match protocol http cookie (cookie map submode)

To add cookies to a cookie map, use the **match protocol http cookie** command in SLB cookie map configuration submode. Multiple match rules can be added to a cookie map. To remove the cookie map name from the cookie map, use the **no** form of this command.

match protocol http cookie *cookie-name* **cookie-value** *cookie-value-expression*

no match protocol http cookie *cookie-name* **cookie-value** *cookie-value-expression*

Syntax Description

cookie-name	Cookie name; the range is from 1 to 63 characters.
cookie-value *cookie-value-expression*	Specifies a cookie value expression; the range is from 1 to 255 characters.

Defaults

This command has no default settings.

Command Modes

SLB cookie map configuration submode

Usage Guidelines

Cookie regular expressions (see "Regular Expressions" section on page 2-3) are based on the UNIX filename specification. URL expressions are stored in a cookie map in the form *cookie-name* = *cookie-value-expression*. Cookie expressions allow spaces if they are escaped or quoted. You must match all cookies in the cookie map.

Command History

Release	Modification
1.1(1)	This command was introduced.

Examples

This example shows how to add cookies to a cookie map:

```
Cat6k-2(config-slb-map-cookie)# match protocol http cookie albert cookie-value 4*
```

Related Commands

cookie-map (policy submode)
map cookie
show module csm map

map dns

To enter the SLB DNS map mode and configure a DNS map, use the **map dns** command. To remove the DNS map from the configuration, use the **no** form of this command.

map *dns-map-name* **dns**

no map *dns-map-name* **dns**

Syntax Description

dns-map-name	Name of an SLB DNS map; the character string range is from 1 to 15 characters.

Defaults

This command has no default settings.

Command Modes

SLB DNS map configuration submode

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

Any match of a DNS regular expression in the DNS map results in a successful match. A maximum of 1023 DNS domains can be configured to a map.

Examples

This example shows how to group DNS domains:

```
Cat6k-2(config-module-csm)# map m1 dns
Cat6k-2(config-slb-map-dns)# exit
Cat6k-2(config)
```

Related Commands

match protocol dns domain (DNS map submode)
show module csm map

match protocol dns domain (DNS map submode)

To add a DNS domain to a DNS map, use the **match protocol dns domain** command in the SLB DNS map configuration submode. To remove the DNS domain from the URL map, use the **no** form of this command.

match protocol dns domain *name*

no match protocol dns domain *name*

Syntax Description

name	Names the DNS domain being mapped.

Defaults

This command has no default settings.

Command Modes

SLB DNS map configuration submode

Command History

Release	Modification
1.1(1)	This command was introduced.
4.1(1)	HTTP method parsing support was introduced.

Examples

This example shows how to add domains to a DNS map:

```
Cat6k-2(config-slb-map-dns)# match protocol dns domain cisco.com
```

Related Commands

map dns
show module csm map

map header

To create a map group for specifying HTTP headers, and then enter the header map configuration submode, use the **map header** command. To remove the HTTP header group from the configuration, use the **no** form of this command.

map *name* **header**

no map *name*

Syntax Description

name	Map instance; the character string is from 1 to 15 characters.

Defaults

This command has no default settings.

Command Modes

Module CSM configuration submode

Command History

Release	Modification
2.1(1)	This command was introduced.

Examples

This example shows how to group HTTP headers and associate them with a content switching policy:

```
Cat6k-2(config-module-csm)# map upnready header
Cat6k-2(config-slb-map-header)# match protocol http header Accept header-value *jpeg*
Cat6k-2(config-slb-map-header)# match protocol http header User-Agent header-value *NT*
Cat6k-2(config-slb-map-header)# match protocol http header Host header-value
www.myhome.com
Cat6k-2(config-slb-map-header)# exit
```

Related Commands

header-map (policy submode)
insert protocol http header (header map submode)
match protocol http header (header map submode)
show module csm map

insert protocol http header (header map submode)

To insert header fields and values into an HTTP request, use the **insert protocol http header** command in SLB header map configuration submode. To remove the header insert item from the header map, use the **no** form of this command.

insert protocol http header *name* **header-value** *value*

no insert protocol http header *name*

Syntax Description

name	Literal name of the generic field in the HTTP header. The name is a string with a range from 1 to 63 characters.
header-value *value*	Specifies the literal header value string to insert in the request.

Defaults

This command has no default settings.

Command Modes

SLB header map configuration submode

Usage Guidelines

You can also use the %is and %id special parameters for header values. The %is value inserts the source IP into the HTTP header, and the %id value inserts the destination IP into the header. You can only specify each special parameter once per header map.

Command History

Release	Modification
3.1(1)	This command was introduced.

Examples

This example shows how to specify header fields and values to search upon a request:

```
Cat6k-2(config-slb-map-header)# insert protocol http header client header-value %is
```

Related Commands

header-map (policy submode)
map header
show module csm map

match protocol http header (header map submode)

To specify header fields and values for the CSM to search for when receiving a request, use the **match protocol http header** command in SLB header map configuration submode. Multiple match rules can be added to a header map. To remove the header match rule from the header map, use the **no** form of this command.

match protocol http header *field* **header-value** *expression*

no match protocol http header *field*

Syntax Description

field	Literal name of the generic field in the HTTP header. The range is from 1 to 63 characters.
header-value *expression*	Specifies the header value expression string to compare against the value in the specified field; the range is from 1 to 127 characters.

Defaults

This command has no default settings.

Command Modes

SLB header map configuration submode

Usage Guidelines

There are predefined fields, for example, Accept-Language, User-Agent, or Host.

Header regular expressions(see "Regular Expressions" section on page 2-3) are based on the UNIX filename specification. URL expressions are stored in a header map in the form *header-name* = *expression*. Header expressions allow spaces provided that they are escaped or quoted. All headers in the header map must be matched

Command History

Release	Modification
2.1(1)	This command was introduced.

Examples

This example shows how to specify header fields and values to search upon a request:

```
Cat6k-2(config-slb-map-header)# match protocol http header Host header-value XYZ
```

Related Commands

header-map (policy submode)
insert protocol http header (header map submode)
map header
show module csm map

map retcode

To enable return code checking, and then enter the return code map submode, use the **map retcode** command. To remove the return code checking from the configuration, use the **no** form of this command.

map *name* **retcode**

no map *name*

Syntax Description

name	Return error code map instance; the character string is limited to 15 characters.
retcode	Keyword to enter the return error code map submode.

Defaults

This command has no default settings.

Command Modes

CSM module submode

Command History

Release	Modification
2.2(1)	This command was introduced.

Examples

This example shows how to enable return error code checking:

```
Cat6k-2(config-module-csm)# map upnready retcode
```

Related Commands

cookie-map (policy submode)
match protocol http cookie (cookie map submode)
show module csm map

match protocol http retcode (return code map submode)

To specify return code thresholds, count and log return codes, and send syslog messages for return code events received from the servers, use the **match protocol http retcode** command in SLB return code map configuration submode. To remove the return code thresholds, use the **no** form of this command.

match protocol http retcode *min max* **action {count | log | remove}** *threshold* [**reset** *seconds*]

no match protocol http retcode *min max*

Syntax Description

min max	Minimum and maximum range of return codes used to perform a count, log, or remove action.
action count	Increments the statistics of the number of occurrences of return codes received.
action log	Specifies where syslog messages are sent when a threshold is reached.
action remove	Specifies where the syslog messages are sent when a threshold is reached and the server is removed from service.
threshold	The number of return occurrences before the log or remove action is taken.
reset *seconds*	(Optional) Number of seconds to wait before the processing can resume.

Defaults

This command has no default settings.

Command Modes

SLB return code map configuration submode

Usage Guidelines

The *threshold* and **reset** values are not configurable for the **count** action. These commands only are available for the **log** and **remove** actions.

Command History

Release	Modification
2.2(1)	This command was introduced.

Examples

This example shows how to specify return codes values to search for in an HTTP request:

```
Cat6k-2(config-slb-map-retcode)# match protocol http retcode 30 50 action log 400 reset 30
```

Related Commands

map retcode (SLB policy configuration submode)

map url

To enter the SLB URL map mode and configure a URL map, use the **map url** command. To remove the URL map from the configuration, use the **no** form of this command.

map *url-map-name* **url**

no map *url-map-name*

Syntax Description

url-map-name	Name of an SLB URL map; the character string range is from 1 to 15 characters.

Defaults

This command has no default settings.

Command Modes

SLB URL map configuration submode

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

Any match of a URL regular expression in the URL map results in a successful match. A maximum of 1023 URLs can be configured to a map.

Examples

This example shows how to group URLs and associate them with a content switching policy:

```
Cat6k-2(config-module-csm)# map m1 url
Cat6k-2(config-slb-map-url)# match protocol http url /index.html
Cat6k-2(config-slb-map-url)# match protocol http url /stocks/csco/
Cat6k-2(config-slb-map-url)# match protocol http url *gif
Cat6k-2(config-slb-map-url)# match protocol http url /st*
Cat6k-2(config-slb-map-url)# exit
Cat6k-2(config)
```

Related Commands

match protocol http url (URL map submode)
show module csm map
url-map (policy submode)

match protocol http url (URL map submode)

To add a URL regular expression to a URL map, use the **match protocol http url** command in the SLB URL map configuration submode. Multiple match rules can be added to a URL map. To remove the URL regular expression from the URL map, use the **no** form of this command.

match protocol http [method *method-expression*] **url** *url-expression*

no match protocol http [method *method-expression*] **url** *url-expressionn*

Syntax Description

method *method-expression*	(Optional) Specifies the method to match.
url *url-expression*	Specifies the regular expression range; the range is from 1 to 255 characters.

Defaults

This command has no default settings.

Command Modes

SLB URL map configuration submode

Usage Guidelines

URL regular expressions (see "Regular Expressions" section on page 2-3) are based on the UNIX filename specification. URL expressions are stored in a cookie map in the form *urln*. URL expressions do not allow spaces and only one of the URLs in the map must be matched

The method expression can either be one of the standard HTTP 1.1 method names (OPTIONS, GET, HEAD, POST, PUT, DELETE, TRACE, or CONNECT) or a string you specify that must be matched exactly (PROTOPLASM).

Command History

Release	Modification
1.1(1)	This command was introduced.
4.1(1)	HTTP method parsing support was introduced.

Examples

This example shows how to add URL expressions to a URL map:

```
Cat6k-2(config-slb-map-url)# match protocol http url html
```

Related Commands

map url
show module csm map
url-map (policy submode)

module csm

To allow the association of load-balancing commands to a specific CSM module, and then enter the CSM module configuration submode for the specified slot, use the **module csm** command. To remove the **module csm** configuration, use the **no** form of this command.

Note The **module ContentSwitching Module** *slot* command is the full syntax; the **module csm** *slot* command is a valid shortcut.

module csm *slot-number*

no module csm *slot-number*

Syntax Description

slot-number	Slot number where the CSM resides.

Defaults

This command has no default settings.

Command Modes

Global configuration submode

Command History

Release	Modification
2.1(1)	This command was introduced.

Usage Guidelines

If you want to use the multiple module configuration, you must change the **ip slb mode** command to **rp**. An existing CSM configuration is migrated to the new configuration when you change the mode from **csm** to **rp**. The default mode is **rp**, which allows multiple CSM support and allows the Catalyst operating system and Cisco IOS software to run on the same switch.

Migrating from a multiple module configuration to a single module configuration is supported. Migrating the Cisco IOS SLB configuration to the CSM configuration is not supported.

To remove connections to a real server, use the **clear module csm** *X* connnection command.

The CSM had its own ARP cache, which was populated with ARP entries through ARP learning. The addition of the **arp** option allows you to statically configure ARP entries.

Examples

This example shows how to configure a CSM:

```
Cat6k-2(config)# module csm 5
Cat6k-2(config-module-csm)# vserver VS1
```

Related Commands

ip slb mode

natpool (module CSM submode)

To configure source NAT and create a client address pool, use the **natpool** command in module CSM configuration submode. To remove a **natpool** configuration, use the **no** form of this command.

natpool *pool-name start-ip end-ip* {**netmask** *netmask* | **prefix-length** *leading_1_bits*}

no natpool *pool-name*

Syntax Description

pool-name	Name of a client address pool; the character string is from 1 to 15 characters.
start-ip end-ip	Specifies the starting and ending IP address that define the range of addresses in the address pool.
netmask *netmask*	(Optional) Mask for the associated IP subnet.
prefix-length *leading_1_bits*	(Optional) Mask for the associated IP subnet.

Defaults

This command has no default settings.

Command Modes

Module CSM configuration submode

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

If you want to use client NAT, you must create at least one client address pool.

A maximum of 255 NAT pool addresses are available for any CSM.

Examples

This example shows how to configure a pool of addresses with the name **web-clients**, an IP address range from 128.3.0.1 through 128.3.0.254, and a subnet mask of 255.255.0.0:

```
Cat6k-2(config-module-csm)# natpool web-clients 128.3.0.1 128.3.0.254 netmask 255.255.0.0
```

Related Commands

nat client (serverfarm submode)
show module csm natpool

variable (module CSM submode)

To specify the environmental variables in the configuration, use the **variable** command. To remove a environmental variables from the configuration, use the **no** form of this command.

variable *name value*

no variable *name*

Syntax Description

name	Specifies a name string for the variable.
value	Specifies a value string for the variable.

Defaults

This command has no default settings.

Command Modes

Module CSM configuration submode

Command History

Release	Modification
4.1(1)	This command was introduced.

Usage Guidelines

This table lists the environmental values used by the CSM.

Name	Default	Valid Values	Description
ARP_INTERVAL	300	Integer (15 to 31536000)	Time (in seconds) between ARP requests for configured hosts
ARP_LEARNED_INTERVAL	14400	Integer (60 to 31536000)	Time (in seconds) between ARP requests for learned hosts
ARP_GRATUITOUS_INTERVAL	15	Integer (10 to 31536000)	Time (in seconds) between gratuitous ARP requests
ARP_RATE	10	Integer (1 to 60)	Seconds between ARP retries
ARP_RETRIES	3	Integer (2 to 15)	Count of ARP attempts before flagging a host as down
ARP_LEARN_MODE	1	Integer (0 to 1)	Indicates whether the CSM learns MAC addresses on responses only (0) or all traffic (1)
ARP_REPLY_FOR_NO_INSERVICE_VIP	D	0	Integer (0 to 1)
ADVERTISE_RHI_FREQ	10	Integer (1 to 65535)	Frequency (in seconds) that the CSM uses to check for RHI updates

Name	Default	Valid Values	Description
AGGREGATE_BACKUP_SF_STATE_TO_VS	0	Integer (0 to 1)	Specifies whether to include the operational state of a backup server farm into the state of a virtual server
COOKIE_INSERT_EXPIRATION_DATE	Fri, 1 Jan 2010 01:01:50 GMT	String (2 to 63 chars)	Configures the expiration time and date for the HTTP cookie inserted by the CSM
DEST_UNREACHABLE_MASK	65535	Integer (0 to 65535)	Bitmask defining which ICMP destination unreachable codes are to be forwarded
FT_FLOW_REFRESH_INT	60	Integer (1 to 65535)	Interval for the FT slow path flow refresh in seconds
HTTP_CASE_SENSITIVE_MATCHING	1	Integer (0 to 1)	Specifies whether the URL (cookie, header) matching and sticky are to be case sensitive
HTTP_URL_COOKIE_DELIMITERS	/?&#+	String (1 to 64 chars)	Configures the list of delimiter characters for cookies in the URL string
MAX_PARSE_LEN_MULTIPLIER	1	Integer (1 to 16)	Multiplies the configured max-parse-len by this amount
NAT_CLIENT_HASH_SOURCE_PORT	0	Integer (0 to 1)	Specifies whether to use the source port to select the client NAT IP address
ROUTE_UNKNOWN_FLOW_PKTS	0	Integer (0 to 1)	Specifies whether to route non-SYN packets that do not match any existing flows
NO_RESET_UNIDIRECTIONAL_FLOWS	0	Integer (0 to 1)	Specifies, if set, that unidirectional flows do not be reset when timed out
SWITCHOVER_RP_ACTION	0	Integer (0 to 1)	Specifies whether to recover (0) or halt/reboot (1) after a supervisor engine RP switchover occurs
SWITCHOVER_SP_ACTION	0	Integer (0 to 1)	Specifies whether to recover (0) or halt/reboot (1) after a supervisor engine SP switchover occurs
SYN_COOKIE_INTERVAL	3	Integer (1 to 60)	Specifies the interval (in seconds), at which a new syn-cookie key is generated
SYN_COOKIE_THRESHOLD	5000	Integer (0 to 1048576)	Specifies the threshold (in number of pending sessions) at which syn-cookie is engaged
TCP_MSS_OPTION	1460	Integer (1 to 65535)	Specifies the maximum segment size (MSS) value sent by CSM for Layer 7 processing

Name	Default	Valid Values	Description
TCP_WND_SIZE_OPTION	8192	Integer (1 to 65535)	Specifies the window size value sent by CSM for Layer 7 processing
VSERVER_ICMP_ALWAYS_RESPOND	false	String (1 to 5 chars)	If the response is “true,” the CSM responds to ICMP probes regardless of virtual server state
XML_CONFIG_AUTH_TYPE	Basic	String (5 to 6 chars)	Specifies the HTTP authentication type for xml-config: Basic or Digest

Examples

This example shows how to enable the environmental variables configuration:

```
Router(config-module-csm)# variable ARP_RATE 20
```

Related Commands

module csm
show module csm variable

owner

To configure an owner object, use the **owner** command in module CSM configuration submode. To remove an **owner** configuration, use the **no** form of this command.

owner *name*

no owner

Syntax Description

name	Name of the object owner.

Defaults

This command has no default settings.

Command Modes

Module CSM configuration submode

Command History

Release	Modification
4.1(1)	This command was introduced.

Usage Guidelines

You can define more than one virtual server to the same owner, associate multiple servers to an owner, and apply a connection watermark. After the sum of the number of open connections to all virtual servers in a particular owner reaches the VIP connection watermark level for that owner, new connections to any of these virtual servers are rejected by the CSM.

Examples

This example shows how to configure an owner object:

```
Cat6k-2(config-module-csm)# owner sequel
```

Related Commands

billing-info (owner submode)
contact-info (owner submode)
maxconns (owner submode)

billing-info (owner submode)

To configure billing information for an owner object, use the **billing-info** command in the owner configuration submode. To remove billing information from the configuration, use the **no** form of this command.

billing-info *billing-address-information*

no billing-info

Syntax Description

billing-address-information	Specifies the owner's billing address.

Defaults

This command has no default settings.

Command Modes

Module CSM configuration submode

Command History

Release	Modification
3.1(1)	This command was introduced.

Examples

This example shows how to configure an owner object:

```
Cat6k-2(config-owner)# billing-info 300 cordera avenue
```

Related Commands

contact-info (owner submode)
owner

contact-info (owner submode)

To configure an e-mail address for an owner object, use the **contact-info** command in owner configuration submode. To remove the contact information from the **owner** configuration, use the **no** form of this command.

contact-info *string*

no contact-info

Syntax Description

string	The owner's information.

Defaults

This command has no default settings.

Command Modes

Module CSM configuration submode

Command History

Release	Modification
3.1(1)	This command was introduced.

Examples

This example shows how to configure an owner object:

```
Cat6k-2(config-owner)# contact-info shaggy@angel.net
```

Related Commands

billing-info (owner submode)
owner

maxconns (owner submode)

To configure the maximum number of concurrent connections allowed for an owner object, use the **maxconns** command in owner configuration submode. To remove the maximum connections from the **owner** configuration, use the **no** form of this command.

maxconns *number*

no maxconns

Syntax Description

number	The number of maximum connections to the owner object.

Defaults

This command has no default settings.

Command Modes

Module CSM configuration submode

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

When the maximum number of connections is reached, the connections are reset and the CSM does not accept further connections.

Examples

This example shows how to configure an owner object:

```
Cat6k-2(config-owner)# maxconns 300
```

Related Commands

billing-info (owner submode)
contact-info (owner submode)
owner

policy

To configure policies, associate attributes to a policy, and then enter the policy configuration submode, use the **policy** command. In this submode, you can configure the policy attributes. The policy is associated with a virtual server in virtual server submode. To remove a policy, use the **no** form of this command.

policy *policy-name*

no policy *policy-name*

Syntax Description

policy-name	Name of an SLB policy instance; the character string is limited to 15 characters.

Defaults

This command has no default settings.

Command Modes

Module CSM configuration submode

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

Policies establish rules for balancing connections to servers. They can contain URL maps, cookie maps, header maps, client groups, sticky groups, DSCP values, and server farms. The order in which policies are linked to a virtual server determines the precedence of the policy. When two or more policies match a requested URL, the policy with the highest precedence is selected.

Note All policies should be configured with a server farm.

Examples

This example shows how to configure a policy named policy_content:

```
Cat6k-2(config-module-csm)# policy policy_content
Cat6k-2(config-slb-policy)# serverfarm new_serverfarm
Cat6k-2(config-slb-policy)# url-map url_map_1
Cat6k-2(config-slb-policy)# exit
```

Related Commands

show module csm owner
slb-policy (virtual server submode)

client-group (policy submode)

To associate an access list with a policy, use the **client-group** command in SLB policy configuration submode. To remove and access list from a policy, use the **no** form of this command.

client-group {*1–99* | *std-access-list-name*}

no client-group

Syntax Description

1–99	Standard IP access list number.
std-access-list-name	Standard access list name.

Defaults

This command has no default settings.

Command Modes

SLB policy configuration submode

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

Only client groups that you create with the **ip access-list standard** command can be associated with an SLB policy. You can only associate one client group with a given SLB policy.

Examples

This example shows how to configure a client group:

```
Cat6k-2(config-slb-policy)# client-group 44
Cat6k-2(config-slb-policy)# exit
```

Related Commands

ip access-list standard
policy
show module csm owner

cookie-map (policy submode)

To associate a list of cookies with a policy, use the **cookie-map** command in SLB policy configuration submode. To remove a cookie map, use the **no** form of this command.

cookie-map *cookie-map-name*

no cookie-map

Syntax Description

cookie-map-name	Name of the cookie list associated with a policy.

Defaults

This command has no default settings.

Command Modes

SLB policy configuration submode

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

You can associate only one cookie map with a policy. To configure cookie maps use the **map cookie** command. The cookie map name must match the name specified in the **map cookie** command.

Examples

This example shows how to configure a cookie-based SLB policy named policy_content:

```
Cat6k-2(config-module-csm)# policy policy_content
Cat6k-2(config-slb-policy)# serverfarm new_serverfarm
Cat6k-2(config-slb-policy)# cookie-map cookie-map-1
Cat6k-2(config-slb-policy)# exit
Cat6k-2(config)
```

Related Commands

map cookie
policy
show module csm owner

header-map (policy submode)

To specify the HTTP header criteria to include in a policy, use the **header-map** command in SLB policy configuration submode. To remove a header map, use the **no** form of this command.

Note If any HTTP header information is matched, the policy rule is satisfied.

header-map *name*

no header-map

Syntax Description

name	Name of the previously configured HTTP header expression group.

Defaults

This command has no default settings.

Command Modes

SLB policy configuration submode

Command History

Release	Modification
2.1(1)	This command was introduced.

Usage Guidelines

Only one header map can be associated with a policy. The header map name must match the name specified in the **map header** command on page A-18.

Examples

This example shows how to configure a header-based policy named policy_content:

```
Cat6k-2(config-module-csm)# policy policy_content
Cat6k-2(config-slb-policy)# serverfarm new_serverfarm
Cat6k-2(config-slb-policy)# header-map header-map-1
Cat6k-2(config-slb-policy)# exit
```

Related Commands

map header
policy
show module csm owner

serverfarm (policy submode)

To associate a server farm with a policy, use the **serverfarm** command in the SLB policy configuration submode. To remove the server farm from the policy, use the **no** form of this command.

serverfarm *primary-serverfarm* [**backup** *sorry-serverfarm* [**sticky**]]

no serverfarm

Syntax Description

primary-serverfarm	Character string used to identify the server farm.
backup *sorry-serverfarm*	(Optional) Sets the sorry-serverfarm name to the backup server farm.
sticky	(Optional) Enables stickiness to the backup server.

Defaults

This command has no default settings.

Command Modes

SLB policy configuration submode

Command History

Release	Modification
1.1(1)	This command was introduced.
3.1(1)	The sorry server (backup server) option was added to this command.

Usage Guidelines

Use the **serverfarm** command to configure the server farm. Only one server farm can be configured per policy. The server farm name must match the name specified in the **serverfarm** module CSM configuration submode command. By default, the sticky option does not apply to the backup server farm. To remove the backup server farm, you can either use the **serverfarm** command without the backup option or use the **no serverfarm** command.

The **backup** *sorry-serverfarm* [**sticky**] value defines whether the sticky group applied to the primary server farm is also applied for the backup server farm. If you do not specify stickiness for the primary server farm, then stickiness also is not applied to the backup server farm.

For example, if you have a sticky group configured for a policy, the primary server farm in this policy becomes sticky. The client will be stuck to the configured real in the primary server farm. When all of the real servers in the primary server farm fail, new requests from this client are sent to the backup server farm. When the real server in the primary server farm is operational, the following actions result:

- The existing connections to the backup real server continue to be serviced by the backup real server.
- The new requests from the client are sent to the backup real server if the sticky option is enabled for the backup server farm.
- The new requests return to the primary real server if the sticky option is not used on the backup server farm.

Examples

This example shows how to associate a server farm named central with a policy:

```
Cat6k-2(config-module-csm)# policy policy
Cat6k-2(config-slb-policy)# serverfarm central backup domino sticky
```

Related Commands

policy
serverfarm (policy submode)
show module csm owner

set ip dscp (policy submode)

To mark packets that match the policy with a DSCP value, use the **set ip dscp** command in the SLB policy configuration submode. To stop marking packet, use the **no** form of this command.

set ip dscp *dscp-value*

no set ip dscp

Syntax Description

dscp-value	The range is from 0 to 63.

Defaults

The default is that the CSM does not store DSCP values.

Command Modes

SLB policy configuration submode

Command History

Release	Modification
1.1(1)	This command was introduced.

Examples

This example shows how to mark packets to match a policy named policy_content:

```
Cat6k-2(config-module-csm)# policy policy_content
Cat6k-2(config-slb-policy)# set ip dscp 22
```

Related Commands

policy
show module csm owner

sticky-group (policy submode)

To associate a sticky group and the sticky group attributes to the policy, use the **sticky-group** command in the SLB policy configuration submode. To remove the sticky group from the policy, use the **no** form of this command.

sticky-group *group-id*

no sticky-group

Syntax Description

group-id	ID of the sticky group to be associated with a policy.

Defaults

The default is 0, which means that no connections are sticky.

Command Modes

SLB policy configuration submode

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

The *group-id* value must match the ID specified in the **sticky** command; the range is from 1 to 255.

Examples

This example shows how to configure a sticky group:

```
Cat6k-2(config-module-csm)# policy policy1
Cat6k-2(config-slb-policy)# sticky-group 5
```

Related Commands

policy
show module csm owner
show module csm sticky
sticky

url-map (policy submode)

To associate a list of URLs with the policy, use the **url-map** command in SLB policy configuration submode. To remove the URL map from the policy, use the **no** form of this command.

url-map *url-map-name*

no url-map

Syntax Description

url-map-name	Name of the URL list to be associated with a policy.

Defaults

The default is no URL map.

Command Modes

SLB policy configuration submode

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

Only one URL map can be associated with a policy. To configure URL maps, use the **map url** command.

Examples

This example shows how to associate a list of URLs with a policy named assembly:

```
Cat6k-2(config-module-csm)# policy policy
Cat6k-2(config-slb-policy)# url-map assembly
```

Related Commands

map url
policy
show module csm owner

probe

To configure a probe and probe type for health monitoring, and then enter the probe configuration submode, use the **probe** command. To remove a probe from the configuration, use the **no** form of this command.

probe *probe-name* {**http** | **icmp** | **telnet** | **tcp** | **ftp** | **smtp** | **dns** | **udp** | **script**}

no probe *probe-name*

Syntax Description

probe-name	Name of the probe; the character string is limited to 15 characters.
http	Creates an HTTP probe with a default configuration.
icmp	Creates an ICMP probe with a default configuration.
telnet	Creates a Telnet probe with a default configuration.
tcp	Creates a TCP probe with a default configuration.
ftp	Creates an FTP probe with a default configuration.
smtp	Creates an SMTP probe with a default configuration.
dns	Creates a DNS probe with a default configuration.
udp	Creates a UPD probe with a default configuration.
script	Creates a script probe with a default configuration.

Defaults

This command has no default settings.

Command Modes

Module CSM configuration submode

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

A probe can be assigned to a server farm in serverfarm submode. The UDP probe requires ICMP because otherwise the UDP probe will be unable to detect when a server has gone down or has been disconnected. You must associate UDP to the supervisor engine and then configure ICMP.

Because the UDP probe is a raw UDP probe, the CSM uses a single byte in the payload for probe responses. The CSM does not expect any meaningful response from the UDP application. The CSM uses the ICMP unreachable message to determine if the UDP application is not reachable. If there is no ICMP unreachable message in the receive timeout, then the CSM assumes that the probe is operating correctly.

If the IP interface of the real server is down or disconnected, the UDP probe does not know that the UDP application is unreachable. You must configure the ICMP probe in addition to the UDP probe for any server.

The CSM uses the DNS probe as the high-level UDP application. You also can use a TCL script to configure this probe.

When configuring Global Server Load Balancing (GSLB) type probes, the **port** submode command is not used to specify which destination UDP port to query. Use the CSM environment variable GSLB_KALAP_UDP_PORT instead. The default is port 5002.

To specify probe frequency and the number of retries for KAL-AP, ICMP, HTTP, and DNS probes when associated with a GSLB server farm environment, the following variables must be used instead of the probe configuration submode commands:

```
GSLB_KALAP_PROBE_FREQ           10
GSLB_KALAP_PROBE_RETRIES        3
GSLB_ICMP_PROBE_FREQ            10
GSLB_ICMP_PROBE_RETRIES         3
GSLB_HTTP_PROBE_FREQ            10
GSLB_HTTP_PROBE_RETRIES         2
GSLB_DNS_PROBE_FREQ             10
GSLB_DNS_PROBE_RETRIES          3
```

Examples

This example shows how to configure an HTTP probe named TREADER:

```
Cat6k-2(config-module-csm)# probe TREADER http
```

Related Commands

probe
show module csm probe

address (probe submode)

To specify a destination IP address for health monitoring, use the **address** command in SLB probe configuration submode. To remove the address, use the **no** form of this command.

address *ip-address* [**routed**]

no address *ip-address*

Syntax Description

ip-address	Specifies the real server's destination IP address.
routed	(Optional) Specifies that the probe is routed according to the CSM routing table.

Defaults

This command has no default settings.

Command Modes

SLB probe configuration submode

Command History

Release	Modification
2.1(1)	This command was introduced.

Usage Guidelines

Multiple addresses can be configured for a DNS probe. For an ICMP probe, you can configure one address. Allows the probes to cross the firewall to check the link to the host on the other side. ICMP is the only probe that supports the address parameter without the **routed** option, which is used for firewall load balancing.

Examples

This example shows how to configure an IP address of the real server:

```
Cat6k-2(config-slb-probe-icmp)# address 101.23.45.36
```

Related Commands

probe
show module csm probe

credentials (probe submode)

To configure basic authentication values for an HTTP probe, use the **credentials** command in the SLB HTTP probe configuration submode. To remove the credentials configuration, use the **no** form of this command.

credentials *username* [*password*]

no credentials

Syntax Description

username	Name that appears in the HTTP header.
password	(Optional) Password that appears in the HTTP header.

Defaults

This command has no default settings.

Command Modes

SLB HTTP probe configuration submode

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

This command is for HTTP probes.

Examples

This example shows how to configure authentication for an HTTP probe:

```
Cat6k-2(config-slb-probe-http)# credentials seamless abercrombie
```

Related Commands

probe
show module csm probe

expect status (probe submode)

To configure a status code for the probe, use the **expect status** command in the SLB HTTP/FTP/Telnet/SMTP probe configuration submode. To remove the status code from the configuration, use the **no** form of this command.

expect status *min-number* [*max-number*]

no expect status *min-number* [*max-number*]

Syntax Description

min-number	Single status code if the *max-number* value is not specified.
max-number	(Optional) Maximum status code in a range.

Defaults

The default range is 0 to 999 (any response from the server is valid).

Command Modes

SLB HTTP/FTP/Telnet/SMTP probe configuration submode

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

This command is for HTTP, FTP, Telnet, and SMTP probes. You can specify multiple status code ranges with this command by entering one command at a time. If you specify the *max-number* value, this number is used as the minimum status code of a range. If you specify no maximum number, this command uses a single number (*min-number*). If you specify both *min-number* and *max-number* values, this command uses the range between the numbers.

Both the minimum number and the maximum number can be any number between 0 and 999 as long as the maximum number is not lower than the minimum number.

For example:

`expect status 5` is the same as **`expect status 5 5`**

`expect status 0` specifies a range of 0 to 4

`expect status 900 999` specifies a range of 900 to 999.

You can specify many expected status ranges.

Note When you remove the expect status, you cannot set the range of numbers to 0 or as a range of numbers that includes the values you set for the expect status. The expect status state becomes invalid and does not restore the default range of 0 through 999. To remove the expect status, remove each set of numbers using the **no expect status** command. For example, enter the **no expect status 0 3** command and then enter the **no expect status 34 99** command.

Examples

This example shows how to configure an HTTP probe with multiple status code ranges:

```
Cat6k-2(config-slb-probe-http)# expect status 34 99
Cat6k-2(config-slb-probe-http)# expect status 0 33
Cat6k-2(config-slb-probe-http)#
```

Related Commands

probe
show module csm probe

failed (probe submode)

To set the time to wait before probing a failed server, use the **failed** command in the SLB probe configuration submode. To reset the time to wait before probing a failed server to default, use the **no** form of this command.

failed *failed-interval*

no failed

Syntax Description

failed-interval	Specifies the interval in seconds before the probe retires a failed server; the range is from 2 to 65535.

Defaults

The default value for the failed interval is 300 seconds.

Command Modes

SLB probe configuration submode

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

This command is used for all probe types.

Examples

This example shows how to configure a failed server probe for 200 seconds:

```
Cat6k-2(config-slb-probe-http)# failed 200
```

Related Commands

probe
show module csm probe

header (probe submode)

To configure a header field for the HTTP probe, use the **header** command in the SLB HTTP probe configuration submode. To remove the header field configuration, use the **no** form of this command.

header *field-name* [*field-value*]

no header *field-name*

Syntax Description

field-name	Name for the header being defined.
field-value	(Optional) Content for the header.

Defaults

This command has no default settings.

Command Modes

SLB HTTP probe configuration submode

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

You can configure multiple headers for each HTTP probe. The length of the *field-name* value plus the length of the *field-value* value plus 4 (for ":", space, and CRLF) cannot exceed 255 characters. This command is for HTTP probes.

Examples

This example shows how to configure a header field for the HTTP probe:

```
Cat6k-2(config-slb-probe-http)# header abacadabra
```

Related Commands

probe
show module csm probe

interval (probe submode)

To set the time interval between probes, use the **interval** command in the SLB probe configuration submode. To reset the time interval between probes to default, use the **no** form of this command.

interval *seconds*

no interval

Syntax Description

seconds	Number of seconds to wait between probes from the end of the previous probe to the beginning of the next probe; the range is from 2 to 65535.

Defaults

The default value for the interval between probes is 120 seconds.

Command Modes

SLB probe configuration submode

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

This command is used for all probe types.

Examples

This example shows how to configure a probe interval of 150 seconds:

```
Cat6k-2(config-slb-probe-http)# interval 150
```

Related Commands

probe
show module csm probe

name (probe submode)

To configure a domain name for the DNS probe, use the **name** command in the SLB DNS probe configuration submode. To remove the name from the configuration, use the **no** form of this command.

name *domain-name*

no name

Syntax Description

domain-name	Domain name that the probe sends to the DNS server.

Defaults

This command has no default settings.

Command Modes

SLB DNS probe configuration submode

Command History

Release	Modification
1.1(1)	This command was introduced.

Examples

This example shows how to specify the probe name that is resolved by the DNS server:

```
Cat6k-2(config-slb-probe-dns)# name astro
```

Related Commands

probe
show module csm probe

open (probe submode)

To set the time to wait for a TCP connection, use the **open** command in the SLB HTTP/TCP/FTP/Telnet/SMTP probe configuration submode. To reset the time to wait for a TCP connection to default, use the **no** form of this command.

open *open-timeout*

no open

Syntax Description

open-timeout	Maximum number of seconds to wait for the TCP connection; the range is from 1 to 65535.

Defaults

The default value for the open timeout is 10 seconds.

Command Modes

SLB HTTP/TCP/FTP/Telnet/SMTP probe configuration submode

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

This command is not used for any non-TCP probes, such as ICMP or DNS.

Note There are two different timeout values: open and receive. The open timeout specifies how many seconds to wait for the connection to open (that is, how many seconds to wait for SYN ACK after sending SYN). The receive timeout specifies how many seconds to wait for data to be received (that is, how many seconds to wait for an HTTP reply after sending a GET/HHEAD request). Because TCP probes close as soon as they open without sending any data, the receive timeout is not used.

Examples

This example shows how to configure a time to wait for a TCP connection of 5 seconds:

```
Cat6k-2(config-slb-probe-http)# open 5
```

Related Commands

probe
show module csm probe

port (probe submode)

To configure an optional port for the DNS probe, use the **port** command in the SLB probe configuration submode. To remove the port from the configuration, use the **no** form of this command.

port *port-number*

no port

Syntax Description

port-number	Sets the port number.

Defaults

The default value for the port number is 0.

Command Modes

This command is available in all SLB probe configuration submodes except ICMP.

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

When the port of a health probe is specified as 0, the health probe uses the configured port number from the real server (if a real server is configured) or the configured port number from the virtual server (if a virtual server is configured and no port is configured for the real server). The default port value is 0. For the ICMP probes, where there is no port number, the port value is ignored. The **port** command is available for all probe types except ICMP.

Examples

This example shows how to specify the port for the DNS server:

```
Cat6k-2(config-slb-probe-dns)# port 63
```

Related Commands

probe
show module csm probe

receive (probe submode)

To set the time to wait for a reply from a server, use the **receive** command in the SLB probe configuration submode. To reset the time to wait for a reply from a server to default, use the **no** form of this command.

receive *receive-timeout*

no receive

Syntax Description

receive-timeout	Number of seconds to wait for reply from a server; the range is from 1 to 65535.

Defaults

The default value for a receive timeout is 10 seconds.

Command Modes

SLB probe configuration submode

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

This command is available for all probe types except TCP.

Note There are two different timeout values: open and receive. The open timeout specifies how many seconds to wait for the connection to open (that is, how many seconds to wait for SYN ACK after sending SYN). The receive timeout specifies how many seconds to wait for data to be received (that is, how many seconds to wait for an HTTP reply after sending a GET/HHEAD request). Because TCP probes close as soon as they open without sending any data, the receive timeout is not used.

Examples

This example shows how to configure a time to wait for a reply from a server to 5 seconds:

```
Cat6k-2(config-slb-probe-http)# receive 5
```

Related Commands

probe
show module csm probe

request (probe submode)

To configure the request method used by the HTTP probe, use the **request** command in the SLB HTTP probe configuration submode. To remove the request method from the configuration, use the **no** form of this command.

request [**method {get** | **head**}] [**url** *path*]

no request [**method {get** | **head**}] [**url** *path*]

Syntax Description

method get	(Optional) Configures a method for the probe request and directs the server to get this page.
method head	(Optional) Configures a method for the probe request and directs and directs the server to get only the header for this page.
url *path*	(Optional) A character string up to 255 characters specifying the URL path.

Defaults

The default path is /.
The default method is the **get** option.

Command Modes

SLB HTTP probe configuration submode

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

The CSM supports only the **get** and **head** request methods. This command is for HTTP probes.

Examples

This example shows how to configure a request method for the probe configuration:

```
Cat6k-2(config-slb-probe-http)# request method head
```

Related Commands

probe
show module csm probe

retries (probe submode)

To set the number of failed probes that are allowed before marking the server failed, use the **retries** command in the SLB probe configuration submode. To reset the number of failed probes allowed before marking a server as failed to default, use the **no** form of this command.

retries *retry-count*

no retries

Syntax Description

retry-count	Number of probes to wait before marking a server as failed; the range is from 0 to 65535.

Defaults

The default value for retries is 3.

Command Modes

SLB probe configuration submode

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

This command is used for all probe types.

Note Set retries to 2 or more. If retries are set to 1, a single dropped probe packet will bring down the server. A setting of 0 places no limit on the number of probes that are sent. Retries are sent until the system reboots.

Examples

This example shows how to configure a retry count of 3:

```
Cat6k-2(config-slb-probe-http)# retries 3
```

Related Commands

probe
show module csm probe

script (probe submode)

To create a script for a probe, use the **script** command.

script *script_name*

Syntax Description

script_name	Specifies a probe script.

Defaults

This command has no default settings.

Command Modes

SLB probe script configuration submode

Usage Guidelines

The script name should match a script in a configured script file.

Command History

Release	Modification
3.1(1)	This command was introduced.

Examples

This example shows how to create a script probe:

```
Cat6k-2(config-module-csm)# ip slb script file tftp://192.168.10.102/csmScripts
Cat6k-2(config-probe-script)# script echoProbe.tcl
Cat6k-2(config-probe-script)# interval 10
Cat6k-2(config-probe-script)# retries 1
Cat6k-2(config-probe-script)# failed 30
```

Related Commands

failed (probe submode)
interval (probe submode)
open (probe submode)
probe
receive (probe submode)
retries (probe submode)
script file
show module csm probe

real

To identify a real server that is a member of the server farm, and then enter the real server configuration submode, use the **real** command in the SLB serverfarm configuration submode. To remove the real server from the configuration, use the **no** form of this command.

real *ip-address* [*port*]

no real *ip-address* [*port*]

Syntax Description

ip-address	Real server IP address.
port	(Optional) Port translation for the real server; the range is from 1 to 65535.

Defaults

The default is no port translation for the real server.

Command Modes

SLB serverfarm configuration submode

Usage Guidelines

The IP address that you supply provides a load-balancing target for the CSM. This target can be any IP addressable object. For example, the IP addressable object may be a real server, a firewall, or an alias IP address of another CSM.

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

You can configure a real server as follows:

- **no inservice**—Using the **no inservice** command in the real server submode, the CSM is specified as out of service. There is no sticky and no new connections being applied.

  Note If you specify no inservice, the CSM does not remove open connections. If you want to remove open connections. you must perform that task manually using the **clear module csm** *slot* **conn** command.

- **inservice**—Using the **inservice** command in the real server submode, the CSM is specified as in service. Sticky is allowed and new connections to the module can be made.
- **inservice standby**—Specifies that when in standby mode, the real server only accepts connections when the primary real server has failed.

Examples

This example shows how to identify a real server and enter the real server submode:

```
Cat6k-2(config-slb-sfarm)# real 102.43.55.60
Cat6k-2(config-slb-real)#
```

Related Commands

inservice (real server submode)
script task
show module csm real
show module csm serverfarm

backup real (real server submode)

To apply new connections to real servers when a primary server is down, use the **backup real** command in the SLB real server configuration submode. To remove a real server from service, use the **no** form of this command.

backup real {*ip* | **name** *name*} [*port*]

no backup real

Syntax Description

ip	Specifies the backup server's IP address.
name *name*	Specifies the real server name.
port	(Optional) Specifies the port where the backup real server is located.

Defaults

This command has no areguments or keywords.

Command Modes

SLB real server configuration submode

Command History

Release	Modification
3.2(1)	This command was introduced.

Usage Guidelines

A weight of 0 is now allowed for graceful shutdown of existing connections. The **backup real** command can be used in these situations where a server farm is specified:

- Directly under a virtual server.
- In a policy and then associated to a virtual server.

Examples

This example shows how to enable a real server:

```
Cat6k-2(config-slb-real)# backup real 10.2.2.1 3
Cat6k-2(config-slb-real)#
```

Related Commands

failaction (serverfarm submode)
real (static NAT submode)
show module csm real

health probe (real server submode)

To configure a probe for the real server, use the **health probe** command in the SLB real server configuration submode. To remove the probe from the configuration, use the **no** form of this command.

health probe *probe-name* **tag** *string*

no health probe

Syntax Description

probe-name	Names the probe.
tag	Specifies a tag for the probe.
string	Specifies a string to identify the probe.

Defaults

This command has no default values.

Command Modes

SLB real server configuration submode

Command History

Release	Modification
1.1(1)	This command was introduced.

Examples

This example shows how to configure a probe for a server:

```
Cat6k-2(config-slb-sfarm)# real 102.2.2.1
Cat6k-2(config-slb-real)# health probe mission tag 12345678
```

Related Commands

real
show module csm real

inservice (real server submode)

To enable the real servers, use the **inservice** command in the SLB real server configuration submode. To remove a real server from service, use the **no** form of this command.

inservice [**standby**]

no inservice

Syntax Description

standby	(Optional) Specifies that when in standby mode, the real server only accepts connections when the primary real server has failed.

Defaults

The default is that a real server is not in service.

Command Modes

SLB real server configuration submode

Command History

Release	Modification
1.1(1)	This command was introduced.
3.2(1)	This command was modified for firewall load-balancing (FWLB) reassignment.

Usage Guidelines

The **standby** keyword is used to remove a real server from rotation when you want to allow sticky and existing connections to continue. You can then set the real server to **no inservice** to remove the remaining active connections.

When you specify the **no inservice** command, the CSM will not remove open connections. To remove open connections, you must remove them using the **clear module csm** *slot* **connection** command.

The CSM performs graceful server shutdown when a real server is taken out of service when you enter the **no inservice** command. This command stops all new sessions from being load balanced to the specified real server while allowing existing sessions to complete or time out. New sessions are load balanced to other servers in the server farm for that virtual server.

This example shows how to remove a real server from service:

```
Router(config-slb-real)# no inservice
```

Examples

This example shows how to enable a real server:

```
Cat6k-2(config-slb-sfarm)# real 10.2.2.1
Cat6k-2(config-slb-real)# inservice
```

Related Commands

real
show module csm real

maxconns (real server submode)

To limit the number of active connections to the real server, use the **maxconns** command in the SLB real server configuration submode. To change the maximum number of connections to its default value, use the **no** form of this command.

maxconns *max-conns*

no maxconns

Syntax Description

max-conns	Maximum number of active connections on the real server at any time; the range is from 1 to 4294967295.

Defaults

The default value is the maximum value or infinite (not monitored).

Command Modes

SLB real server configuration submode

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

When you specify the **minconns** command, you must also specify the **maxconns** command.

Examples

This example shows how to limit the connections to a real server:

```
Cat6k-2(config-slb-sfarm)# real 10.2.2.1
Cat6k-2(config-slb-real)# maxconns 4000
```

Related Commands

minconns (real server submode)
real
show module csm real

minconns (real server submode)

To establish a minimum connection threshold for the real server, use the **minconns** command in the SLB real server configuration submode. To change the minimum number of connections to the default value, use the **no** form of this command.

minconns *min-cons*

no minconns

Syntax Description

min-cons	Minimum number of connections allowed on the real server; the range is from 0 to 4294967295.

Defaults

The default value is the set minumum number of connections.

Command Modes

SLB real server configuration submode

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

When the threshold of the **maxconns** command is exceeded, the CSM stops sending connections until the number of connections falls below the **minconns** command threshold. This value must be lower than the maximum number of connections configured by the **maxconns** command. When you specify the **minconns** command, you must also specify the **maxconns** command.

Examples

This example shows how to establish a minimum connection threshold for a server:

```
Cat6k-2(config-slb-sfarm)# real 102.2.2.1
Cat6k-2(config-slb-real)# minconns 4000
```

Related Commands

maxconns (real server submode)
real
show module csm real

redirect-vserver (real server submode)

To configure a real server to receive traffic redirected by a redirect virtual server, use the **redirect-vserver** command in the SLB real server configuration submode. To specify that traffic is not redirected to the real server, use the **no** form of this command.

redirect-vserver *name*

no redirect-vserver

Syntax Description

name	Name of the virtual server that has its requests redirected.

Defaults

Traffic is not redirected to the server.

Command Modes

SLB real server configuration submode

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

Mapping real servers to redirect virtual servers provides persistence for clients to real servers across TCP sessions. Before using this command, you must create the redirect virtual server in serverfarm submode with the **redirect-vserver** command.

Examples

This example shows how to map a real server to a virtual server:

```
Cat6k-2(config-slb-sfarm)#   real 10.2.2.1
Cat6k-2(config-slb-real)# redirect-vserver timely
```

Related Commands

real
redirect-vserver
show module csm real
show module csm vserver redirect

weight (real server submode)

To configure the capacity of the real servers in relation to the other real servers in the server farm, use the **weight** command in the SLB real server configuration submode. To change the server's weight to its default capacity, use the **no** form of this command.

weight *weighting-value*

no weight

Syntax Description

weighting-value	Value to use for the server farm predictor algorithm; the range is from 0 to 100.

Defaults

The weighting value default is 8.

Command Modes

SLB real server configuration submode

Command History

Release	Modification
1.1(1)	This command was introduced.

Examples

This example shows how to configure the weight of a real server:

```
Cat6k-2(config-slb-sfarm)#   real 10.2.2.1
Cat6k-2(config-slb-real)# weight 8
```

Related Commands

predictor (serverfarm submode)
real
show module csm real

redirect-vserver

To specify the name of a virtual server to receive traffic redirected by the server farm, and then enter redirect virtual server configuration submode, use the **redirect-vserver** command. To remove the redirect virtual server, use the **no** form of this command.

redirect-vserver *name*

no redirect-vserver *name*

Syntax Description

name	Name of the virtual server to receive traffic redirected by the server farm; the virtual server name can be no longer than 15 characters.

Defaults

This command has no default settings.

Command Modes

SLB serverfarm configuration submode

Command History

Release	Modification
1.1(1)	This command was introduced.

Examples

This example shows how to name the virtual server:

```
Cat6k-2(config-slb-sfarm)#   redirect-vserver quantico
```

Related Commands

real
redirect-vserver (real server submode)
script task
show module csm serverfarm
show module csm vserver redirect

advertise (redirect virtual server submode)

To allow the CSM to advertise the IP address of the virtual server as the host route, use the **advertise** command in the SLB redirect virtual server configuration mode. To stop advertising the host route for this virtual server, use the **no** form of this command.

advertise [active]

no advertise

Syntax Description

active	(Optional) Allows the CSM to advertise the IP address of the virtual server as the host route.

Defaults

The default for network mask is 255.255.255.255 if the network mask is not specified.

Command Modes

SLB redirect virtual server configuration submode

Usage Guidelines

Without the active option, the CSM always advertises the virtual server IP address whether or not there is any active real server attached to this virtual server.

Command History

Release	Modification
1.1(1)	This command was introduced.

Examples

This example shows how to restrict a client from using the redirect virtual server:

```
Cat6k-2(config-slb-redirect-vs)# advertise 10.5.2.1 exclude
```

Related Commands

show module csm vserver redirect
vserver

client (redirect virtual server submode)

To restrict which clients are allowed to use the redirect virtual server, use the **client** command in the SLB redirect virtual server configuration mode. To remove the client definition from the configuration, use the **no** form of this command.

client *ip-address* [*network-mask*] [**exclude**]

no client *ip-address* [*network-mask*]

Syntax Description

ip-address	Client's IP address.
network-mask	(Optional) Client's IP mask.
exclude	(Optional) Specifies that the IP address is disallowed.

Defaults

The default for network mask is 255.255.255.255 if the network mask is not specified.

Command Modes

SLB redirect virtual server configuration submode

Usage Guidelines

The network mask is applied to the source IP address of incoming connections and the result must match the IP address before the client is allowed to use the virtual server. If you do not specify the **exclude** option, the IP address and network mask combination is allowed.

Command History

Release	Modification
1.1(1)	This command was introduced.

Examples

This example shows how to restrict a client from using the redirect virtual server:

```
Cat6k-2(config-slb-redirect-vs)# client 10.5.2.1 exclude
```

Related Commands

client-group (policy submode)
show module csm vserver redirect
vserver

idle (redirect virtual server submode)

To specify the connection idle timer duration, use the **idle** command in the SLB redirect virtual server configuration submode. To disable the idle timer, use the **no** form of this command.

idle *duration*

no idle

Syntax Description

duration	SLB connection idle timer in seconds; the range is from 4 to 65535.

Defaults

The default is 3600.

Command Modes

SLB redirect virtual server configuration submode

Command History

Release	Modification
1.1(1)	This command was introduced.

Examples

This example shows how to specify the connection idle timer duration:

```
Cat6k-2(config-slb-redirect-vs)# idle 7
```

Related Commands

redirect-vserver (real server submode)
show module csm vserver redirect

inservice (redirect virtual server submode)

To enable the real server for use by the CSM, use the **inservice** command in the SLB redirect virtual server configuration submode. If this command is not specified, the virtual server is defined but not used. To disable the virtual server, use the **no** form of this command.

inservice

no inservice

Syntax Description

This command has no arguments or keywords.

Defaults

The virtual server is disabled.

Command Modes

SLB redirect virtual server configuration submode

Command History

Release	Modification
1.1(1)	This command was introduced.

Examples

This example shows how to enable a redirect virtual server for use by the CSM:

```
Cat6k-2(config-slb-redirect-vs)# inservice
```

Related Commands

redirect-vserver
show module csm vserver redirect

replicate csrp (redirect virtual server submode)

To enable connection redundancy, use the **replicate csrp** command in the SLB redirect virtual server configuration submode. To remove connection redundancy, use the **no** form of this command.

replicate csrp

no replicate csrp

Syntax Description

This command has no keywords or arguments.

Defaults

Connection redundancy is removed.

Command Modes

SLB virtual server configuration submode

Command History

Release	Modification
2.1(1)	This command was introduced.

Examples

This example shows how to enable connection redundancy:

```
Cat6k-2(config-slb-redirect-vs)# replicate csrp
```

Related Commands

show module csm vserver redirect
vserver

ssl (redirect virtual server submode)

To redirect an HTTP request to either HTTPS (SSL) or the FTP service, use the **ssl** command in the SLB redirect virtual server configuration submode . To reset the redirect of an HTTP request to an HTTP service, use the **no** form of this command.

ssl {**https** | **ftp** | *ssl-port-number*}

no ssl

Syntax Description

https	Specifies secure HTTP service.
ftp	Specifies FTP service.
ssl-port-number	SSL port number; the range is from 1 to 65535.

Defaults

HTTP service.

Command Modes

SLB redirect virtual server configuration submode

Command History

Release	Modification
1.1(1)	This command was introduced.

Examples

This example shows how to enable SSL forwarding:

```
Cat6k-2(config-slb-redirect-vs)# ssl 443
```

Related Commands

redirect-vserver (real server submode)
show module csm vserver redirect

virtual (redirect virtual server submode)

To specify the virtual server's IP address, the protocol used for traffic, and the port the protocol is using, use the **virtual** command in SLB redirect virtual server configuration submode. To reset the virtual server to its defaults, use the **no** form of this command.

virtual *v_ipaddress* **tcp** *port*

no virtual *v_ipaddress*

Syntax Description

v_ipaddress	Redirect virtual server's IP address.
tcp	Specifies the protocol used for redirect virtual server traffic.
port	Port number used by the protocol.

Defaults

The default IP address is 0.0.0.0, which prevents packet forwarding.

Command Modes

SLB redirect virtual server configuration submode

Command History

Release	Modification
1.1(1)	This command was introduced.

Examples

This example shows how to specify the virtual server's IP address, the protocol for redirect virtual server traffic, and the port number used by the protocol:

```
Cat6k-2(config-slb-redirect)# virtual 130.32.44.50 tcp 80
```

Related Commands

redirect-vserver (real server submode)
show module csm vserver redirect

vlan (redirect virtual server submode)

To define which source VLANs can be accessed on the redirect virtual server, use the **vlan** command in the SLB redirect virtual server submode. To remove the VLAN, use the **no** form of this command.

vlan {*vlan-number* | **all**}

no vlan

Syntax Description

vlan-number	The VLAN that the virtual server can access.
all	Specifies that all VLANs are accessed by the virtual server.

Defaults

The default is all VLANs are accessed.

Command Modes

SLB virtual server configuration submode

Command History

Release	Modification
2.1(1)	This command was introduced.

Examples

This example shows how to specify a VLAN for redirect virtual server access:

```
Cat6k-2(config-slb-redirect-vs)# vlan 5
```

Related Commands

sticky
sticky-group (policy submode)
show module csm sticky
show module csm vserver redirect

webhost backup (redirect virtual server submode)

To specify a backup string sent in response to HTTP requests, use the **webhost backup** command in SLB redirect virtual server configuration submode. To disable the backup string, use the **no** form of this command.

webhost backup *backup-string* [**301** | **302**]

no webhost backup

Syntax Description

backup-string	String sent in response to redirected HTTP requests; the maximum length is 127 characters.
301	(Optional) Specifies the HTTP status code: "The requested resource has been assigned a new permanent URL."
302	(Optional) Specifies the HTTP status code: "The requested resource resides temporarily under a different URL."

Defaults

The default status code is 302.

Command Modes

SLB redirect virtual server configuration submode

Usage Guidelines

This command is used in situations where the redirect virtual server has no available real servers. The **301** value or **302** value is used to specify the redirect code. The backup string may include a %p at the end to indicate inclusion of the path in the HTTP redirect location statement field.

Command History

Release	Modification
1.1(1)	This command was introduced.

Examples

This example shows how to specify a backup string that is sent in response to HTTP requests:

```
Cat6k-2(config-slb-redirect-vs)# webhost backup www.mybackup.com%p 301
```

Related Commands

redirect-vserver (real server submode)
show module csm vserver redirect

webhost relocation (redirect virtual server submode)

To specify a relocation string sent in response to HTTP requests, use the **webhost relocation** command in the SLB redirect virtual server configuration submode. To disable the relocation string, use the **no** form of this command.

webhost relocation *relocation string* [**301** | **302**]

no webhost relocation

Syntax Description

relocation string	String sent in response to redirected HTTP requests; the maximum length is 127 characters.
301	(Optional) Specifies the HTTP status code: "The requested resource has been assigned a new permanent URL."
302	(Optional) Specifies the HTTP status code: "The requested resource resides temporarily under a different URL."

Defaults

The default status code is 302.

Command Modes

SLB redirect virtual server configuration submode

Usage Guidelines

The backup string may include a %p at the end to indicate inclusion of the path in the HTTP redirect location statement field.

Command History

Release	Modification
1.1(1)	This command was introduced.

Examples

This example shows how to specify a relocation string that is sent in response to HTTP requests:

```
Cat6k-2(config-slb-redirect-vs)# webhost relocation www.myhome1.com%p 301
```

Related Commands

redirect-vserver (real server submode)
show module csm vserver redirect

reverse-sticky

To ensure that the CSM switches connections in the opposite direction and back to the original source, use the **reverse-sticky** command. To remove the reverse sticky option from the policy or the default policy of a virtual server, use the **no** form of this command.

reverse-sticky *group-id*

no reverse-sticky

Syntax Description

group-id	Number identifying the sticky group to which the virtual server belongs; the range is from 0 to 255.

Defaults

The default is that the reverse sticky option is not connected. Sticky connections are not tracked. The group ID default is 0.

Command Modes

SLB virtual server configuration submode.

Command History

Release	Modification
1.1(1)	This command was introduced.
3.1(1)	The **IP reverse-sticky** command is introduced.

Usage Guidelines

The sticky feature is not used for other virtual servers.

Examples

This example shows how to set the IP reverse-sticky feature:

```
Cat6k-2(config-module-csm)# vserver PUBLIC_HTTP
Cat6k-2(config-slb-vserver)# reverse-sticky 60
```

Related Commands

sticky
sticky-group (policy submode)
show module csm sticky
show module csm vserver redirect

script file

To load scripts from a script file to the CSM, use the **script file** command. To remove the script file command from the configuration, use the **no** form of this command.

script file {*file-url* | *bootflash:* | *const_nvram:* | *disk0:* | *flash:* | *ftp:* | *null:* | *nvram:* | *rcp:* | *slot0:* | *sup-bootflash:* | *sup-microcode:* | *sup-slot0:* | *system:* | *tftp:*}

no script file

Syntax Description

file-url	Sets the location of the script file to a URL.
bootflash:	Sets the standard Cisco IOS file name, such as *bootflash:webprobe.tcl*.
const_nvram:	Sets the location of the script file to the switch NVRAM.
disk0:	Sets the location of the script file on the CSM hard disk.
flash:	Sets the location of the script file to the CSM Flash memory.
ftp:	Sets the location of the script file to an FTP location.
null:	Sets the location of the script file to NULL.
nvram:	Sets the location of the script file to the NVRAM.
rcp:	Sets the location of the script file to the switch.
slot0:	Sets the location of the script file to the switch.
sup-bootflash:	Sets the location of the script file to the switch supervisor engine bootflash.
sup-microcode:	Sets the location of the script file to the switch supervisor microcode.
sup-slot0:	Sets the location of the script file to the switch supervisor engine.
system:	Sets the location of the script file to the switch.
tftp:	Sets the location of the script file to a TFTP location.

Defaults

This command has no default settings.

Command Modes

Module CSM configuration submode

Usage Guidelines

The file URL is a standard Cisco IOS file name such as *bootflash:webprobe.tcl*.

Command History

Release	Modification
3.1(1)	This command was introduced.

Examples

This example shows how to load scripts from a script file to the CSM:

```
Cat6k-2(config-module-csm)# script file file-url
```

Related Commands show module csm script

script task

To run a standalone task, use the **script task** command. To remove the standalone task from the configuration, use the **no** form of this command.

script task 1-100 script name

no script task 1-100 script name

Syntax Description

1-100	Task ID that identifies a specific running script.
script name	Identifies the script by name.

Defaults

This command has no default settings.

Command Modes

Module CSM configuration submode

Command History

Release	Modification
3.1(1)	This command was introduced.

Examples

This example shows how to run a standalone script:

```
Cat6k-2(config-module-csm)# script task 30 filerun
```

Related Commands

show module csm script