the SSL client uses the negotiated version instead of the maximum supported version (as specified in the ClientHello message).

When you enter the **tls-rollback current** command, the SSL protocol version can be either the maximum supported version or the negotiated version.

When you enter the **tls-rollback any** command, the SSL protocol version is not checked at all.

Examples

This example shows how to enter the SSL-policy configuration submode:

```
ssl-proxy (config)# ssl-proxy policy ssl sslpl1
ssl-proxy (config-ssl-policy)#
```

This example shows how to define the cipher suites that are supported for the SSL-policy:

```
ssl-proxy (config-ssl-policy)# cipher RSA_WITH_3DES_EDE_CBC_SHA
ssl-proxy (config-ssl-policy)#
```

This example shows how to enable the SSL-session closing protocol:

```
ssl-proxy (config-ssl-policy)# close-protocol enable
ssl-proxy (config-ssl-policy)#
```

This example shows how to disable the SSL-session closing protocol:

```
ssl-proxy (config-ssl-policy)# no close-protocol enable
ssl-proxy (config-ssl-policy)#
```

These examples shows how to set a given command to its default setting:

```
ssl-proxy (config-ssl-policy)# default cipher
ssl-proxy (config-ssl-policy)# default close-protocol
ssl-proxy (config-ssl-policy)# default session-cache
ssl-proxy (config-ssl-policy)# default version
ssl-proxy (config-ssl-policy)#
```

This example shows how to enable session-cache:

```
ssl-proxy (config-ssl-policy)# session-cache enable
ssl-proxy (config-ssl-policy)#
```

This example shows how to disable session-cache:

```
ssl-proxy (config-ssl-policy)# no session-cache enable
ssl-proxy (config-ssl-policy)#
```

This example shows how to set the maximum number of session entries to be allocated for a given service:

```
ssl-proxy (config-ssl-policy)# session-cache size 22000
ssl-proxy (config-ssl-policy)#
```

This example shows how to configure the session timeout to absolute:

```
ssl-proxy (config-ssl-policy)# timeout session 30000 absolute
ssl-proxy (config-ssl-policy)#
```

These examples show how to enable the support of different SSL versions:

```
ssl-proxy (config-ssl-policy)# version all
ssl-proxy (config-ssl-policy)# version ssl3
ssl-proxy (config-ssl-policy)# version tls1
ssl-proxy (config-ssl-policy)#
```

This example shows how to print out a help page:

```
ssl-proxy (config-ssl-policy)# help
ssl-proxy (config-ssl-policy)#
```

Related Commands

show ssl-proxy stats
show ssl-proxy stats ssl

ssl-proxy policy tcp

To enter the proxy policy TCP configuration submode, use the **ssl-proxy policy tcp** command. In proxy-policy TCP configuration submode, you can define the TCP policy templates.

ssl-proxy policy tcp *tcp-policy-name*

Syntax Description

tcp-policy-name	TCP policy name.

Defaults

The defaults are as follows:

- **timeout inactivity** is 600 seconds.
- **timeout fin-wait** is 600 seconds.
- **buffer-share rx** is 32768 bytes.
- **buffer-share tx** is 32768 bytes.
- **mss** is 1500 bytes.
- **timeout syn** is 75 seconds.
- **timeout reassembly** is 60 seconds.
- **tos carryover** is disabled

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS Release 12.1(13)E and SSL Services Module Release 1.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.
SSL Services Module Release 1.2(1)	This command was changed to add the **timeout reassembly** *time* subcommand.
SSL Services Module Release 2.1(4)	This command was changed to add the **tos carryover**subcommand.

Usage Guidelines

After you define the TCP policy, you can associate the TCP policy with a proxy server using the proxy-policy TCP configuration submode commands.

Each proxy-policy TCP configuration submode command is entered on its own line.

Table 2-4 lists the commands that are available in proxy-policy TCP configuration submode.

Table 2-4 Proxy-policy TCP Configuration Submode Command Descriptions

default	Sets a command to its default settings.
exit	Exits from proxy-service configuration submode.
[**no**] **timeout fin-wait** *timeout-in-seconds*	Allows you to configure the FIN wait timeout; valid values are from 75 to 600 seconds. Use the **no** form of this command to return to the default setting.
help	Provides a description of the interactive help system.
[**no**] **timeout inactivity** *timeout-in-seconds*	Allows you to configure the inactivity timeout; valid values are from 0 to 960 seconds. This command allows you to set the aging timeout for an idle connection and helps protect the connection resources. Use the **no** form of this command to return to the default setting.
[**no**] **buffer-share rx** *buffer-limit-in-bytes*	Allows you to configure the maximum size of the receive buffer share per connection; valid values are from 8192 to 262144. Use the **no** form of this command to return to the default setting. **Note** When large encrypted files are transferred by the module, the receive buffer size must be at least the maximum SSL record size of 16384 bytes for reassembly of the SSL record. We recommend a receive buffer size of at least 20000 bytes for optimal performance.
[**no**] **buffer-share tx** *buffer-limit-in-bytes*	Allows you to configure the maximum size of the transmit buffer share per connection; valid values are from 8192 to 262144. Use the **no** form of this command to return to the default setting. **Note** When large encrypted files are transferred by the module, the transmit buffer size must be at least the maximum SSL record size of 16384 bytes for reassembly of the SSL record. We recommend a transmit buffer size of at least 20000 bytes for optimal performance.
[**no**] **mss** *max-segment-size-in-bytes*	Allows you to configure the maximum segment size that the connection identifies in the generated SYN packet; valid values are from 64 to 1460. Use the **no** form of this command to return to the default setting.
[**no**] **timeout syn** *timeout-in-seconds*	Allows you to configure the connection establishment timeout; valid values are from 5 to 75 seconds. Use the **no** form of this command to return to the default setting.

Table 2-4 Proxy-policy TCP Configuration Submode Command Descriptions (continued)

[**no**] **timeout reassembly** *time*	Allows you to configure the amount of time in seconds before the reassembly queue is cleared; valid values are from 0 to 960 seconds (0 = disabled). If the transaction is not complete within the specified time, the reassembly queue is cleared and the connection is dropped. Use the **no** form of this command to return to the default setting.
[**no**] **tos carryover**	Forwards the type of service (ToS) value to all packets within a flow. **Note** If the policy is configured as a server TCP policy, the ToS value is sent from the server to the client. If the policy is configured as a virtual policy, the ToS value is sent from the client to the server. **Note** The ToS value needs to be learned before it can be propagated. For example, when a ToS value is configured to be propagated from the server to client connection, the server connection must be established before the value is learned and propagated. Therefore, some of the initial packets will not carry the ToS value.

Usage Guidelines

TCP commands that you enter on the SSL Services Module can apply either globally or to a particular proxy server.

You can configure a different maximum segment size for the client side and the server side of the proxy server.

The TCP policy template allows you to define parameters that are associated with the TCP stack.

You can either enter the **no** form of the command or use the **default** keyword to return to the default setting.

Examples

This example shows how to enter the proxy-policy TCP configuration submode:

```
ssl-proxy (config)# ssl-proxy policy tcp tcppl1
ssl-proxy (config-tcp-policy)#
```

These examples show how to set a given command to its default value:

```
ssl-proxy (config-tcp-policy)# default timeout fin-wait
ssl-proxy (config-tcp-policy)# default inactivity-timeout
ssl-proxy (config-tcp-policy)# default buffer-share rx
ssl-proxy (config-tcp-policy)# default buffer-share tx
ssl-proxy (config-tcp-policy)# default mss
ssl-proxy (config-tcp-policy)# default timeout syn
ssl-proxy (config-tcp-policy)#
```

This example shows how to define the FIN-wait timeout in seconds:

```
ssl-proxy (config-tcp-policy)# timeout fin-wait 200
ssl-proxy (config-tcp-policy)#
```

This example shows how to define the inactivity timeout in seconds:

```
ssl-proxy (config-tcp-policy)# timeout inactivity 300
ssl-proxy (config-tcp-policy)#
```

This example shows how to define the maximum size for the receive buffer configuration:

```
ssl-proxy (config-tcp-policy)# buffer-share rx 16384
ssl-proxy (config-tcp-policy)#
```

This example shows how to define the maximum size for the transmit buffer configuration:

```
ssl-proxy (config-tcp-policy)# buffer-share tx 13444
ssl-proxy (config-tcp-policy)#
```

This example shows how to define the maximum size for the TCP segment:

```
ssl-proxy (config-tcp-policy)# mss 1460
ssl-proxy (config-tcp-policy)#
```

This example shows how to define the initial connection (SYN)-timeout value:

```
ssl-proxy (config-tcp-policy)# timeout syn 5
ssl-proxy (config-tcp-policy)#
```

This example shows how to define the reassembly-timeout value:

```
ssl-proxy (config-tcp-policy)# timeout reassembly 120
ssl-proxy (config-tcp-policy)#
```

This example shows how to enable carryover the ToS value to all packets within a flow:

```
ssl-proxy (config-tcp-policy)# tos carryover
ssl-proxy (config-tcp-policy)#
```

Related Commands

show ssl-proxy policy

ssl-proxy policy url-rewrite

To enter the URL rewrite configuration submode, use the **ssl-proxy policy url-rewrite** command. In URL rewrite configuration submode, you can define the URL-rewrite content policy that is applied to the payload.

ssl-proxy policy url-rewrite *url-rewrite-policy-name*

Syntax Description

url-rewrite-policy-name	URL rewrite policy name.

Defaults

This command has no arguments or keywords.

Command Modes

Global configuration

Command History

Release	Modification
SSL Services Module Release 2.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.

Usage Guidelines

URL rewrite allows you to rewrite redirection links only.

A URL rewrite policy consists of up to 32 rewrite rules for each SSL proxy service.

Table 2-5 lists the commands that are available in proxy-policy configuration submode.

Table 2-5 Proxy-policy Configuration Submode Command Descriptions

default	Sets a command to its default settings.
exit	Exits from proxy-policy configuration submode.
help	Provides a description of the interactive help system.
[**no**] **url** *url-string*[**clearport** *port-number* | **sslport** *port-number*]	Allows you to configure the URL string to be rewritten. Use the **no** form of this command to remove the policy.

url-string—Specifies the host portion of the URL link to be rewritten; it can have a maximum of 251 characters. You can use the "*" wildcard only as a prefix or a suffix of a *hostname* in a rewrite rule. For example, you can use the *hostname* in one of the following ways:

- www.cisco.com
- *.cisco.com
- wwwin.cisco.*

clearport *port-number*—(Optional) Specifies the port portion of the URL link that is to be rewritten; valid values are from 1 to 65535.

sslport *port-number*—(Optional) Specifies the *port* portion of the URL link that is to be written; valid values are from 1 to 65535.

Enter the **no** form of the command to remove the policy.

Note When a server includes the default HTTP port number 80 in a URL redirect (for example, www.example.com:80), then the **url** command must be configured in the same manner (for example, **url www.example.com:80**). Non-standard port numbers need not be configured as part of the URL, but may instead by configured using the **clearport** keyword.

Examples

This example shows how to enter the URL rewrite configuration submode for the test1 policy:

```
ssl-proxy (config)# ssl-proxy policy url-rewrite test1
ssl-proxy(config-url-rewrite-policy#
```

This example shows how to define the URL rewrite policy for the test1 policy:

```
ssl-proxy (config)# ssl-proxy policy url-rewrite test1
ssl-proxy(config-url-rewrite-policy# url www.cisco.com clearport 80 sslport 443
ssl-proxy(config-url-rewrite-policy#
```

This example shows how to delete the URL rewrite policy for the test1 policy:

```
ssl-proxy (config)# ssl-proxy policy url-rewrite test1
ssl-proxy(config-url-rewrite-policy# no url www.cisco.com clearport 80 sslport 443
ssl-proxy(config-url-rewrite-policy#
```

Related Commands

show ssl-proxy policy

ssl-proxy pool ca

To enter the certificate authority pool configuration submode, use the **ssl-proxy pool ca** command. In the certificate authority pool configuration submode, you can configure a certificate authority pool, which lists the CAs that the module can trust.

ssl-proxy pool *ca-pool-name*

Syntax Description

ca-pool-name	Certificate authority pool name.

Defaults

This command has no arguments or keywords.

Command Modes

Global configuration

Command History

Release	Modification
SSL Services Module Release 2.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.

Usage Guidelines

Enter each certificate-authority pool configuration submode command on its own line.

Table 2-6 lists the commands that are available in certificate-authority pool configuration submode.

Table 2-6 Proxy-policy TCP Configuration Submode Command Descriptions

ca	Configures a certificate authority. The available subcommand is as follows: **trustpoint** *ca-trustpoint-name*—Configures a certificate-authority trustpoint. Use the **no** form of this command to return to the default setting.
default	Sets a command to its default settings.
exit	Exits from proxy-service configuration submode.
help	Allows you to configure the connection-establishment timeout; valid values are from 5 to 75 seconds. Use the **no** form of this command to return to the default setting.

Examples

This example shows how to add a certificate-authority trustpoint to a pool:

```
ssl-proxy (config)# ssl-proxy pool test1
ssl-proxy(config-ca-pool)# ca trustpoint test20
ssl-proxy(config-ca-pool)#
```

ssl-proxy service

To enter the proxy-service configuration submode, use the **ssl-proxy-service** command.

ssl-proxy service *ssl-proxy-name* [**client**]

Syntax Description

ssl-proxy-name	SSL proxy name.
client	(Optional) Allows you to configure the SSL-client proxy services. See the **ssl-proxy service client** command.

Defaults

Server NAT is enabled, and client NAT is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS Release 12.1(13)E and SSL Services Module Release 1.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.
SSL Services Module Release 2.1(1)	This command was changed to include the following keywords: • **authenticate**—Configures the certificate verification method. • **client**—Configures the SSL-client proxy services. • **policy urlrewrite—**Applies a URL rewrite policy to a proxy server. • **sslv2**—Enables SSL version 2; see the **server ipaddr** *ip-addr* **protocol** *protocol* **port** *portno* subcommand. • **trusted-ca** *ca-pool-name*—Applies the trusted certificate authority configuration to a proxy server.

Usage Guidelines

In proxy-service configuration submode, you can configure the virtual IP address and port that is associated with the proxy service and the associated target IP address and port. You can also define TCP and SSL policies for both the client side (beginning with the **virtual** keyword) and the server side of the proxy (beginning with the **server** keyword).

In client proxy-service configuration submode, you specify that the proxy service accept clear-text traffic, encrypt it into SSL traffic, and forward it to the back-end SSL server.

In most cases, all of the SSL-server-proxy configurations that are performed are also valid for the SSL-client-proxy configuration, except for the following:

- You must configure a certificate for the SSL-server-proxy but you do not have to configure a certificate for the SSL-client-proxy. If you configure a certificate for the SSL-client-proxy, that certificate is sent in response to the certificate request message that is sent by the server during the client-authentication phase of the handshake protocol.
- The SSL policy is attached to the virtual subcommand for ssl-server-proxy where as it is attached to server SSL-client-proxy subcommand.

Enter each proxy-service or proxy-client configuration submode command on its own line.

Table 2-7 lists the commands that are available in proxy-service or proxy-client configuration submode.

Table 2-7 Proxy-service Configuration Submode Command Descriptions

Syntax	Description
authenticate verify {**all** | **signature-only**}	Configures the method for certificate verification. You can specify the following: • **all**—Verifies CRLs and signature authority. • **signature-only**—Verifies the signature only.
certificate rsa general-purpose trustpoint *trustpoint-name*	Configures the certificate with RSA general-purpose keys and associates a trustpoint to the certificate.
default {**certificate** | **inservice** | **nat** | **server** | **virtual**}	Sets a command to its default settings.
exit	Exits from proxy-service or proxy-client configuration submode.
help	Provides a description of the interactive help system.
inservice	Declares a proxy server or client as administratively up.
nat {**server** | **client** *natpool-name*}	• **server—**Enables the network address translation (NAT) for the destination IP addresses, when the client-side traffic is forwarded to the server. When this is enabled, the destination IP address is replaced with the service's server IP addresses. By default **nat server** is enabled. • **client** *natpool-name*—Enables network address translation (NAT) for the source IP addresses when the client-side traffic is forwarded to the server. The pool of addresses is defined in a corresponding instance of the nat pool command. **Note** A pool of minimum eight IP addresses must be configured. By default **nat client** is disabled.
policy urlrewrite *policy-name*	Applies a URL rewrite policy to a proxy server.
server ipaddr *ip-addr* **protocol** *protocol* **port** *portno* [**sslv2**]	Defines the IP address of the target server for the proxy server. You can also specify the port number and the transport protocol. The target IP address can be a virtual IP address of an SLB device or a real IP address of a web server. The **sslv2** keyword specifies the server that is used for handling SSL version 2 traffic.
server policy tcp *server-side-tcp-policy-name*	Applies a TCP policy to the server side of a proxy server. You can specify the port number and the transport protocol.
trusted-ca *ca-pool-name*	Applies a trusted certificate authenticate configuration to a proxy server.

Table 2-7 Proxy-service Configuration Submode Command Descriptions (continued)

Syntax	Description
virtual {**ipaddr** *ip-addr*} {**protocol** *protocol*} {**port** *portno*} [**secondary**]	Defines the virtual IP address of the virtual server to which the STE is proxying. You can also specify the port number and the transport protocol. The valid values for *protocol* are **tcp**; valid values for *portno* is from 1 to 65535. The **secondary** keyword (optional) prevents the STE from replying to the ARP request coming to the virtual IP address.
virtual {**policy ssl** *ssl-policy-name*}	Applies an SSL policy with the client side of a proxy server.
virtual {**policy tcp** *client-side-tcp-policy-name*}	Applies a TCP policy to the client side of a proxy server.

Both secured and bridge mode between the Content Switching Module (CSM) and the SSL Services Module is supported.

Use the **secondary** keyword (optional) for bridge-mode topology.

Examples

This example shows how to enter the proxy-service configuration submode:

```
ssl-proxy (config)# ssl-proxy service S6
ssl-proxy (config-ssl-proxy)#
```

This example shows how to configure the method for certificate verification:

```
ssl-proxy (config-ssl-proxy)# authenticate verify all
ssl-proxy (config-ssl-proxy)#
```

This example shows how to configure the certificate for the specified SSL-proxy services:

```
ssl-proxy (config-ssl-proxy)# certificate rsa general-purpose trustpoint tp1
ssl-proxy (config-ssl-proxy)#
```

These examples show how to set a specified command to its default value:

```
ssl-proxy (config-ssl-proxy)# default certificate
ssl-proxy (config-ssl-proxy)# default inservice
ssl-proxy (config-ssl-proxy)# default nat
ssl-proxy (config-ssl-proxy)# default server
ssl-proxy (config-ssl-proxy)# default virtual
ssl-proxy (config-ssl-proxy)#
```

This example shows how to apply a trusted-certificate authenticate configuration to a proxy server:

```
ssl-proxy (config-ssl-proxy)# trusted-ca test1
ssl-proxy (config-ssl-proxy)#
```

This example shows how to configure a virtual IP address for the specified virtual server:

```
ssl-proxy (config-ssl-proxy)# virtual ipaddr 207.59.100.20 protocol tcp port 443
ssl-proxy (config-ssl-proxy)#
```

This example shows how to configure the SSL policy for the specified virtual server:

```
ssl-proxy (config-ssl-proxy)# virtual policy ssl sslpl1
ssl-proxy (config-ssl-proxy)#
```

This example shows how to configure the TCP policy for the specified virtual server:

```
ssl-proxy (config-ssl-proxy)# virtual policy tcp tcppl1
ssl-proxy (config-ssl-proxy)#
```

This example shows how to configure a clear-text web server for the SSL Services Module to forward the decrypted traffic:

```
ssl-proxy (config-ssl-proxy)# server ipaddr 207.50.0.50 protocol tcp port 80
ssl-proxy (config-ssl-proxy)#
```

This example shows how to configure a TCP policy for the given clear-text web server:

```
ssl-proxy (config-ssl-proxy)# server policy tcp tcppl1
ssl-proxy (config-ssl-proxy)#
```

This example shows how to configure a NAT pool for the client address that is used in the server connection of the specified service SSL offload:

```
ssl-proxy (config-ssl-proxy)# nat client NP1
ssl-proxy (config-ssl-proxy)#
```

This example shows how to enable NAT for the destination IP addresses, when the client-side traffic is forwarded to the server and how to enable NAT for the source IP addresses when the client-side traffic is forwarded to the server.

```
ssl-proxy (config-ssl-proxy)# nat server
  client  Enable client nat
  server  Enable server nat

Ssl-proxy(config-ssl-proxy)#nat server

Ssl-proxy(config-ssl-proxy)#nat client
Ssl-proxy(config-ssl-proxy)#exit
Ssl-proxy(config-context)#natpool Test_nat 192.168.10.1 192.168.10.8
  netmask  netmask
Ssl-proxy(config-context)#natpool Test_nat 192.168.10.1 192.168.10.8 netmask 255.255.255.0
Ssl-proxy(config-context)#natpool Test_nat 192.168.10.1 192.168.10.8 netmask 255.255.255.0
```

Related Commands

show ssl-proxy service

ssl-proxy service client

To enter the client proxy-service configuration submode, use the **ssl-proxy service client** command.

ssl-proxy service *ssl-proxy-name* **client**

Syntax Description

ssl-proxy-name	SSL proxy service name.

Defaults

Client NAT is disabled.

Command Modes

Global configuration

Command History

Release	Modification
SSL Services Module Release 2.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.

Usage Guidelines

In client proxy-service configuration submode, you specify that the proxy service accept clear-text traffic, encrypt it into SSL traffic, and forward it to the back-end SSL server.

In most cases, all of the SSL-server-proxy configurations that are performed are also valid for the SSL-client-proxy configuration, except for the following:

- You must configure a certificate for the SSL-server-proxy but you do not have to configure a certificate for the SSL-client-proxy. If you configure a certificate for the SSL-client-proxy, that certificate is sent in response to the certificate request message that is sent by the server during the client-authentication phase of handshake protocol.
- The SSL policy is attached to the virtual subcommand for ssl-server-proxy where as it is attached to server SSL-client-proxy subcommand.

Each proxy-service or proxy-client configuration submode command is entered on its own line.

Table 2-8 lists the commands that are available in proxy-client configuration submode.

Table 2-8 Proxy-client Configuration Submode Command Descriptions

Syntax	Description
certificate rsa general-purpose trustpoint *trustpoint-name*	Configures the certificate with RSA general-purpose keys and associates a trustpoint to the certificate.
default {**certificate** | **inservice** | **nat** | **server** | **virtual**}	Sets a command to its default settings.
exit	Exits from proxy-client configuration submode.
help	Provides a description of the interactive help system.
inservice	Declares a proxy client as administratively up.

Table 2-8 Proxy-client Configuration Submode Command Descriptions (continued)

Syntax	Description
nat {**server** | **client** *natpool-name*}	Specifies the usage of either server NAT or client NAT for the server side connection that is opened by the SSL Services Module.
policy urlrewrite *policy-name*	Applies a URL rewrite policy to the proxy server.
server ipaddr *ip-addr* **protocol** *protocol* **port** *portno* [**sslv2**]	Defines the IP address of the target server for the proxy server. You can also specify the port number and the transport protocol. The target IP address can be a virtual IP address of an SLB device or a real IP address of a web server. The **sslv2** keyword enables SSL version 2.
server policy tcp *server-side-tcp-policy-name*	Applies a TCP policy to the server side of a proxy server. You can specify the port number and the transport protocol.
virtual {**ipaddr** *ip-addr*} {**protocol** *protocol*} {**port** *portno*} [**secondary**]	Defines the IP address of the target server for the proxy server. You can also specify the port number and the transport protocol. The target IP address can be a virtual IP address of an SLB device or a real IP address of a web server. The **sslv2** keyword specifies the server that is used for handling SSL version 2 traffic.
virtual {**policy ssl** *ssl-policy-name*}	Applies an SSL policy with the client side of a proxy server.
virtual {**policy tcp** *client-side-tcp-policy-name*}	Applies a TCP policy to the client side of a proxy server.

Both secured and bridge mode between the Content Switching Module (CSM) and the SSL Services Module is supported.

Use the **secondary** keyword (optional) for bridge-mode topology.

Examples

This example shows how to enter the client proxy-service configuration submode:

```
ssl-proxy (config)# ssl-proxy service S7 client
ssl-proxy (config-ssl-proxy)#
```

This example shows how to configure the certificate for the specified SSL-proxy services:

```
ssl-proxy (config-ssl-proxy)# certificate rsa general-purpose trustpoint tp1
ssl-proxy (config-ssl-proxy)#
```

These examples show how to set a specified command to its default value:

```
ssl-proxy (config-ssl-proxy)# default certificate
ssl-proxy (config-ssl-proxy)# default inservice
ssl-proxy (config-ssl-proxy)# default nat
ssl-proxy (config-ssl-proxy)# default server
ssl-proxy (config-ssl-proxy)# default virtual
ssl-proxy (config-ssl-proxy)#
```

This example shows how to configure a virtual IP address for the specified virtual server:

```
ssl-proxy (config-ssl-proxy)# virtual ipaddr 207.59.100.20 protocol tcp port 443
ssl-proxy (config-ssl-proxy)#
```

This example shows how to configure the SSL policy for the specified virtual server:

```
ssl-proxy (config-ssl-proxy)# virtual policy ssl sslpl1
ssl-proxy (config-ssl-proxy)#
```

This example shows how to configure the TCP policy for the specified virtual server:

```
ssl-proxy (config-ssl-proxy)# virtual policy tcp tcppl1
ssl-proxy (config-ssl-proxy)#
```

This example shows how to configure a clear-text web server for the SSL Services Module to forward the decrypted traffic:

```
ssl-proxy (config-ssl-proxy)# server ipaddr 207.50.0.50 protocol tcp port 80
ssl-proxy (config-ssl-proxy)#
```

This example shows how to configure a TCP policy for the given clear-text web server:

```
ssl-proxy (config-ssl-proxy)# server policy tcp tcppl1
ssl-proxy (config-ssl-proxy)#
```

This example shows how to configure a NAT pool for the client address that is used in the server connection of the specified service SSL offload:

```
ssl-proxy (config-ssl-proxy)# nat client NP1
ssl-proxy (config-ssl-proxy)#
```

This example shows how to enable a NAT server address for the server connection of the specified service SSL offload:

```
ssl-proxy (config-ssl-proxy)# nat server
ssl-proxy (config-ssl-proxy)#
```

Related Commands

show ssl-proxy service

ssl-proxy ssl ratelimit

To prohibit new connections during overload conditions, use the **ssl-proxyy ssl ratelimit** command. Use the **no** form of this command to allow new connections if memory is available.

ssl-proxyy ssl ratelimit

no ssl-proxyy ssl ratelimit

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS Release 12.1(13)E and SSL Services Module Release 1.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.

Examples

This example shows how to prohibit new connections during overload conditions:

```
ssl-proxy (config)# ssl-proxy ssl ratelimit
ssl-proxy (config)#
```

This example shows how to allow new connections during overload conditions if memory is available:

```
ssl-proxy (config)# no ssl-proxy ssl ratelimit
ssl-proxy (config)#
```

ssl-proxy vlan

To enter the proxy-VLAN configuration submode, use the **ssl-proxy vlan** command. In proxy-VLAN configuration submode, you can configure a VLAN for the SSL Services Module.

ssl-proxy vlan *vlan*

Syntax Description

vlan	VLAN ID; valid values are from 1 to 1005.

Defaults

The defaults are as follows:

- *hellotim* is 3 seconds.
- *holdtime* is 10 seconds.
- *priority* is 100.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS Release 12.1(13)E and SSL Services Module Release 1.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.
SSL Services Module Release 2.1(1)	This command was changed to include the **standby** keyword and arguments to configure HSRP.

Usage Guidelines

VLAN 1 is not supported by the CSM.

Extended-range VLANs are not supported by the SSL Services Module.

Enter each proxy-VLAN configuration submode command on its own line.

Table 2-9 lists the commands that are available in proxy-VLAN configuration submode.

Table 2-9 Proxy-VLAN Configuration Submode Command Descriptions

Syntax	Description
admin	Configures the VLAN as an administration VLAN.
exit	Exits from the proxy-VLAN configuration submode.
gateway *prefix* [**drop** | **forward**]	Configures the VLAN with a gateway to the Internet.
help	Provides a description of the interactive help system.
ipaddr *prefix mask*	Configures the VLAN with an IP address and a subnet mask.
no	Negates a command or sets its defaults.

Table 2-9 Proxy-VLAN Configuration Submode Command Descriptions (continued)

Syntax	Description
route {*prefix mask*} {**gateway** *prefix*}	Configures a gateway so that the SSL Services Module can reach a nondirect connected subnetwork.
standby [*group-number*] {**authentication text** *string*} | {**delay minimum** [*min-delay*] **reload** [*reload-delay*]} | {**ip** [*ip-address* [**secondary**]]} | {**mac-address** *mac-address*} | {**mac-refresh** *seconds*} | {**name** *group-name*} | {**preempt** [**delay**{**minimum** *delay* | **reload** *delay* | **sync** *delay*}]} | {**priority** *priority*} | {**redirects** [**enable** | **disable**] [**timers** *advertisement holddown*] [**unknown**]} | {**timers** [**msec**] *hellotime* [**msec**] *holdtime*} | {**track** *object-number* [**decrement** *priority*]}	Configures redundancy on the VLAN. See the following commands for valid values: • **standby authentication** • **standby delay minimum reload** • **standby ip** • **standby mac-address** • **standby mac-refresh** • **standby name** • **standby preempt** • **standby priority** • **standby redirects** • **standby timers** • **standby track** • **standby use-bia**

You must remove the administration VLAN status of the current administration VLAN before you can configure a different administration VLAN.

An administration VLAN is used for communication with the certificate agent (PKI) and the management station (SNMP).

When configuring the gateway, the **drop** keyword allows the SSL Services Module to drop a packet if a virtual service cannot be found relating to the packet.

When configuring the gateway, the **forward** keyword allows the SSL Services Module to forward a packet to the gateway of the specified VLAN if a virtual service cannot be found relating to the packet.

The valid values for configuring HSRP are as follows:

- *group-number*—(Optional) Group number on the interface for which HSRP is being activated; valid values are from 0 to 255. If you do not specify a *group-number*, group **0** is used.
- **ip** *ip-addr*—Specifies the IP address of the HSRP interface.
- **priority** *priority*— Specifies the priority for the HSRP interface. Increase the priority of at least one interface in the HSRP group. The interface with the highest priority becomes active for that HSRP group.
- **prempt** —Enables preemption. When you enable preemption, if the local router has a hot standby priority that is higher than the current active router, the local router attempts to assume control as the active router. If you do not configure preemption, the local router assumes control as the active router only if it receives information indicating that no router is in the active state (acting as the designated router).

- **delay**—(Optional) Specifies the preemption delay. When a router first comes up, it does not have a complete routing table. If it is configured to preempt, it becomes the active router but cannot provide adequate routing services. You can configure a delay before the preempting router actually preempts the currently active router.
- *type time*—Specifies the preemption type and delay; valid values are as follows:
  - **minimum** *time*—Specifies the minimum delay period in delay seconds; valid values are from 0 to 3600 seconds (1 hour).
  - **reload** *time*—Specifies the preemption delay after a reload only.
  - **sync** *time*—Specifies the maximum synchronization period in delay seconds.
- **timers** [**msec**] *hellotime holdtime*—Configures the time between hello packets and the time before other routers declare the active hot standby or standby router to be down; valid values are as follows:
  - **msec**—(Optional) Interval in milliseconds. Millisecond timers allow for faster failover.
  - *hellotime*—Hello interval (in seconds); valid values are from 1 to 254 seconds. If you specify the **msec** keyword, the hello interval is in milliseconds; valid values are from 15 to 999 milliseconds. The default is 3 seconds.
  - *holdtime*—Time (in seconds) before the active or standby router is declared to be down; valid values are from x to 255. If you specify the **msec** keyword, the holdtime is in milliseconds; valid values are from y to 3000 milliseconds. The default is 10 seconds.

    Where:

    x is the *hellotime* plus 50 milliseconds and is rounded up to the nearest 1 second.

    y is greater than or equal to 3 times the *hellotime* and is not less than 50 milliseconds.

Examples

This example shows how to enter the proxy-VLAN configuration submode:

```
ssl-proxy (config)# ssl-proxy vlan 6
ssl-proxy (config-vlan)#
```

These examples show how to set a specified command to its default value:

```
ssl-proxy (config-vlan)# default admin
ssl-proxy (config-vlan)# default gateway
ssl-proxy (config-vlan)# default ipaddr
ssl-proxy (config-vlan)# default route
```

This example shows how to configure the specified VLAN with a gateway:

```
ssl-proxy (config-vlan)# gateway 209.0.207.5
ssl-proxy (config-vlan)#
```

This example shows how to configure the specified VLAN with an IP address and subnet mask:

```
ssl-proxy (config-vlan)# ipaddr 208.59.100.18 255.0.0.0
ssl-proxy (config-vlan)#
```

This example shows how to configure a gateway for the SSL Services Module to reach a nondirect subnetwork:

```
ssl-proxy (config-vlan)# route 210.0.207.0 255.0.0.0 gateway 209.0.207.6
ssl-proxy (config-vlan)#
```

This example shows how to configure the HSRP on the SSL module:

```
ssl-proxy(config)# ssl-proxy vlan 100
ssl-proxy(config-vlan)# ipaddr 10.1.0.20 255.255.255.0
```

```
ssl-proxy(config-vlan)# gateway 10.1.0.1
ssl-proxy(config-vlan)# admin
ssl-proxy(config-vlan)# standby 1 ip 10.1.0.21
ssl-proxy(config-vlan)# standby 1 priority 110
ssl-proxy(config-vlan)# standby 1 preempt
ssl-proxy(config-vlan)# standby 2 ip 10.1.0.22
ssl-proxy(config-vlan)# standby 2 priority 100
ssl-proxy(config-vlan)# standby 2 preempt
ssl-proxy(config-vlan)# end
ssl-proxy#
```

Related Commands

show ssl-proxy vlan

standby authentication

To configure an authentication string for HSRP, use the **standby authentication** command. Use the **no** form of this command to delete an authentication string.

standby [*group-number*] **authentication text** *string*

no standby [*group-number*] **authentication text** *string*

Syntax Description

group-number	(Optional) Group number on the interface to which this authentication string applies.
text *string*	Authentication string, which can be up to eight characters.

Defaults

The defaults are as follows:

- *group-number* is **0**.
- *string* is **cisco**.

Command Modes

Proxy-VLAN configuration submode

Command History

Release	Modification
SSL Services Module Release 2.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.

Usage Guidelines

HSRP ignores unauthenticated HSRP messages.

The authentication string is sent unencrypted in all HSRP messages. You must configure the same authentication string on all routers and access servers on a cable to ensure interoperation. Authentication mismatch prevents a device from learning the designated hot standby IP address and the hot standby timer values from the other routers that are configured with HSRP.

When you use group number 0, no group number is written to NVRAM, providing backward compatibility.

Examples

This example shows how to configure “word” as the authentication string to allow hot standby routers in group 1 to interoperate:

```
ssl-proxy (config-vlan)# standby 1 authentication text word
ssl-proxy (config-vlan)#
```

standby delay minimum reload

To configure a delay before the HSRP groups are initialized, use the **standby delay minimum reload** command. Use the **no** form of this command to disable the delay.

standby delay minimum [*min-delay*] **reload** [*reload-delay*]

no standby delay minimum [*min-delay*] **reload** [*reload-delay*]

Syntax Description

min-delay	(Optional) Minimum time (in seconds) to delay HSRP group initialization after an interface comes up; valid values are from ____ to ____ seconds.
reload-delay	(Optional) Time (in seconds) to delay after the router has reloaded; valid values are from ____ to ____ seconds.

Defaults

The defaults are as follows:

- *min-delay* is **1** second.
- *reload-delay* is **5** seconds.

Command Modes

Proxy-VLAN configuration submode

Command History

Release	Modification
SSL Services Module Release 2.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.

Usage Guidelines

The *min-delay* applies to all subsequent interface events.

The *reload-delay* applies only to the first interface-up event after the router has reloaded.

If the active router fails or you remove it from the network, the standby router automatically becomes the new active router. If the former active router comes back online, you can control whether it takes over as the active router by using the **standby preempt** command.

However, in some cases, even if you do not use the **standby preempt** command, the former active router resumes the active role after it reloads and comes back online. Use the **standby delay minimum reload** command to set a delay for HSRP group initialization. This command allows time for the packets to get through before the router resumes the active role.

We recommend that you use the **standby delay minimum reload** command if the **standby timers** command is configured in milliseconds or if HSRP is configured on a VLAN interface of a switch.

In most configurations, the default values provide sufficient time for the packets to get through and configuring longer delay values is not necessary.

The delay is canceled if an HSRP packet is received on an interface.

Examples

This example shows how to set the minimum delay to 30 seconds and the delay after the first reload to 120 seconds:

```
ssl-proxy (config-vlan)# standby delay minimum 30 reload 120
ssl-proxy (config-vlan)#
```

Related Commands

show standby delay
standby preempt
standby timers

standby ip

To activate HSRP, use the **standby ip** command. Use the **no** form of this command to disable HSRP.

standby [*group-number*] **ip** [*ip-address* [**secondary**]]

no standby [*group-number*] **ip** [*ip-address*]

Syntax Description

group-number	(Optional) Group number on the interface for which HSRP is being activated.
ip-address	(Optional) IP address of the hot standby router interface.
secondary	(Optional) Indicates the IP address is a secondary hot standby router interface.

Defaults

The defaults are as follows:

- *group-number* is 0.
- HSRP is disabled by default.

Command Modes

Proxy-VLAN configuration submode

Command History

Release	Modification
SSL Services Module Release 2.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.

Usage Guidelines

The **standby ip** command allows you to configure primary and secondary HSRP addresses.

The **standby ip** command activates HSRP on the configured interface. If you specify an IP address, that address is used as the designated address for the hot standby group. If you do not specifiy an IP address, the designated address is learned through the standby function. So that HSRP can elect a designated router, at least one router on the cable must have been configured with, or have learned, the designated address. Configuring the designated address on the active router always overrides a designated address that is currently in use.

When you enable the **standby ip** command on an interface, the handling of proxy ARP requests is changed (unless proxy ARP was disabled). If the hot standby state of the interface is active, proxy ARP requests are answered using the MAC address of the hot standby group. If the interface is in a different state, proxy ARP responses are suppressed.

When you use group number 0, no group number is written to NVRAM, providing backward compatibility.

Examples

This example shows how to activate HSRP for group 1 on Ethernet interface 0. The IP address that is used by the hot standby group is learned using HSRP.

```
ssl-proxy (config-vlan)# standby 1 ip
ssl-proxy (config-vlan)#
```

This example shows how to indicate that the IP address is a secondary hot standby router interface:

```
ssl-proxy (config-vlan)# standby ip 1.1.1.254
ssl-proxy (config-vlan)# standby ip 1.2.2.254 secondary
ssl-proxy (config-vlan)# standby ip 1.3.3.254 secondary
```

standby mac-address

To specify a virtual MAC address for HSRP, use the **standby mac-address** command. Use the **no** form of this command to revert to the standard virtual MAC address (0000.0C07.AC*xy)*.

standby [*group-number*] **mac-address** *mac-address*

no standby [*group-number*] **mac-address**

Syntax Description

group-number	(Optional) Group number on the interface for which HSRP is being activated. The default is 0.
mac-address	MAC address.

Defaults

If this command is not configured, and the **standby use-bia** command is not configured, the standard virtual MAC address is used: 0000.0C07.AC*xy*, where *xy* is the group number in hexadecimal. This address is specified in RFC 2281, *Cisco Hot Standby Router Protocol (HSRP)*.

Command Modes

Proxy-VLAN configuration submode

Command History

Release	Modification
SSL Services Module Release 2.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.

Usage Guidelines

This command cannot be used on a Token Ring interface.

You can use HSRP to help end stations locate the first-hop gateway for IP routing. The end stations are configured with a default gateway. However, HSRP can provide first-hop redundancy for other protocols. Some protocols, such as Advanced Peer-to-Peer Networking (APPN), use the MAC address to identify the first hop for routing purposes. In this case, it is often necessary to be able to specify the virtual MAC address; the virtual IP address is unimportant for these protocols. Use the **standby mac-address** command to specify the virtual MAC address.

The specified MAC address is used as the virtual MAC address when the router is active.

This command is intended for certain APPN configurations. The parallel terms are shown in Table 2-10.

Table 2-10 Parallel Terms Between APPN and IP

APPN	IP
End node	Host
Network node	Router or gateway

In an APPN network, an end node is typically configured with the MAC address of the adjacent network node. Use the **standby mac-address** command in the routers to set the virtual MAC address to the value that is used in the end nodes.

Examples

This example shows how to configure HSRP group 1 with the virtual MAC address:

```
ssl-proxy (config-vlan)# standby 1 mac-address 4000.1000.1060
ssl-proxy (config-vlan)#
```

Related Commands

show standby
standby use-bia

standby mac-refresh

To change the interval at which packets are sent to refresh the MAC cache when HSRP is running over FDDI, use the **standby mac-refresh** command. Use the **no** form of this command to restore the default value.

standby mac-refresh *seconds*

no standby mac-refresh

Syntax Description

seconds	Number of seconds in the interval at which a packet is sent to refresh the MAC cache; valid values are from 1 to 255 seconds.

Defaults

seconds is **10** seconds.

Command Modes

Proxy-VLAN configuration submode

Command History

Release	Modification
SSL Services Module Release 2.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.

Usage Guidelines

This command applies to HSRP running over FDDI only. Packets are sent every 10 seconds to refresh the MAC cache on learning bridges or switches. By default, the MAC cache entries age out in 300 seconds (5 minutes).

All other routers participating in HSRP on the FDDI ring receive the refresh packets, although the packets are intended only for the learning bridge or switch. Use this command to change the interval. Set the interval to 0 if you want to prevent refresh packets (if you have FDDI but do not have a learning bridge or switch).

Examples

This example shows how to change the MAC-refresh interval to 100 seconds. In this example, a learning bridge needs to miss three packets before the entry ages out.

```
ssl-proxy (config-vlan)# standby mac-refresh 100
ssl-proxy (config-vlan)#
```

standby name

To configure the name of the standby group, use the **standby name** command. Use the **no** form of this command to disable the name.

standby name *group-name*

no standby name *group-name*

Syntax Description

group-name	Specifies the name of the standby group.

Defaults

HSRP is disabled.

Command Modes

Proxy-VLAN configuration submode

Command History

Release	Modification
SSL Services Module Release 2.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.

Usage Guidelines

The *group-name* argument specifies the HSRP group.

Examples

This example shows how to specifiy the standby name as SanJoseHA:

```
ssl-proxy (config-vlan)# standby name SanJoseHA
ssl-proxy (config-vlan)#
```

Related Commands

ip mobile home-agent redundancy (refer to the *Cisco IOS Release 12.2 Command Reference)*

standby preempt

To configure HSRP preemption and preemption delay, use the **standby preempt** command. Use the **no** form of this command to restore the default values.

standby [*group-number*] **preempt** [**delay**{**minimum** *delay* | **reload** *delay* | **sync** *delay*}]

no standby [*group-number*] **preempt** [**delay**{**minimum** *delay* | **reload** *delay* | **sync** *delay*}]

Syntax Description

group-number	(Optional) Group number on the interface to which the other arguments in this command apply.
delay	(Optional) Required if either the **minimum**, **reload**, or **sync** keywords are specified.
minimum *delay*	(Optional) Specifies the minimum delay in *delay* seconds; valid values are from 0 to 3600 seconds (1 hour).
reload *delay*	(Optional) Specifies the preemption delay after a reload only.
sync *delay*	(Optional) Specifies the maximum synchronization period in *delay* seconds.

Defaults

The defaults are as follows:

- *group-number* is 0.
- *delay* is 0 seconds; the router preempts immediately. By default, the router that comes up later becomes the standby router.

Command Modes

Proxy-VLAN configuration submode

Command History

Release	Modification
SSL Services Module Release 2.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.

Usage Guidelines

The *delay* argument causes the local router to postpone taking over the active role for *delay* (minimum) seconds since that router was last restarted.

When you use this command, the router is configured to preempt, which means that when the local router has a hot standby priority that is higher than the current active router, the local router should attempt to assume control as the active router. If you do not configure preemption, the local router assumes control as the active router only if it receives information indicating no router is in the active state (acting as the designated router).

When a router first comes up, it does not have a complete routing table. If you configure the router to preempt, it becomes the active router, but it cannot provide adequate routing services. You can configure a delay before the preempting router actually preempts the currently active router.

When you use group number 0, no group number is written to NVRAM, providing backward compatibility.

IP-redundancy clients can prevent preemption from taking place. The **standby preempt delay sync** *delay* command specifies a maximum number of seconds to allow IP-redundancy clients to prevent preemption. When this expires, preemption takes place regardless of the state of the IP-redundancy clients.

The **standby preempt delay reload** *delay* command allows preemption to occur only after a router reloads. This provides stabilization of the router at startup. After this initial delay at startup, the operation returns to the default behavior.

The **no standby preempt delay** command disables the preemption delay but preemption remains enabled. The **no standby preempt delay minimum** *delay* command disables the minimum delay but leaves any synchronization delay if it was configured.

Examples

This example shows how to configure the router to wait for 300 seconds (5 minutes) before attempting to become the active router:

```
ssl-proxy (config-vlan)# standby preempt delay minimum 300
ssl-proxy (config-vlan)#
```

standby priority

To configure the priority for HSRP, use the **standby priority** command. Use the **no** form of this command to restore the default values.

standby [*group-number*] **priority** *priority*

no standby [*group-number*] **priority** *priority*

Syntax Description

group-number	(Optional) Group number on the interface to which the other arguments in this command apply.
priority	Priority value that prioritizes a potential hot standby router; valid values are from 1 to 255, where 1 denotes the lowest priority and 255 denotes the highest priority.

Defaults

The defaults are as follows:

- *group-number* is 0.
- *priority* is 100.

Command Modes

Proxy-VLAN configuration submode

Command History

Release	Modification
SSL Services Module Release 2.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.

Usage Guidelines

The router in the HSRP group with the highest priority value becomes the active router.

When you use group number 0, no group number is written to NVRAM, providing backward compatibility.

The assigned priority is used to help select the active and standby routers. Assuming that preemption is enabled, the router with the highest priority becomes the designated active router. In case of ties, the primary IP addresses are compared, and the higher IP address has priority.

The priority of the device can change dynamically if an interface is configured with the **standby track** command and another interface on the router goes down.

Examples

This example shows how to change the router priority:

```
ssl-proxy (config-vlan)# standby priority 120
ssl-proxy (config-vlan)#
```

Examples

standby track

standby redirects

To enable HSRP filtering of Internet Control Message Protocol (ICMP) redirect messages, use the **standby redirects** command. Use the **no** form of this command to disable the HSRP filtering of ICMP redirect messages.

standby redirects [**enable** | **disable**] [**timers** *advertisement holddown*] [**unknown**]

no standby redirects [**unknown**]

Syntax Description

enable	(Optional) Allows the filtering of ICMP redirect messages on interfaces that are configured with HSRP, where the next-hop IP address may be changed to an HSRP virtual IP address.
disable	(Optional) Disables the filtering of ICMP redirect messages on interfaces that are configured with HSRP.
timers	(Optional) Adjusts HSRP-router advertisement timers.
advertisement	(Optional) HSRP-router advertisement interval in seconds; valid values are from 10 to 180 seconds.
holddown	(Optional) HSRP-router holddown interval in seconds; valid values are from 61 to 3600.
unknown	(Optional) Allows sending of ICMP packets to be sent when the next-hop IP address that is contained in the packet is unknown in the HSRP table of real IP addresses and active virtual IP addresses.

Defaults

The defaults are as follows:

- HSRP filtering of ICMP redirect messages is enabled if you configure HSRP on an interface.
- *advertisement* is 60 seconds.
- *holddown* is 180 seconds.

Command Modes

Proxy-VLAN configuration submode

Command History

Release	Modification
SSL Services Module Release 2.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.

Usage Guidelines

You can configure the **standby redirects** command globally or on a per-interface basis. When you first configure HSRP on an interface, the setting for that interface inherits the global value. If you explicitly disable the filtering of ICMP redirects on an interface, then the global command cannot reenable this functionality.

The **no standby redirects** command is the same as the **standby redirects disable** command. We do not recommend that you save the **no** form of this command to NVRAM. Because the command is enabled by default, we recommend that you use the **standby redirects disable** command to disable the functionality.

With the **standby redirects** command enabled, the real IP address of a router can be replaced with a virtual IP address in the next-hop address or gateway field of the redirect packet. HSRP looks up the next-hop IP address in its table of real IP addresses versus virtual IP addresses. If HSRP does not find a match, the HSRP router allows the redirect packet to go out unchanged. The host HSRP router is redirected to a router that is unknown, that is, a router with no active HSRP groups. You can specify the **no standby redirects unknown** command to stop these redirects from being sent.

Examples

This example shows how to allow HSRP to filter ICMP redirect messages:

```
ssl-proxy (config-vlan)# standby redirects
ssl-proxy (config-vlan)#
```

This example shows how to change the HSRP router advertisement interval to 90 seconds and the holddown timer to 270 seconds on interface Ethernet 0:

```
ssl-proxy (config-vlan)# standby redirects timers 90 270
ssl-proxy (config-vlan)#
```

Related Commands

show standby
show standby redirect

standby timers

To configure the time between hello packets and the time before other routers declare the active hot standby or standby router to be down, use the **standby timers** command. Use the **no** form of this command to return to the default settings.

standby [*group-number*] **timers** [**msec**] *hellotime* [**msec**] *holdtime*

no standby [*group-number*] **timers** [**msec**] *hellotime* [**msec**] *holdtime*

Syntax Description

group-number	(Optional) Group number on the interface to which the timers apply.
msec	(Optional) Interval in milliseconds.
hellotime	Hello interval (in seconds); see the "Usage Guidelines" section for valid values.
holdtime	Time (in seconds) before the active or standby router is declared to be down; see the "Usage Guidelines" section for valid values.

Defaults

The defaults are as follows:

- *group-number* is 0.
- *hellotime* is 3 seconds.
- *holdtime* is 10 seconds.

Command Modes

Proxy-VLAN configuration submode

Command History

Release	Modification
SSL Services Module Release 2.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.

Usage Guidelines

The valid values for *hellotime* are as follows:

- If you did not enter the **msec** keyword, valid values are from 1 to 254 seconds.
- If you enter the **msec** keyword, valid values are from 15 to 999 milliseconds.

The valid values for *holdtime* are as follows:

- If you did not enter the **msec** keyword, valid values are from *x* to 255 seconds, where *x* is the *hellotime* and 50 milliseconds and is rounded up to the nearest 1 second.
- If you enter the **msec** keyword, valid values are from *y* to 3000 milliseconds, where *y* is greater than or equal to 3 times the *hellotime* and is not less than 50 milliseconds.

If you specify the **msec** keyword, the hello interval is in milliseconds. Millisecond timers allow for faster failover.

The **standby timers** command configures the time between standby hello packets and the time before other routers declare the active or standby router to be down. Routers or access servers on which timer values are not configured can learn timer values from the active or standby router. The timers configured on the active router always override any other timer settings. All routers in a Hot Standby group should use the same timer values. Normally, holdtime is greater than or equal to 3 times the value of hellotime. The range of values for holdtime force the holdtime to be greater than the hellotime. If the timer values are specified in milliseconds, the holdtime is required to be at least three times the hellotime value and not less than 50 milliseconds.

Some HSRP state flapping can occasionally occur if the holdtime is set to less than 250 milliseconds, and the processor is busy. It is recommended that holdtime values less than 250 milliseconds be used on Cisco 7200 platforms or better, and on Fast-Ethernet or FDDI interfaces or better. Setting the **process-max-time** command to a suitable value may also help with flapping.

The value of the standby timer will not be learned through HSRP hellos if it is less than 1 second.

When group number 0 is used, no group number is written to NVRAM, providing backward compatibility.

Examples

This example sets, for group number 1 on Ethernet interface 0, the time between hello packets to 5 seconds, and the time after which a router is considered to be down to 15 seconds:

```
interface ethernet 0
 standby 1 ip
 standby 1 timers 5 15
```

This example sets, for the hot router interface that is located at 172.19.10.1 on Ethernet interface 0, the time between hello packets to 300 milliseconds, and the time after which a router is considered to be down to 900 milliseconds:

```
interface ethernet 0
 standby ip 172.19.10.1
 standby timers msec 300 msec 900
```

This example sets, for the hot router interface that is located at 172.18.10.1 on Ethernet interface 0, the time between hello packets to 15 milliseconds, and the time after which a router is considered to be down to 50 milliseconds. Note that the holdtime is three times larger than the hellotime because the minimum holdtime value in milliseconds is 50.

```
interface ethernet 0
 standby ip 172.18.10.1
 standby timers msec 15 msec 50
```

standby track

To configure HSRP to track an object and change the hot standby priority based on the state of the object, use the **standby track** command. Use the **no** form of this command to remove the tracking.

standby [*group-number*] **track** *object-number* [**decrement** *priority*]

no standby [*group-number*] **track** *object-number* [**decrement** *priority*]

Syntax Description

group-number	(Optional) Group number to which the tracking applies.
object-number	Object number in the range from 1 to 500 representing the object to be tracked.
decrement *priority*	(Optional) Amount by which the hot standby priority for the router is decremented (or incremented) when the tracked object goes down (or comes back up).
group-number	(Optional) Group number on the interface to which the tracking applies.

Defaults

The defaults are as follows:

- *group-number* is **0**.
- *priority* is **10**.

Command Modes

Proxy-VLAN configuration submode

Command History

Release	Modification
SSL Services Module Release 2.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.

Usage Guidelines

This command ties the hot standby priority of the router to the availability of its tracked objects. Use the **track interface** or **track ip route** global configuration command to track an interface object or an IP route object. The HSRP client can register its interest in the tracking process by using the **standby track** command commands and take action when the object changes.

When a tracked object goes down, the priority decreases by 10. If an object is not tracked, its state changes do not affect the priority. For each object configured for hot standby, you can configure a separate list of objects to be tracked.

The optional *priority* argument specifies how much to decrement the hot standby priority when a tracked object goes down. When the tracked object comes back up, the priority is incremented by the same amount.

When multiple tracked objects are down, the decrements are cumulative, whether configured with *priority* values or not.

Use the **no standby** *group-number* **track** command to delete all tracking configuration for a group.

When you use group number 0, no group number is written to NVRAM, providing backward compatibility.

The **standby track** command syntax prior to Release 12.2(15)T is still supported. Using the older form will cause a tracked object to be created in the new tracking process. This tracking information can be displayed using the **show track** command.

Examples

This example shows how to track the IP routing capability of serial interface 1/0. HSRP on Ethernet interface 0/0 registers with the tracking process to be informed of any changes to the IP routing state of serial interface 1/0. If the IP state on Serial interface 1/0 goes down, the priority of the HSRP group is reduced by 10.

If both serial interfaces are operational, Router A becomes the HSRP active router because it has the higher priority.

However, if IP routing on serial interface 1/0 in Router A fails, the HSRP group priority is reduced and Router B takes over as the active router, thus maintaining a default virtual gateway service to hosts on the 10.1.0.0 subnet.

Router A Configuration

```
!
track 100 interface serial1/0 ip routing
!
interface Ethernet0/0
  ip address 10.1.0.21 255.255.0.0
  standby 1 ip 10.1.0.1
  standby 1 priority 105
  standby 1 track 100 decrement 10
```

Router B Configuration

```
!
track 100 interface serial1/0 ip routing
!
interface Ethernet0/0
  ip address 10.1.0.22 255.255.0.0
  standby 1 ip 10.1.0.1
  standby 1 priority 100
  standby 1 track 100 decrement 10
```

Related Commands

standby preempt
standby priority

standby use-bia

To configure HSRP to use the burned-in address of the interface as its virtual MAC address instead of the preassigned MAC address (on Ethernet and FDDI) or the functional address (on Token Ring), use the **standby use-bia** command. Use the **no** form of this command to restore the default virtual MAC address.

standby use-bia [**scope interface**]

no standby use-bia

Syntax Description

scope interface	(Optional) Specifies that this command is configured only for the subinterface on which it was entered, instead of the major interface.

Defaults

HSRP uses the preassigned MAC address on Ethernet and FDDI or the functional address on Token Ring.

Command Modes

Proxy-VLAN configuration submode

Command History

Release	Modification
SSL Services Module Release 2.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.

Usage Guidelines

You can configure multiple standby groups on an interface when you enter the **standby use-bia** command. Hosts on the interface must have a default gateway configured. We recommend that you set the **no ip proxy-arp** command on the interface. We also recommend that you configure the **standby use-bia** command on a Token Ring interface if there are devices that reject ARP replies with source hardware addresses that are set to a functional address.

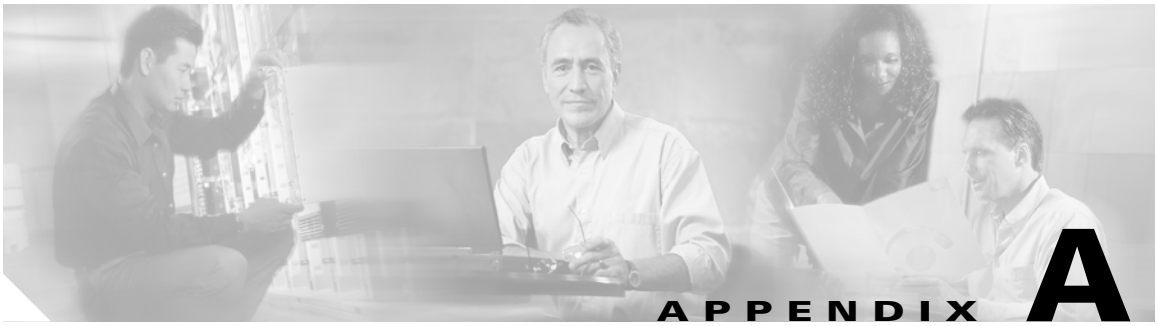
When HSRP runs on a multiple-ring, source-routed bridging environment and the HRSP routers reside on different rings, configuring the **standby use-bia** command can prevent confusion about the routing information field (RFI).

Without the **scope interface** keywords, the **standby use-bia** command applies to all subinterfaces on the major interface. You cannot enter the **standby use-bia** command both with and without the **scope interface** keywords at the same time.

Examples

This example shows how to map the virtual MAC address to the virtual IP address:

```
ssl-proxy (config-vlan)# standby use-bia
ssl-proxy (config-vlan)#
```



Acronyms

Table A-1 defines the acronyms that are used in this publication.

Table A-1 List of Acronyms

Acronym	Expansion
AAL	ATM adaptation layer
ACE	access control entry
ACL	access control list
ACNS	Application and Content Networking System
AFI	authority and format identifier
Agport	aggregation port
ALPS	Airline Protocol Support
AMP	Active Monitor Present
APaRT	Automated Packet Recognition and Translation
ARP	Address Resolution Protocol
ATA	Analog Telephone Adaptor
ATM	Asynchronous Transfer Mode
AV	attribute value
BDD	binary decision diagrams
BECN	backward explicit congestion notification
BGP	Border Gateway Protocol
Bidir	bidirectional PIM
BPDU	bridge protocol data unit
BRF	bridge relay function
BSC	Bisync
BSTUN	Block Serial Tunnel
BUS	broadcast and unknown server
BVI	bridge-group virtual interface
CAM	content-addressable memory
CAR	committed access rate

Table A-1 List of Acronyms (continued)

Acronym	Expansion
CBAC	context based access control
CCA	circuit card assembly
CDP	Cisco Discovery Protocol
CEF	Cisco Express Forwarding
CHAP	Challenge Handshake Authentication Protocol
CIR	committed information rate
CIST	Common and Internal Spanning Tree
CLI	command-line interface
CLNS	Connection-Less Network Service
CMNS	Connection-Mode Network Service
CNS	Cisco Networking Services
COPS	Common Open Policy Server
COPS-DS	Common Open Policy Server Differentiated Services
CoS	class of service
CPLD	Complex Programmable Logic Device
CRC	cyclic redundancy check
CRF	concentrator relay function
CSM	Content Switching Module
CST	Common Spanning Tree
CUDD	University of Colorado Decision Diagram
DCC	Data Country Code
dCEF	distributed Cisco Express Forwarding
DDR	dial-on-demand routing
DE	discard eligibility
DEC	Digital Equipment Corporation
DF	designated forwarder
DFC	Distributed Forwarding Card
DFI	Domain-Specific Part Format Identifier
DFP	Dynamic Feedback Protocol
DISL	Dynamic Inter-Switch Link
DLC	Data Link Control
DLSw	Data Link Switching
DMP	data movement processor
DNS	Domain Name System
DoD	Department of Defense
DoS	denial of service

Table A-1 List of Acronyms (continued)

Acronym	Expansion
dot1q	802.1Q
dot1x	802.1x
DRAM	dynamic RAM
DRiP	Dual Ring Protocol
DSAP	destination service access point
DSCP	differentiated services code point
DSPU	downstream SNA Physical Units
DTP	Dynamic Trunking Protocol
DTR	data terminal ready
DXI	data exchange interface
EAP	Extensible Authentication Protocol
EARL	Enhanced Address Recognition Logic
EEPROM	electrically erasable programmable read-only memory
EHSA	enhanced high system availability
EIA	Electronic Industries Association
ELAN	Emulated Local Area Network
EOBC	Ethernet out-of-band channel
EOF	end of file
EoMPLS	Ethernet over Multiprotocol Label Switching
ESI	end-system identifier
FAT	File Allocation Table
FIB	Forwarding Information Base
FIE	Feature Interaction Engine
FECN	forward explicit congestion notification
FM	feature manager
FRU	field replaceable unit
fsck	file system consistency check
FSM	feasible successor metrics
FSU	fast software upgrade
FWSM	Firewall Services Module
GARP	General Attribute Registration Protocol
GBIC	Gigabit Interface Converter
GMRP	GARP Multicast Registration Protocol
GVRP	GARP VLAN Registration Protocol
HSRP	Hot Standby Routing Protocol
ICC	Inter-card Communication or interface controller card

Table A-1 List of Acronyms (continued)

Acronym	Expansion
ICD	International Code Designator
ICMP	Internet Control Message Protocol
IDB	interface descriptor block
IDP	initial domain part or Internet Datagram Protocol
IDSM	Intrusion Detection System Module
IFS	IOS File System
IGMP	Internet Group Management Protocol
IGMPv2	IGMP version 2
IGMPv3	IGMP version 3
IGRP	Interior Gateway Routing Protocol
ILMI	Integrated Local Management Interface
IP	Internet Protocol
IPC	interprocessor communication
IPX	Internetwork Packet Exchange
IS-IS	Intermediate System-to-Intermediate System Intradomain Routing Protocol
ISL	Inter-Switch Link
ISL VLANs	Inter-Switch Link VLANs
ISO	International Organization of Standardization
ISR	Integrated SONET router
LACP	Link Aggregation Control Protocol
LACPDU	Link Aggregation Control Protocol data unit
LAN	local area network
LANE	LAN Emulation
LAPB	Link Access Procedure, Balanced
LCP	Link Control Protocol
LDA	Local Director Acceleration
LEC	LAN Emulation Client
LECS	LAN Emulation Configuration Server
LEM	link error monitor
LER	link error rate
LES	LAN Emulation Server
LLC	Logical Link Control
LOU	logical operation units
LTL	Local Target Logic
MAC	Media Access Control

Table A-1 List of Acronyms (continued)

Acronym	Expansion
MD5	message digest 5
MDIX	media-dependent interface crossover
MDSS	Multicast Distributed Shortcut Switching
MFD	multicast fast drop
MIB	Management Information Base
MII	media-independent interface
MLS	Multilayer Switching
MLSE	maintenance loop signaling entity
MLSM	multilayer switching for multicast
MOP	Maintenance Operation Protocol
MOTD	message-of-the-day
MPLS	Multiprotocol Label Switching
MRM	multicast routing monitor
MSDP	Multicast Source Discovery Protocol
MSFC	Multilayer Switching Feature Card
MSM	Multilayer Switch Module
MST	Multiple Spanning Tree (802.1s)
MTU	maximum transmission unit
MVAP	multiple VLAN access port
NAM	Network Analysis Module
NBP	Name Binding Protocol
NCIA	Native Client Interface Architecture
NDE	NetFlow Data Export
NDR	no drop rate
NET	network entity title
NetBIOS	Network Basic Input/Output System
NFFC	NetFlow Feature Card
NMP	Network Management Processor
NSAP	network service access point
NTP	Network Time Protocol
NVGEN	nonvolatile generation
NVRAM	nonvolatile RAM
OAM	Operation, Administration, and Maintenance
ODM	order dependent merge
OIF	Outgoing interface of a multicast {*,G} or {source, group} flow

Table A-1 List of Acronyms (continued)

Acronym	Expansion
OSI	Open System Interconnection
OSM	Optical Services Module
OSPF	open shortest path first
PAE	port access entity
PAgP	Port Aggregation Protocol
PBD	packet buffer daughterboard
PBR	policy-based routing
PC	Personal Computer (formerly PCMCIA)
PCM	pulse code modulation
PCR	peak cell rate
PDP	policy decision point
PDU	protocol data unit
PEP	policy enforcement point
PFC	Policy Feature Card
PGM	Pragmatic General Multicast
PHY	physical sublayer
PIB	policy information base
PIM	protocol independent multicast
PPP	Point-to-Point Protocol
ppsec	packets per second
PRID	Policy Rule Identifiers
PVLANs	private VLANs
PVST+	Per-VLAN Spanning Tree+
QDM	QoS device manager
QM	QoS manager
QM-SP	SP QoS manager
QoS	quality of service
Q-in-Q	802.1Q in 802.1Q
RACL	router interface access control list
RADIUS	Remote Access Dial-In User Service
RAM	random-access memory
RCP	Remote Copy Protocol
RF	Redundancy Facility
RGMP	Router-Ports Group Management Protocol
RIB	routing information base
RIF	Routing Information Field

Table A-1 List of Acronyms (continued)

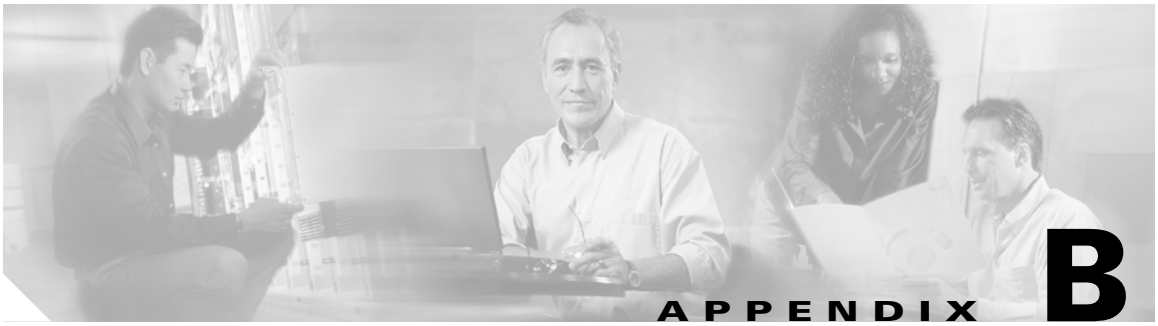
Acronym	Expansion
RMON	remote network monitor
ROM	read-only memory
ROMMON	ROM monitor
RP	route processor or rendezvous point
RPC	remote procedure call
RPF	reverse path forwarding
RPR	Route Processor Redundancy
RPR+	Route Processor Redundancy+
RSPAN	remote SPAN
RST	reset
RSTP	Rapid Spanning Tree Protocol
RSTP+	Rapid Spanning Tree Protocol plus
RSVP	ReSerVation Protocol
SAID	Security Association Identifier
SAP	service access point
SCM	service connection manager
SCP	Switch-Module Configuration Protocol
SDLC	Synchronous Data Link Control
SFP	small form factor pluggable
SGBP	Stack Group Bidding Protocol
SIMM	single in-line memory module
SLB	server load balancing
SLCP	Supervisor Line-Card Processor
SLIP	Serial Line Internet Protocol
SMDS	Software Management and Delivery Systems
SMF	software MAC filter
SMP	Standby Monitor Present
SMRP	Simple Multicast Routing Protocol
SMT	Station Management
SNAP	Subnetwork Access Protocol
SNMP	Simple Network Management Protocol
SPAN	Switched Port Analyzer
SREC	S-Record format, Motorola defined format for ROM contents
SSL	Secure Sockets Layer
SSM	Source Specific Multicast
SSTP	Cisco Shared Spanning Tree

Table A-1 List of Acronyms (continued)

Acronym	Expansion
STP	Spanning Tree Protocol
SVC	switched virtual circuit
SVI	switched virtual interface
TACACS+	Terminal Access Controller Access Control System Plus
TARP	Target Identifier Address Resolution Protocol
TCAM	Ternary Content Addressable Memory
TCL	table contention level
TCP/IP	Transmission Control Protocol/Internet Protocol
TFTP	Trivial File Transfer Protocol
TIA	Telecommunications Industry Association
TopN	Utility that allows the user to analyze port traffic by reports
ToS	type of service
TLV	type-length-value
TTL	Time To Live
TVX	valid transmission
UDLD	UniDirectional Link Detection Protocol
UDP	User Datagram Protocol
UNI	User-Network Interface
UTC	Coordinated Universal Time
VACL	VLAN access control list
VCC	virtual channel circuit
VCI	virtual circuit identifier
VCR	Virtual Configuration Register
VINES	Virtual Network System
VLAN	virtual LAN
VMPS	VLAN Membership Policy Server
VMR	value mask result
VPN	virtual private network
VRF	VPN routing and forwarding
VTP	VLAN Trunking Protocol
VVID	voice VLAN ID
WAN	wide area network
WCCP	Web Cache Coprocessor Protocol
WFQ	weighted fair queueing
WRED	weighted random early detection

Table A-1 List of Acronyms (continued)

Acronym	Expansion
WRR	weighted round-robin
XNS	Xerox Network System



Acknowledgments for Open-Source Software

The Cisco IOS software on the Catalyst 6500 series switches software pipe command uses Henry Spencer's regular expression library (regex).

Henry Spencer's regular expression library (regex). Copyright 1992, 1993, 1994, 1997 Henry Spencer. All rights reserved. This software is not subject to any license of the American Telephone and Telegraph Company or of the Regents of the University of California.

Permission is granted to anyone to use this software for any purpose on any computer system, and to alter it and redistribute it, subject to the following restrictions:

1. The author is not responsible for the consequences of use of this software, no matter how awful, even if they arise from flaws in it.
2. The origin of this software must not be misrepresented, either by explicit claim or by omission. Since few users ever read sources, credits must appear in the documentation.
3. Altered versions must be plainly marked as such, and must not be misrepresented as being the original software. Since few users ever read sources, credits must appear in the documentation.
4. This notice may not be removed or altered.

Symbols

Numerics

A

B

C

D

E

F

G

H

I

L

M

N

O

P

Q

R

S

T

U

V

W