

Service Redundancy Protocol Configuration Mode Commands

The Service Redundancy Protocol Mode is used to configure properties for Interchassis Session Recovery (ICSR) services.

Command Modes

Exec > Global Configuration > Context Configuration > Service Redundancy Protocol Configuration

configure > context *context_name* **> service-redundancy-protocol**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-srp)#
```

Important The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

Important SRP commands must be identically configured on both the active and standby ICSR chassis.

- advertise-routes-in-standby-state, on page 2
- audit, on page 3
- bfd-mon-ignore-dead-interval, on page 5
- bind, on page 5
- chassis-mode, on page 6
- checkpoint session, on page 7
- configuration-interval, on page 9
- dead-interval, on page 9
- delay-interval, on page 10
- delta-route-modifier, on page 11
- do show, on page 12
- dscp-marking, on page 12
- end, on page 13
- exit, on page 14
- guard-timer, on page 14

- handle-interim-resource-msg, on page 15
- hello-interval, on page 16
- internal-switchover-retry-interval, on page 17
- monitor authentication-probe, on page 18
- monitor bfd , on page 19
- monitor bgp, on page 20
- monitor diameter, on page 21
- monitor hsrp, on page 23
- monitor sx , on page 24
- monitor system, on page 25
- num-internal-switchover-retry, on page 26
- peer-ip-address, on page 27
- priority, on page 28
- retain-complete-sess-info, on page 29
- route-modifier, on page 29
- standby database-recovery, on page 30
- switchover allow-all-data-traffic, on page 31
- switchover allow-early-active-transition, on page 32
- switchover allow-volte-data-traffic, on page 33
- switchover control-outage-optimization, on page 33

advertise-routes-in-standby-state

Enables advertising BGP routes from an ICSR chassis in standby state.

Product

All products that support ICSR

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Service Redundancy Protocol Configuration

configure > context *context_name* **> service-redundancy-protocol**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-srp)#
```

Syntax Description

advertise-routes-in-standby-state [hold-off-time *hold-off-time* **] [reset-bfd-nbrs** *bfd-down-time* **]**
default advertise-routes-in-standby-state [hold-off-time] [reset-bfd-nbrs]
no advertise-routes-in-standby-state [hold-off-time] [reset-bfd-nbrs]

default

Sets the specified route advertisement option to its default value–:

- **hold-off-time** – 30 seconds
- **reset-bfd-nbrs** – ??? milliseconds

no

Disables the specified type of route advertisement.

[hold-off-time *hold-off-time*]

This option delays advertising the BGP routes until the timer expires. Specify *hold-off-time* in seconds as an integer from 1 to 300.

[reset-bfd-nbrs *bfd-down-time*]

After resetting BFD, this option keeps the BFD sessions down for the configured number of milliseconds to improve network convergence. Specify *bfd-down-time* as an integer from 50 to 120000.

Usage Guidelines

Use this command and its keywords to take advantage of faster network convergence accrued from deploying BGP Prefix Independent Convergence (PIC) in the Optical Transport Network Generation Next (OTNGN).

BGP PIC is intended to improve network convergence which will safely allow for setting aggressive ICSR failure detection timers.

Example

The following command enables route advertisement from a standby ICSR chassis after a 40-second delay and will suppress BFD sessions for 50 milliseconds following a BFD reset.

```
advertise-routes-in-standby-state hold-off-time 40 reset-bfd-nbrs 50
```

audit

Sets the start time and periodicity for ICSR Service Redundancy Protocol (SRP) audits. This command can also be used to enter a schedule for running the audit.

Product

All products supporting ICSR

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Service Redundancy Protocol Configuration

configure > context *context_name* **> service-redundancy-protocol**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-srp)#
```

Syntax Description

```
[no] audit cron [ daily hour hour_number minute minute_number ] [ day-of-month
 day_number ] [ month month_number ] [ week-of-day day_name ]
[no] audit daily-start-time hour minute
[no] audit periodicity minutes
default audit periodicity
```

default

Resets the specified parameter to its default setting of 60.

no

Disables the specified function.

audit cron [daily hour *hour_number* minute *minute_number*] [day-of-month *day_number*] [month *month_number*] [week-of-day *day_name*]

Configures a cron job (time-based job scheduler) for running the audit. Supported scheduling variables include:

- **daily hour** *hour_number* **minute** *minute_number* – configures the hour and minute of the day when the job will run. Specify *hour_number* as an integer from 0 to 23 and *minute_number* as an integer from 0 to 59.
- **day-of-month** *day_number* – configures the day of the month when the job will run. Specify *day_number* as an integer from 1 to 31.
- **month** *month_number* – configures the month of the year when the job will run. Specify month_number as an integer from 1 to 12.
- **week-of-day** *day_name* – configures the week day on which the job will run. Specify *day_name* as one of the following names: friday, monday, saturday, sunday, thursday, tuesday, or wednesday.

daily-start-time *hour minute*

Specifies the daily start time. *hour* is a two-digit integer from 00 through 23. *minute* is a two-digit interval from 00 through 59. For example, a start time of 06 00 indicates that the audit will begin at 6:00 AM.

periodicity *minutes*

Specifies the interval in minutes for generating SRP audit statistics as an integer from 60 through 43200. For example, a periodicity of 90 indicates that SRP audit statistics will be generated every 90 minutes beginning at the specified start time. Default = 60.

Usage Guidelines

Use this command and its keywords to specify the start time and periodicity for generating ICSR SRP audit statistics.

You can also schedule audits to be run based on time-of-day, day-of-week, day-of-month and month-of-year.

This audit ensures that two ICSR peers are in synch and identifies any discrepancies prior to scheduled or unscheduled switchover events.

Example

The following command sequence specifies a start time of midnight and a periodicity of every two hours for generating SRP statistics:

```
audit daily-start-time 06 00
audit periodicity 90
```

The following command schedules the audit to run at midnight every Sunday.

```
cron daily hour 0 minute 0 week-of-day sunday
```

bfd-mon-ignore-dead-interval

Causes the standby ICSR chassis to ignore the dead interval and remain in the standby state until all the BFD chassis-to-chassis monitors fail.

Product

All products that support ICSR.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Service Redundancy Protocol Configuration

configure > context *context_name* **> service-redundancy-protocol**

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-srp)#`

Syntax Description

bfd-mon-ignore-dead-interval
default bfd-mon-ignore-dead-interval

default

Disables this feature.

Usage Guidelines

Enable this feature in association with BFD chassis-to-chassis monitoring to support more aggressive ICSR failure detection times.

For additional information, see the descriptions of the **dead-interval** and **monitor bfd** commands.

Example

The following command enables this feature:

bfd-mon-ignore-dead-interval

bind

Binds the service to the IP address of the local chassis.

Product

All products supporting ICSR

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Service Redundancy Protocol Configuration

configure > context *context_name* **> service-redundancy-protocol**

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-srp)#`

Syntax Description

```
bind address { ipv4 _address | ipv6_address }
no bind address
```

no

Removes the IP bind address.

ipv4 _address | ipv6_address

Specifies the system IP address using IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.



Important Both peers must be using the same address family (IPv4 or IPv6) or the Service Redundancy Protocol (SRP) connection will not be established.

Usage Guidelines Defines the IP address of the local chassis defined as part of the ICSR configuration.

Example

The following example binds the service to the IP address *10.1.1.1*:

```
bind address 10.1.1.1
```

chassis-mode

Defines the chassis's operational mode - primary or backup - for ICSR.

Product All products supporting ICSR

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > Service Redundancy Protocol Configuration

configure > context *context_name* **> service-redundancy-protocol**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-srp)#
```

Syntax Description

```
chassis-mode { backup | primary }
default chassis-mode
```

default

Resets the chassis mode to the default setting of backup.

backup

(Default) Configures the system as the backup chassis operating in standby state.

primary

Configures the system as the primary chassis operating in active state.

Usage Guidelines

Sets the chassis mode (primary or backup) for the system within the framework of ICSR.

Example

The following example configures the system as the primary chassis operating in active state

```
chassis-mode primary
```

checkpoint session

Configures checkpointing parameters between ICSR active and standby chassis.

Product

All products supporting ICSR

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Service Redundancy Protocol Configuration

configure > context *context_name* **> service-redundancy-protocol**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-srp)#
```

Syntax Description

```
checkpoint session compression { lz4 | zlib }
checkpoint session duration { ims-session | non-ims-session } seconds
checkpoint session nack { macro | micro } [ max-response number ]
checkpoint session periodic-interval minutes
default checkpoint session { compression | duration { ims-session |
non-ims-session } | periodic-interval }
no checkpoint session { compression | duration { ims-session |
non-ims-session } | nack { macro | micro } | periodic-interval }
```

default

Resets the following checkpoint session parameters to their default values:

- compression = zlib
- duration = 60 seconds
- periodic-interval = 48 minutes

no

Disables **compression, duration, nack,** and **periodic-interval** features.

compression { lz4 | zlib }

Specifies whether the LZ4 or zlib compression algorithm will be used to compress SRP payload messages.

LZ4 compression is effective only if both chassis are configured with LZ4. If any one chassis has zlib (default) configured, the compression algorithm reverts to zlib. The algorithm is negotiated only during initial socket establishment. Once agreed no more negotiation takes place until the TCP socket connection is reset.

Important A change in the configured compression algorithm resets the TCP Link.

duration { ims-session | non-ims-session } *seconds*

Specifies whether the checkpoint duration is being set for IMS (IP Multimedia Subsystem) or non-IMS sessions. The duration is the amount of time that a call must be active before it is check pointed. and is expressed as an integer from 0 through 65535 (Default = 60).

nack { macro | micro } [max-response *number*]

Enables a NACK feature for checkpoints. When this feature is enabled, the standby chassis sends a NACK in response to the receipt of a micro-checkpoint (MC) that fails to be successfully applied. The standby chassis will send more NACKs (configurable, default = 3) within a 10-minute window if an FC is not received. NACKs will continue to be sent within the 10-minute reset window until an FC is received and applied, or the configured number of maximum-responses is reached.

max-response is the total number NACKs that can be sent within the 10-minute window in response to a failed MC or FC expressed as an integer from 1 through 65535 (Default = 3).

Note The time interval window of 10 minutes is not configurable.

periodic-interval *minutes*

Configures the minimum periodic checkpoint duration in multiples of 12 minutes for sending macro-checkpoints (FCs) from the Active to the Standby chassis. The interval is specified as an integer divisible by 12 in the range from 24 through 1440 (Default = 48 minutes). The interval range for sending full checkpoints is 24 minutes to 24 hours (1140 minutes).

Usage Guidelines

Sets the type of compression algorithm to be used for SRP payload messages.

Sets the amount of time the chassis waits before check pointing an existing call session. Checkpoints can be separately set for IMS and/or non-IMS sessions.

Enable the NACK feature for handling checkpointing messaging on the Standby chassis.

Configures the interval between the sending of macro-checkpoints (full checkpoints) between the active and standby chassis.

Important The **compression**, **nack** and **periodic-interval** keywords will only appear if a special ICSR optimization feature license has been purchased and installed. Contact your Cisco account representative for assistance.

For additional information on ICSR checkpointing, see the *System Administration Guide*.

Example

The following example configures sets the checkpoint session duration for an IMS session to 6500 seconds:

```
checkpoint session duration ims-session 6500
```

The following command resets the periodic interval for sending full checkpoints to 36 minutes:

```
checkpoint session periodic-interval 36
```

configuration-interval

Defines the configuration validation interval.

Product

All products supporting ICSR

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Service Redundancy Protocol Configuration

configure > context *context_name* **> service-redundancy-protocol**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-srp)#
```

Syntax Description

configuration-interval *interval*
default configuration-interval

default

Resets the configuration interval to the default setting of 3600 seconds.

interval

Specifies the amount of time (number of seconds) between one configuration validation and the next configuration validation. *interval* must be an integer from 1 through 65535. Default = 3600.

Usage Guidelines

This configures the interval between configuration validations of the primary and backup chassis.

Example

The following example sets the configuration interval to 34 seconds:

```
configuration-interval 34
```

dead-interval

Defines the timeout interval before a peer is determined to be down.

Product All products supporting ICSR

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > Service Redundancy Protocol Configuration

configure > context *context_name* **> service-redundancy-protocol**

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-srp)#`

Syntax Description

dead-interval *interval*
default dead-interval

default

Resets the dead interval to the default setting of 30 seconds.

interval

Specifies the amount of time (in seconds) for the dead interval. *interval* must be an integer from 1 through 65535. Default = 30.

Usage Guidelines This command specifies the amount of time that one chassis waits to receive a communication from a peer before the listening chassis determines that the peer chassis is down.

Example

The following example sets the dead interval to 65 seconds:

```
dead-interval 65
```

delay-interval

Configures the delay time for starting the dead timer after configuration files are loaded.

Product All products supporting ICSR

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > Service Redundancy Protocol Configuration

configure > context *context_name* **> service-redundancy-protocol**

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-srp)#`

Syntax Description

delay-interval *interval*
default delay-interval

default

Sets or restores the default value assigned for the specified parameter.

interval

Specifies the amount of time (in seconds) for the delay interval. *interval* must be an integer from 1 through 65535.

Usage Guidelines

This configures interval for starting the dead timer after configuration files are loaded.

Example

The following example sets the delay interval to 65 seconds after the configuration files are loaded:

```
delay interval 65
```

delta-route-modifier

Specifies the delta used to compute the route modifier difference between the active and standby chassis. This delta is applied only in the standby state. *For Release 15.0 or higher,* it is used in both states.

Product

All products supporting ICSR

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Service Redundancy Protocol Configuration

configure > context *context_name* **> service-redundancy-protocol**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-srp)#
```

Syntax Description

delta-route-modifier *value*
default delta-route-modifier

default

Sets or restores the default value assigned for the specified parameter. Default = 1.

value

Specifies the value to be used when computing the route-modifier. *value* must be an integer from 1 through 15 (for 21.7 and later releases), or 1 through 7 (for releases prior to 21.7). Default: 1.

Usage Guidelines

The delta-route-modifier is used to compute the route modifier difference between active and standby chassis.

Example

The following example sets the delta for the route modifier to 2:

```
delta-route-modifier 2
```

do show

Executes all **show** commands while in Configuration mode.

Product All

Privilege Security Administrator, Administrator

Syntax Description

```
do show
```

Usage Guidelines Use this command to run all Exec mode **show** commands while in Configuration mode. It is not necessary to exit the Config mode to run a **show** command.

The pipe character **|** is only available if the command is valid in the Exec mode.



Caution There are some Exec mode **show** commands which are too resource intensive to run from Config mode. These include: **do show support collection**, **do show support details**, **do show support record** and **do show support summary**. If there is a restriction on a specific **show** command, the following error message is displayed:

```
Failure: Cannot execute 'do show support' command from Config mode.
```

dscp-marking

Sets DSCP marking values for SRP control and checkpoint (session maintenance) messages.

Product All products supporting ICSR

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > Service Redundancy Protocol Configuration

configure > context *context_name* **> service-redundancy-protocol**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-srp)#
```

Syntax Description

```
dscp-marking { control | session } dscp_value
default dscp-marking { control | session }
```

default

Sets the DSCP value to its default: **be** (Best Effort Per-Hop-Behaviour).

{ control | session }

Specifies the SRP message type for which a DSCP value is being set.

- **control** – SRP control messages [originate from vpnmgr]
- **session** – checkpoint messages (session maintenance) [originate from sessmgr]

dscp_value

Specifies the DSCP value to be used:

- **af11** – Assured Forwarding Class 1 low drop PHB (Per Hop Behavior)
- **af12** – Assured Forwarding Class 1 medium drop PHB
- **af13** – Assured Forwarding Class 1 high drop PHB
- **af21** – Assured Forwarding Class 2 low drop PHB
- **af22** – Assured Forwarding Class 2 medium drop PHB
- **af23** – Assured Forwarding Class 2 high drop PHB
- **af31** – Assured Forwarding Class 3 low drop PHB
- **af32** – Assured Forwarding Class 3 medium drop PHB
- **af33** – Assured Forwarding Class 3 high drop PHB
- **af41** – Assured Forwarding Class 4 low drop PHB
- **af42** – Assured Forwarding Class 4 medium drop PHB
- **af43** – Assured Forwarding Class 4 high drop PHB
- **be** – Best effort Per-Hop-Behaviour (default)
- **cs1** – Class selector 1 PHB
- **cs2** – Class selector 2 PHB
- **cs3** – Class selector 3 PHB
- **cs4** – Class selector 4 PHB
- **cs5** – Class selector 5 PHB
- **cs6** – Class selector 6 PHB
- **cs7** – Class selector 7 PHB
- **ef** – Expedited Forwarding PHB, for low latency traffic



Important If *dscp_value* is set incorrectly, packet drops may occur in intermediate devices.

Usage Guidelines Use this command to enable DSCP marking of SRP and checkpoint messages in ICSR environments.

Example

The following command sequence sets DSCP marking of control messages to Expedited Forwarding:

```
dcsp-marking control ef
```

end

Exits the current configuration mode and returns to the Exec mode.

Product All

Privilege Security Administrator, Administrator

Syntax Description **end**

Usage Guidelines Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product All

Privilege Security Administrator, Administrator

Syntax Description **exit**

Usage Guidelines Use this command to return to the parent configuration mode.

guard-timer

Configures the redundancy-guard-period and monitor-damping-period for SRP service monitoring.

Product All products supporting ICSR

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > Service Redundancy Protocol Configuration

configure > context *context_name* **> service-redundancy-protocol**

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-srp)#`

Syntax Description

guard-timer { aaa-switchover-timers { damping-period *seconds* **| guard-period** *seconds* **} | diameter-switchover-timers { damping-period** *seconds* **| guard-period** *seconds* **} | srp-redundancy-timers { aaa { damping-period** *seconds* **| guard-period** *seconds* **} | bgp { damping-period** *seconds* **| guard-period** *seconds* **} | diam { damping-period** *seconds* **| guard-period** *seconds* **} }**
default guard-timer aaa-switchover-timers { damping-period | guard-period }
default guard-timer diameter-switchover-timers { damping-period | guard-period }
default guard-timer srp-redundancy-timers { aaa { damping-period | guard-period } | bgp { damping-period | guard-period } | diam { damping-period | guard-period } }

default

Sets the specified guard timer to its default value:

- **damping-period** = 60 seconds
- **guard-period** = 60 seconds

aaa-switchover-timers

Sets timers that prevent back-to-back ICSR switchovers due to an AAA failure (post ICSR switchover) while the network is still converging.

diameter-switchover-timers

Sets timers that prevent a back-to-back ICSR switchover due to a Diameter failure (post ICSR switchover) while the network is still converging.

srp-redundancy-timers

Sets timers that prevent an ICSR switchover while the system is recovering from a local card-reboot/critical-task-restart failure.

damping-period *seconds*

Configures a delay time to trigger an ICSR switchover due to a monitoring failure within the guard-period. Specify *seconds* as an integer from 0 to 300.

guard-period *seconds*

Configures the local-failure-recovery network-convergence timer. Specify *seconds* as an integer from 0 to 300.

{ aaa | bgp | diam }

Specifies the type of SRP redundancy timer:

- **aaa** – local failure followed by AAA monitoring failure
- **bgp** – local failure followed by BGP monitoring failure
- **diam** – local failure followed by Diameter monitoring failure

Usage Guidelines

Use these guard timers to ensure that local failures, such as card reboots and task restarts, do not result in ICSR events which can be disruptive.

Example

The following command sets an SRP redundancy AAA guard period of 45 seconds:

```
guard-timer srp-redundancy-timers aaa guard-period 45
```

handle-interim-resource-msg

Enables the proper handling of version 16.1 SRP Interim Resource messages during an ICSR upgrade from prior releases.

Product

All products supporting ICSR

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Service Redundancy Protocol Configuration

configure > context *context_name* **> service-redundancy-protocol**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-srp)#
```

Syntax Description

handle-interim-resource-msg version-16.1
no handle-interim-resource-msg version-16.1

no

Disables this feature after it has been enabled. By default this feature is disabled to preserve compatibility with release versions prior to 16.1.

Usage Guidelines

Use this feature to properly handle Interim Resource messages when upgrading to StarOS 16.1. If you do not enable this feature, an ICSR configuration may experience PCRF binding problems (5002 error code message) when performing an ICSR upgrade from previous StarOS versions.

Example

The following command enables this feature:

handle-interim-resource-msg version-16.1

hello-interval

Defines the lapse time between sending the hello message.

Product

All products supporting ICSR

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Service Redundancy Protocol Configuration

configure > context *context_name* **> service-redundancy-protocol**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-srp)#
```

Syntax Description

hello-interval *interval*
default hello-interval

default

Resets the hello interval to the default setting of 10 seconds.

interval

Specifies the lapse time (in seconds) between sending the hello message. *interval* must be an integer from 1 through 65535. Default = 10.

Usage Guidelines

This command configures the hello interval - the amount of time that lapses between the sending of each hello message. Each chassis sends the other chassis a hello message at the expiration of every hello interval.

Example

The following example sets the hello interval to 35 seconds:

```
hello-interval 35
```

internal-switchover-retry-interval

Defines the interval between internal switchover retries.

Product

All products supporting ICSR

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Service Redundancy Protocol Configuration

configure > context *context_name* **> service-redundancy-protocol**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-srp)#
```

Syntax Description

internal-switchover-retry-interval *interval*
default internal-switchover-retry-interval

default

Resets the internal switchover retry interval to the default setting of 60 seconds.

interval

Specifies the amount of time (in seconds) between internal switchover retries. *interval* must be an integer from 10 through 120. Default = 60.

Usage Guidelines

This configures the interval between internal switchover retries. The system only initiates internal switchovers if Service Redundancy Protocol (SRP) monitoring is configured.



Important

See the **monitor authentication-probe**, **monitor bgp**, or **monitor diameter** commands for more information on associated SRP monitoring.

Example

The following example sets the internal switchover retry interval to 34 seconds:

```
internal-switchover-retry-interval 34
```

monitor authentication-probe

Enables SRP monitoring of the connection between the specified AAA server and the primary chassis.

Product

All products supporting ICSR

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Service Redundancy Protocol Configuration

configure > context *context_name* **> service-redundancy-protocol**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-srp)#
```

Syntax Description

`[ no ] monitor authentication-probe context` *`context_name`* **`{`** *`ipv4_address`* **`|`** *`ipv6_address`* **`} [ group`** *`group_id`* **`] [ port`** *`port_number`* **`]`**

no

Turns off the monitoring.

context *context_name*

Identifies the context being used.

context_name must be an existing context expressed as an alphanumeric string of 1 through 79 characters.

ipv4 _address | *ipv6_address*

Defines the IP address of the AAA server to be monitored in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

group *group_id*

Defines a Service Redundancy Protocol (SRP) peer group as an integer from 0 through 9. Default = 0.

In an Interchassis Session Recovery (ICSR) configuration, failover would occur if all peers within a group fail.

port *port_number*

Identifies a specific AAA server port for the authentication probe. *port_number* must be an integer from 1 through 65535.

Usage Guidelines This command initiates monitoring of the connection between the primary chassis and the specified AAA server through the use of authentication probe packets. If the connection drops, the standby chassis becomes active.

Example

The following example initiates the connection monitoring between the primary chassis and AAA server *10.2.3.4* at port *1025*:

```
monitor authentication-probe context test1 10.2.3.4 port 1025
```

monitor bfd

Enables SRP monitoring of the connection between the specified Bidirectional Forwarding Detection (BFD) neighbor and the primary chassis.

Product All products supporting ICSR

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > Service Redundancy Protocol Configuration

configure > context *context_name* **> service-redundancy-protocol**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-srp)#
```

Syntax Description **`[ no ] monitor bfd context`** *`context_name`* **`{`** *`ipv4_address`* **`|`** *`ipv6_address`* **`} { chassis-to-chassis | chassis-to-router }`**

no

Disables monitoring.

context *context_name*

Identifies the context being used. *context_name* must be an existing context expressed as an alphanumeric string of 1 through 79 characters.

The context refers to where the BFD peer is configured (SRP context).

ipv4 _address | *ipv6_address*

Defines the IP address of the BFD neighbor to be monitored, entered using IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

It refers to the IP address of the configured BFD (ICSR) peer.

chassis-to-chassis | chassis-to-router

chassis-to-chassis: BFD runs between primary and backup chassis on non-SRP links.

chassis-to-router: BFD runs between chassis and router.

Usage Guidelines This command initiates monitoring of the connection between the primary chassis and the specified BFD neighbor in the specified context. If the connection drops, the standby chassis becomes active.



Important BFD monitoring must run between chassis-to-chassis or chassis-to-router.

For additional information, see the description of the **bfd-mon-ignore-dead-interval** command.

Example

The following example initiates the chassis-to-chassis connection monitoring between the primary chassis and BFD neighbor *12.2.1.54*:

```
monitor bfd context test 12.2.1.54 chassis-to-chassis
```

monitor bgp

Enables SRP monitoring of the connection between the specified Border Gateway Protocol (BGP) peer and the primary chassis.

Product All products supporting ICSR

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > Service Redundancy Protocol Configuration

configure > context *context_name* **> service-redundancy-protocol**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-srp)#
```

Syntax Description **[no] monitor bgp [context** *context_name* **{** *ipv4_address* **|** *ipv6_address* **} [group** *group_id* **[vrf** *vrf_name* **]]] [exclusive-failover] | [vrf-srp-validate]**

no

Disables monitoring.

context *context_name*

Identifies the context being used. *context_name* must be an existing context expressed as an alphanumeric string of 1 through 79 characters.

ipv4_address | *ipv6_address*

Specifies the IP address of the BGP peer to be monitored in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

group *group_id*

Defines a Service Redundancy Protocol (SRP) peer group as an integer from 0 through 9. Default = 0.

In an Interchassis Session Recovery (ICSR) configuration, failover would occur if all peers within a group fail (instead of all BGP peers in a context). This option is useful in deployments in which a combination of IPv4 and IPv6 peers are spread across multiple paired VLANs and IPv4 or IPv6 connectivity is lost by all members of a peer group.

vrf *vrf_name*

Defines the VPN Routing/Forwarding instance as an alphanumeric string of 1 through 63 characters.

exclusive-failover

Flags BGP monitor failure on a single BGP peer failure.

On implementing this keyword, the behavior is as follows:

- BGP peer group is Up if any BGP peer in that group is Up.
- Including a BGP peer in group 0 is same as making it non-group (omitting group).
- BGP monitor is down if any BGP peer group or any non-group BGP peer is down.

vrf-srp-validate

Enables SRP validation for BGP VRF configuration.

Usage Guidelines

This command initiates monitoring of the connection between the primary chassis and the specified BGP peer in the specified context. If the connection drops, the standby chassis becomes active.

Example

The following example initiates the connection monitoring between the primary chassis and BGP peer *125.2.1.56*:

```
monitor bgp context test 125.2.1.56
```

monitor diameter

Enables SRP monitoring of the connection between the specified Diameter server and the primary chassis.

Product

All products supporting ICSR

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Service Redundancy Protocol Configuration

configure > context *context_name* **> service-redundancy-protocol**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-srp)#
```

Syntax Description

[no] monitor diameter context *context_name* **endpoint** *endpoint_name* **[fqdn** *fqdn* **| group** *group_id* **| peer {** *ipv4_address* **|** *ipv6_address* **}] [port** *port_number* **]**

no

Turns off the monitoring.

context *context_name*

Identifies the context being used. *context_name* must be an existing context expressed as an alphanumeric string of 1 through 79 characters.

endpoint *endpoint_name*

Identifies the endpoint being used. *endpoint_name* must be for the Diameter server expressed as an alphanumeric string of 1 through 63 characters.

fqdn *fqdn*

Identifies a Fully Qualified Domain Name (FQDN). *fqdn* must be for the Diameter server expressed an alphanumeric string of 1 through 127 characters.

group *group_id*

Defines a Service Redundancy Protocol (SRP) peer group as an integer from 0 through 9. Default = 0.

In an Interchassis Session Recovery (ICSR) configuration, failover would occur if all peers within the specified group fail.

peer { *ipv4_address* | *ipv6_address* }

Defines the IP address of the Diameter server to be monitored, entered using IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

port *port_number*

Identifies a specific port to monitor. *port_number* must be the port for the Diameter server and an integer from 1 through 65535.

Usage Guidelines

This command initiates monitoring of the connection between the primary chassis and the specified Diameter server in the specified context. If the connection drops, the standby chassis becomes active.

Important Endpoint name, FQDN, IP address, and port must all match the Diameter protocol configured values for the peer state to be updated.

Example

The following example initiates the connection monitoring between the primary chassis and the Diameter server on context *test1* and endpoint *end2*:

```
monitor diameter context test1 10.6.7.8 endpoint end2
```

monitor hsrp

Enables monitoring of the Hot Standby Router Protocol (HSRP) connection between the ASR 9000 Route Switch Processor (RSP) and the StarOS Security Gateway (SecGW) running in a virtual machine on the Virtualized Services Module. HSRP is employed in high availability (HA) SecGW configurations. (ASR 9000 VSM only)

Product

SecGW

Privilege

System Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Service Redundancy Protocol Configuration

configure > context *context_name* **> service-redundancy-protocol**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-srp)#
```

Syntax Description

monitor hsrp interface *if_name* **afi-type** *type* **hsrp-group** *hsrp_group*
no monitor hsrp

no

Turns off the monitoring.

interface *if_name*

Specifies the name of an existing RSP interface as an alphanumeric string of 1 through 63 characters.

afi-type *type*

Specifies the RSP name of an existing Address Family Type (IPv4 or IPv6) as an alphanumeric string of 4 through 15 characters.

hsrp-group *hsrp_group*

Specifies the RSP name of an existing HSRP Group ID as an integer from 0 through 4095.

Usage Guidelines

Use this command to enable monitoring of the HSRP connection between the ASR 9000 RSP and the SecGW running in a virtual machine on the VSM.

This command must be associated with the Service Redundancy Protocol (SRP) context.

A maximum of one HSRP monitor is supported per VPC-VSM instance.



Important The above parameters must match those of the HSRP configuration in the ASR 9000 RSP.

Example

The following command enables monitoring of Cisco HSRP on an ASR 9000 VSM running SecGW in a virtual machine:

```
monitor hsrp interface GigabitEthernet0/1/0/3 afi-type ipv4 hsrp-group 2
```

monitor sx

Enables or disables Sx monitoring on the Active UP and Standby UP.

Product

All products supporting ICSR

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Service Redundancy Protocol Configuration

configure > context *context_name* **> service-redundancy-protocol**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-srp)#
```

Syntax Description

`[ no ] monitor sx [ { context` *`context_name`* **`| bind-address {`***`ipv4_address`* **`|`***`ipv6_address`* **`} | { peer-address {`***`ipv4_address`* **`|`** *`ipv6_address`* **`} } ] | [ disallow-switchover-on-peer-monitor-fail [ timeout`** *`seconds`***`] ]`**

no

Disables monitoring.

context *context_name*

Specifies the context of the Sx service. *context_name* must be an existing context expressed as an alphanumeric string of 1 through 79 characters.

bind-address {*ipv4 _address* | *ipv6_address*}

Defines the service IP address of the Sx service entered using IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

peer-address {*ipv4 _address* | *ipv6_address*}

Defines the service IP address of the Sx service entered using IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

disallow-switchover-on-peer-monitor-fail [timeout *seconds*]

Prevents the switchback of the UP to Active state when the working status of the UP to CP link is unknown.

timeout *seconds*: Timeout after which the switchback is allowed even if the Sx failure status is not reset in the Standby peer. The valid values range from 0 to 2073600 (24 days).

Note Assigning 0 seconds as the the timeout allows unplanned switchover.

If **timeout** keyword is not specified, the Active chassis waits indefinitely for the Sx failure status to be reset in the Standby peer.

The default configuration is to allow unplanned switchover due to Sx monitor failure in all conditions.

Usage Guidelines This command enables or disables Sx monitoring on the Active UP and Standby UP.

monitor system

Enables or disables failure monitoring on the VPC-DI system.

Product All products supporting ICSR

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > Service Redundancy Protocol Configuration

configure > context *context_name* **> service-redundancy-protocol**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-srp)#
```

Syntax Description

[no] monitor system card-fail

monitor system vpp delay-period *0-300 seconds*

no monitor system vpp

no

Disables card fault monitoring.

card-fail

Enables card failure monitoring on the VPC-DI system. When configured, the VPN monitor checks the card failure status to assess if it is feasible to trigger an ICSR switchover.

The following scenarios trigger an ICSR switchover on the VPC-DI platform:

- When any Active SF card fails without Standy card.
- During a planned SF card migration failure without a standby card available.

vpp delay-period { *0-300 seconds*}

Specifies the delay period in seconds for a switchover, after a VPP failure.

If the delay period is a value greater than zero, then the switchover is initiated after the specified delay period when VPP fails. The last VPP status notification within the delay period is the final trigger for switchover

action. The default value is 0 seconds. When the value is 0, there is an immediate switchover when VPP goes down.

The need for delay is to address the scenario wherein the VPP is temporarily down and the revival is in process. This implies that a switchover may not be necessary.

Usage Guidelines Use this command to enable or disable failure monitoring on the VPC-DI system.

This command is disabled by default.



Note This CLI command is *not* supported on the ASR 5500 or VPC-SI platforms. It is supported only on the VPC-DI platform.

Example

The following command enables card failure monitoring.

```
monitor system card-fail
```

num-internal-switchover-retry

Defines the number of times an internal switchover would be retried.

Product All products supporting ICSR

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > Service Redundancy Protocol Configuration

configure > context *context_name* **> service-redundancy-protocol**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-srp)#
```

Syntax Description

```
num-internal-switchover-retry retries
default num-internal-switchover-retry
```

default

Resets the configuration interval to the default setting of 3 retries.

retries

The number of times an internal switchover would be retried in case of standby chassis. *retries* must be an integer from 1 through 10.

Default: 3

Usage Guidelines This configures the number of times an internal switchover would be retried in case of standby chassis failure to respond or become active.

Example

The following example sets the retry number to *5*:

```
num-internal-switchover-retry 5
```

peer-ip-address

Specifies the IP address for the peer chassis.

Product

All products supporting ICSR

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Service Redundancy Protocol Configuration

configure > **context** *context_name* > **service-redundancy-protocol**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-srp)#
```

Syntax Description

```
peer-ip-address { ipv4_address | ipv6_address }
no peer-ip-address
```

no

Removes the peer IP address of the backup chassis.

ipv4_address | *ipv6_address*

Specifies the IP address of the backup chassis, entered using IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

Important Both peers must be using the same address family (IPv4 or IPv6) or the Service Redundancy Protocol (SRP) connection will not be established.

Usage Guidelines

This command is used to identify the peer chassis in the ICSR configuration. From the primary's perspective, the peer is the backup and from the backup's perspective, the peer is the primary.

Example

The following example specifies *10.2.3.4* as a backup peer system to the primary system:

```
peer-ip-address 10.2.3.4
```

priority

Sets the initial ICSR priority of each peer chassis.

Important **priority** takes affect only during simultaneous initializing of all chassis in an ICSR configuration, and only if a misconfiguration has both chassis in the same mode (both Primary or both Backup).

Product

All products supporting ICSR

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Service Redundancy Protocol Configuration

configure > context *context_name* **> service-redundancy-protocol**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-srp)#
```

Syntax Description

priority *priority_value*
default priority

default

Resets the priority to the default setting of 125.

priority_value

Specifies the priority for the chassis. *priority_value* must be an integer from 1 through 255, where 1 is the highest priority. Default = 125.

Usage Guidelines

This command determines which chassis transitions to the Active state when all chassis have the same mode configuration. **priority** acts as a tie breaker for the state determination only when all chassis initialize simultaneously. The chassis with the higher priority (lower number) becomes Active, while the chassis with the lower priority (higher number) becomes Standby.

Once chassis become operational (after initialization), if there is an event requiring a chassis change of state, then each chassis returns to its previous state (Active or Standby) after both chassis recover.

Example

The following example sets the priority value to 5:

```
priority 5
```

retain-complete-sess-info

The new CLI command is added to retain complete session information locally when transitioning to the Standby state during a switchover.

Product

P-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Service Redundancy Protocol Configuration

configure > context *context_name* **> service-redundancy-protocol**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-srp)#
```

Syntax Description

retain-complete-sess-info
[no] retain-complete-sess-info

no

Disables the command.

Usage Guidelines

The new CLI command is added to retain complete session information locally when transitioning to the Standby state during a switchover.

Example

The following command retains complete session information when transitioning from Active to Standby state during a switchover:

retain-complete-sess-info

route-modifier

Sets the route modifier for the peer chassis.

Product

All products supporting ICSR

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Service Redundancy Protocol Configuration

configure > context *context_name* **> service-redundancy-protocol**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-srp)#
```

Syntax Description

route-modifier threshold *threshold_value*
default route-modifier

default

Resets the route modifier to the default setting of 16.

threshold_value

Specifies the value that causes the route-modifier counter to be reset to the initial value. *threshold_value* must be an integer from 2 through 32. Default = 16.

Usage Guidelines

This command is used to determine when the route modifier should be reset to its initial value to avoid rollover.

Example

The following example sets the route modifier threshold to *10*:

```
route-modifier threshold 10
```

standby database-recovery

Configures the preferred method of SRP database synchronization on the Standby ICSR chassis.

Product

All products supporting ICSR

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Service Redundancy Protocol Configuration

configure > context *context_name* **> service-redundancy-protocol**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-srp)#
```

Syntax Description

```
standby database-recovery { aggressive | normal }
default standby database-recovery
```

default

Restore SRP database recovery method to normal

{ aggressive | normal }

The **normal** (default) method for synchronizing the SRP database requires tens of seconds of delay whenever the TCP connection between the Active and Standby session managers is established. Once the TCP connection is established, heart beat messages are exchanged between both ICSR chassis every 3 seconds. The standby chassis waits for 7 heart beat messages from the active chassis before it is ready to accept data. This causes the significant delay in session manager database synchronization on the standby chassis.

The **aggressive** method for synchronizing the session manager database reduces recovery time in the following scenarios:

- Standby Session Manager crash
- Packet processing card crash on Standby chassis

- Standby chassis crash/reboot
- Temporary loss and recovery of SRP connection

The **aggressive** method reduces the number of heartbeat messages and amount of housekeeping information exchanged between ICSR chassis.

Usage Guidelines Use this command to enable a more aggressive method for synchronizing the session manager database on a Standby ICSR chassis.

Example

The following command enables the aggressive method of session manager database recovery on a standby ICSR chassis:

```
standby database-recovery aggressive
```

switchover allow-all-data-traffic

Allows all data traffic (VoLTE and non-VoLTE) during switchover transition. This command overwrites the **switchover allow-volte-data-traffic** command if enabled on a P-GW.



Important A special ICSR license is required to run this command. Contact your Cisco account representative for additional information.

Product P-GW

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > Service Redundancy Protocol Configuration

configure > **context** *context_name* > **service-redundancy-protocol**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-srp)#
```

Syntax Description

```
switchover allow-all-data-traffic
no switchover allow-all-data-traffic
```

no

Disables this feature. The default behavior is to not allow data traffic during switchover.

Usage Guidelines Use this command to allow all data traffic (VoLTE and non-VoLTE) during an ICSR switchover. This feature reduces data traffic outage during the switchover.



Important This CLI command must be run on both the active and standby chassis to enable this feature.

All data traffic is allowed on the active chassis during flushing and internal auditing. The billing information is reconciled in the background once the flush is complete.

Example

The following command enables this feature:

```
switchover allow-all-data-traffic
```

switchover allow-early-active-transition

Enables or disables early transition to active state during an ICSR switchover. By default this feature is disabled.



Important A special ICSR license is required to run this command. Contact your Cisco account representative for additional information.



Important You must enable the **switchover allow-all-data-traffic** or **allow-volte-data-traffic** (without **maintain accounting**) command on both chassis prior to enabling this command.

Product

All products supporting ICSR

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Service Redundancy Protocol Configuration

configure > context *context_name* **> service-redundancy-protocol**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-srp)#
```

Syntax Description

```
switchover allow-early-active-transition
no switchover allow-early-active-transition
```

no

Disables early transition following an ICSR switchover.

Usage Guidelines

Use this command in conjunction with the **switchover allow-all-data-traffic** or **allow-volte-data-traffic** (without **maintain accounting**) command to further reduce data outage during a planned switchover. The outage window is the amount time between initiating an ICSR switchover and when the newly active chassis starts processing data.

Example

The following command enables this feature:

```
switchover allow-early-active-transition
```

switchover allow-volte-data-traffic

Allows VoLTE data traffic during ICSR switchover transition.

Important A special ICSR license is required to run this command. Contact your Cisco account representative for additional information.

Product

P-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Service Redundancy Protocol Configuration

configure > context *context_name* **> service-redundancy-protocol**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-srp)#
```

Syntax Description

```
switchover allow-volte-data-traffic [ maintain-accounting ]
```

[maintain-accounting]

When enabled this option maintains accounting accuracy for VoLTE calls.VoLTE data is allowed on the active chassis after VoLTE accounting statistics are flushed.

Usage Guidelines

Use this command to allow VoLTE data traffic during ICSR switchover transition. VoLTE data traffic is allowed on the active chassis during flushing and internal auditing. There may be some billing inaccuracy. Non-VoLTE data traffic is allowed after flushing and the internal audit are completed.

This feature is superseded when the **switchover allow-all-data- traffic** command is enabled.

Example

The following command enables this feature:

```
switchover allow-volte-data-traffic maintain-accounting
```

switchover control-outage-optimization

Optimizes restoration of control traffic (call-setup, modification, deletion) following an ICSR switchover.

Important A special ICSR license is required to run this command. Contact your Cisco account representative for additional information.

Product

All products supporting ICSR

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Service Redundancy Protocol Configuration

configure > context *context_name* **> service-redundancy-protocol**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-srp)#
```

Syntax Description

```
switchover control-outage-optimization
no switchover control-outage-optimization
```

no

Disables optimization for restoring control traffic following an ICSR switchover.

Usage Guidelines

Use this command to optimize restoration of control traffic following an ICSR switchover.

Example

The following command enables this feature:

```
switchover control-outage-optimization
```