High Availability Commands

clear secure-stackwise-virtual interface

To clear the Secure StackWise Virtual interface statistics counters, use the **clear secure-stackwise-virtual interface** command in privileged EXEC mode.

clear secure-stackwise-virtualinterface*interface-id*

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.x	This command was introduced.

Example:

The following example shows how to clear a Secure StackWise Virtual 40 Gigabit Ethernet interface:

```
Device# clear secure-stackwise-virtual interface fortyGigabitEthernet 1/0/10
```

debug secure-stackwise-virtual

To enable debugging of Secure StackWise Virtual , use the **debugsecure-stackwise-virtual** command in privileged EXEC mode.

To disable debugging, use the **undebug secure-stackwise-virtual** command.

debug secure-stackwise-virtual
undebug secure-stackwise-virtual

Command Default Debugging is disabled.

Command Modes Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.x	This command was introduced.

Example:

The following is a sample output of the **debugsecure-stackwise-virtual** command :

```
Device# debug secure-stackwise-virtual
Secure-SVL debugging is on
Switch#
```

The following is a sample output of the **undebugsecure-stackwise-virtual** command :

```
Device# undebug secure-stackwise-virtual
Secure-SVL debugging is off
Switch#
```

hw-module beacon

To control the blue beacon LED in a field-replaceable unit (FRU), use the **hw-module beacon** command in priviledged EXEC mode.

hw-module beacon {**RP** {**active** | **standby**} | **fan-tray** | **power-supply** *power-supply slot number* | **slot** *slot number*} {**off** | **on** | **status**}

Syntax Description

RP	Selects the route processorfor the selected switch.
fan-tray	Selects the fan for the selected switch.
power-supply *power-supply slot number*	Specifies the power supply slot number. Valid values are 1 to 4.
slot *slot-number*	Specifies the slot number. Valid values are 1 to 4.
off	Switches off the beacon LED for the route processor and the slot, and switches off the fan and the power supply for the selected switch.
on	Switches on the beacon LED for the route processor and the slot, and switches off the fan and the power supply for the selected switch.
status	Displays the beacon LED status for the route processor, fan-tray, power-supply slot, and slot for the selected switch.

Command Default

None

Command Modes

Priviledged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1	This command was introduced.

main-cpu

To enter the redundancy main configuration submode and enable the standby supervisor module, use the **main-cpu** command in redundancy configuration mode.

main-cpu

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Redundancy configuration (config-red)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1	This command was introduced.

Usage Guidelines

From the redundancy main configuration submode, use the **standby console enable** command to enable the standby supervisor module.

This example shows how to enter the redundancy main configuration submode and enable the standby supervisor module:

```
Device(config)# redundancy
Device(config-red)# main-cpu
Device(config-r-mc)# standby console enable
Device#
```

mode sso

To set the redundancy mode to stateful switchover (SSO), use the **mode sso** command in redundancy configuration mode.

mode sso

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Redundancy configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1	This command was introduced.

Usage Guidelines

The **mode sso** command can be entered only from within redundancy configuration mode.

Follow these guidelines when configuring your system to SSO mode:

- You must use identical Cisco IOS images on the supervisor modules to support SSO mode. Redundancy may not work due to differences between the Cisco IOS releases.
- If you perform an online insertion and removal (OIR) of the module, the switch resets during the stateful switchover and the port states are restarted only if the module is in a transient state (any state other than Ready).
- The forwarding information base (FIB) tables are cleared on a switchover. Routed traffic is interrupted until route tables reconverge.

This example shows how to set the redundancy mode to SSO:

```
Device(config)# redundancy
Device(config-red)# mode sso
Device(config-red)#
```

policy config-sync prc reload

To reload the standby supervisor module if a parser return code (PRC) failure occurs during configuration synchronization, use the **policy config-sync reload** command in redundancy configuration mode. To specify that the standby supervisor module is not reloaded if a parser return code (PRC) failure occurs, use the **no** form of this command.

policy config-sync {**bulk** | **lbl**} **prc reload**
no policy config-sync {**bulk** | **lbl**} **prc reload**

Syntax Description

bulk	Specifies bulk configuration mode.
lbl	Specifies line-by-line (lbl) configuration mode.

Command Default

The command is enabled by default.

Command Modes

Redundancy configuration (config-red)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1	This command was introduced.

This example shows how to specify that the standby supervisor module is not reloaded if a parser return code (PRC) failure occurs during configuration synchronization:

```
Device(config-red)# no policy config-sync bulk prc reload
```

redundancy

To enter redundancy configuration mode, use the **redundancy** command in global configuration mode.

redundancy

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1	This command was introduced.

Usage Guidelines

The redundancy configuration mode is used to enter the main CPU submode, which is used to enable the standby supervisor module.

To enter the main CPU submode, use the **main-cpu** command while in redundancy configuration mode.

From the main CPU submode, use the **standby console enable** command to enable the standby supervisor module.

Use the **exit** command to exit redundancy configuration mode.

This example shows how to enter redundancy configuration mode:

```
Device(config)# redundancy
Device(config-red)#
```

This example shows how to enter the main CPU submode:

```
Device(config)# redundancy
Device(config-red)# main-cpu
Device(config-r-mc)#
```

Related Commands

Command	Description
show redundancy	Displays redundancy facility information.

reload

To reload the entire system and to apply configuration changes, use the **reload** command in privileged EXEC mode.

reload [{ **/noverify** | **/verify** }] [{ **at** | **cancel** | **in** | **pause** | **reason** *reason* }]

Syntax Description

/noverify	(Optional) Specifies to not verify the file signature before the reload.
/verify	(Optional) Verifies the file signature before the reload.
at	(Optional) Specifies the time in hh:mm format for the reload to occur.
cancel	(Optional) Cancels the pending reload.
in	(Optional) Specifies a time interval for reloads to occur.
pause	(Optional) Pauses the reload.
reason *reason*	(Optional) Specifies the reason for reloading the system.

Command Default

Immediately reloads the entire system and configuration change come into effect.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1	This command was introduced.

Examples

The following example shows the reload of the active system on a Catalyst 9600 Series Switches with StackWise Virtual:

```
Device# reload
System configuration has been modified. Save? [yes/no]: yes
Reload command is being issued on Active unit, this will reload the whole stack
Proceed with reload? [confirm] yes

*Jan 17 08:49:38.035: %SYS-5-RELOAD: Reload requested by console. Reload Reason: Reload
Command.
 Jan 17 08:49:50.023: %PMAN-5-EXITACTION: B0/0: pvp: Process manager is exiting: process
exit with reload fru code
Jan 17 08:50:18.805: %PMAN-5-EXITACTION: R0/0: pvp: Process manager is exiting: process
exit with reload chassis code


Initializing Hardware...

Initializing Hardware......

System Bootstrap, Version 17.7.1r[FC3], RELEASE SOFTWARE (P)
Compiled Thu Oct 28 00:16:50 2021 by rel
```

```
Current ROMMON image : Primary Rommon Image
```

secure-stackwise-virtual authorization-key 128-bits

To configure the Secure StackWise Virtual authorization key, use the **secure-stackwise-virtual authorization-key 128-bits** command in global configuration mode.

To remove the authorization key on all nodes, use the **no**form of this command.

secure-stackwise-virtual authorization-key 128-bits
nosecure-stackwise-virtual authorization-key 128-bits

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.x	This command was introduced.

Usage Guidelines

The StackWise Virtual authorization key must be configured individually on all stack members before they join the stack.

The same authorization key must be set on all members of the stack.

The **nosecure-stackwise-virtualauthorization-key** command will remove the authorization key without zeroizing it. You must remove the authorization key from all members of the stack

Example:

The following is a sample output of the **secure-stackwise-virtual authorization-key 128-bits** command.

```
Device(config)#secure-stackwise-virtual authorization-key 128-bits
Device(config)#$ual authorization-key FACEFACEFACEFACEFACEFACEFACEFACE
SECURE SVL key successfully set.
The stacking will run in SECURE SVL
mode after the reload. Make sure you set the
same secure-svl key on all the members of the stack.
nyq_SVL(config)#
```

secure-stackwise-virtual zeroize sha1-key

To zeroize the Secure StackWise Virtual SHA-1 key from the device, use the **secure-stackwise-virtual zeroize sha1-key** command in global configuration mode.

secure-stackwise-virtual zeroize sha1-key

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.x	This command was introduced.

Usage Guidelines

Note This command will zeroize the Secure StackWise Virtual SHA-1 key from the device by deleting the IOS image and configuration from the device by deleting the IOS image and configuration files.

Example:

The following is a sample output of the **secure-stackwise-virtual zeroize sha1-key** command.

```
Device(config)#secure-stackwise-virtual zeroize sha1-key

**Critical Warning** - This command is irreversible and will zeroize the Secure-SVL-VPK by
 Deleting the IOS image and config files, please use extreme caution and confirm with Yes
on each of three
iterations to complete. The system will reboot after the command executes successfully
 Proceed ?? (yes/[no]): yes
 Proceed ?? (yes/[no]): yes
 Proceed with zeroization ?? (yes/[no]): yes

% Proceeding to zeroize image. "Reload" session to remove the loaded image.
*Dec 14 11:04:43.004: %SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Removing packages.conf
The configuration is reset and the system will now reboot
```

show redundancy

To display redundancy facility information, use the **show redundancy** command in privileged EXEC mode

show redundancy [{**clients** | **config-sync** | **counters** | **history** [{**reload** | **reverse**}] | {**clients** | **counters**} | **states** | **switchover history** [**domain default**]}]

Syntax Description

clients	(Optional) Displays information about the redundancy facility client.
config-sync	(Optional) Displays a configuration synchronization failure or the ignored mismatched command list (MCL).
counters	(Optional) Displays information about the redundancy facility counter.
history	(Optional) Displays a log of past status and related information for the redundancy facility.
history reload	(Optional) Displays a log of past reload information for the redundancy facility.
history reverse	(Optional) Displays a reverse log of past status and related information for the redundancy facility.
clients	Displays all redundancy facility clients in the specified secondary switch.
counters	Displays all counters in the specified standby switch.
states	(Optional) Displays information about the redundancy facility state, such as disabled, initialization, standby or active.
switchover history	(Optional) Displays information about the redundancy facility switchover history.
domain default	(Optional) Displays the default domain as the domain to display switchover history for.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1	This command was introduced.

This example shows how to display information about the redundancy facility:

```
Device# show redundancy

Redundant System Information :
------------------------------
       Available system uptime = 6 days, 5 hours, 28 minutes
Switchovers system experienced = 0
              Standby failures = 0
        Last switchover reason = none
```

```
                Hardware Mode = Duplex
    Configured Redundancy Mode = sso
     Operating Redundancy Mode = sso
              Maintenance Mode = Disabled
                Communications = Up

Current Processor Information :
-------------------------------
               Active Location = slot 5
        Current Software state = ACTIVE
       Uptime in current state = 6 days, 5 hours, 28 minutes
                 Image Version = Cisco IOS Software, Catalyst L3 Switch Software
(CAT9K_IOSXE),Experimental Version 16.x.x [S2C-build-v16x_throttle-4064-/
nobackup/mcpre/BLD-BLD_V16x_THROTTLE_LATEST 102]
Copyright (c) 1986-201x by Cisco Systems, Inc.
Compiled Mon 07-Oct-xx 03:57 by mcpre
                        BOOT = bootflash:packages.conf;
        Configuration register = 0x102

Peer Processor Information :
----------------------------
              Standby Location = slot 6
        Current Software state = STANDBY HOT
       Uptime in current state = 6 days, 5 hours, 25 minutes
                 Image Version = Cisco IOS Software, Catalyst L3 Switch Software
(CAT9K_IOSXE), Experimental Version 16.x.x [S2C-build-v16x_throttle-4064-/
nobackup/mcpre/BLD-BLD_V16x_THROTTLE_LATEST_20191007_000645 102]
Copyright (c) 1986-201x by Cisco Systems, Inc.
Compiled Mon 07-Oct-xx 03:57 by mcpre
                        BOOT = bootflash:packages.conf;
                  CONFIG_FILE =
        Configuration register = 0x102
Device#
```

This example shows how to display redundancy facility client information:

```
Device# show redundancy clients

Group ID =     1
     clientID = 29       clientSeq = 60       Redundancy Mode RF
     clientID = 139      clientSeq = 62       IfIndex
     clientID = 25       clientSeq = 71       CHKPT RF
     clientID = 10001    clientSeq = 85       QEMU Platform RF
     clientID = 77       clientSeq = 87       Event Manager
     clientID = 1340     clientSeq = 104      RP Platform RF
     clientID = 1501     clientSeq = 105      CWAN HA
     clientID = 78       clientSeq = 109      TSPTUN HA
     clientID = 305      clientSeq = 110      Multicast ISSU Consolidation RF
     clientID = 304      clientSeq = 111      IP multicast RF Client
     clientID = 22       clientSeq = 112      Network RF Client
     clientID = 88       clientSeq = 113      HSRP
     clientID = 114      clientSeq = 114      GLBP
     clientID = 225      clientSeq = 115      VRRP
     clientID = 4700     clientSeq = 118      COND_DEBUG RF
     clientID = 1341     clientSeq = 119      IOSXE DPIDX
     clientID = 1505     clientSeq = 120      IOSXE SPA TSM
     clientID = 75       clientSeq = 130      Tableid HA
     clientID = 501      clientSeq = 137      LAN-Switch VTP VLAN

<output truncated>
```

The output displays the following information:

- clientID displays the client's ID number.

- clientSeq displays the client's notification sequence number.
- Current redundancy facility state.

This example shows how to display the redundancy facility counter information:

```
Device# show redundancy counters

Redundancy Facility OMs
               comm link up = 0
             comm link down = 0

          invalid client tx = 0
          null tx by client = 0
                tx failures = 0
      tx msg length invalid = 0

      client not rxing msgs = 0
 rx peer msg routing errors = 0
           null peer msg rx = 0
         errored peer msg rx = 0

                 buffers tx = 135884
     tx buffers unavailable = 0
                 buffers rx = 135109
      buffer release errors = 0

 duplicate client registers = 0
  failed to register client = 0
       Invalid client syncs = 0

Device#
```

This example shows how to display redundancy facility history information:

```
Device# show redundancy history

00:00:04 client added: Redundancy Mode RF(29) seq=60
00:00:04 client added: IfIndex(139) seq=62
00:00:04 client added: CHKPT RF(25) seq=71
00:00:04 client added: QEMU Platform RF(10001) seq=85
00:00:04 client added: Event Manager(77) seq=87
00:00:04 client added: RP Platform RF(1340) seq=104
00:00:04 client added: CWAN HA(1501) seq=105
00:00:04 client added: Network RF Client(22) seq=112
00:00:04 client added: IOSXE SPA TSM(1505) seq=120
00:00:04 client added: LAN-Switch VTP VLAN(501) seq=137
00:00:04 client added: XDR RRP RF Client(71) seq=139
00:00:04 client added: CEF RRP RF Client(24) seq=140
00:00:04 client added: MFIB RRP RF Client(306) seq=150
00:00:04 client added: RFS RF(520) seq=163
00:00:04 client added: klib(33014) seq=167
00:00:04 client added: Config Sync RF client(5) seq=168
00:00:04 client added: NGWC FEC Rf client(10007) seq=173
00:00:04 client added: LAN-Switch Port Manager(502) seq=190
00:00:04 client added: Access Tunnel(530) seq=192
00:00:04 client added: Mac address Table Manager(519) seq=193
00:00:04 client added: DHCPC(100) seq=238
00:00:04 client added: DHCPD(101) seq=239
00:00:04 client added: SNMP RF Client(34) seq=251
00:00:04 client added: CWAN APS HA RF Client(1502) seq=252
00:00:04 client added: History RF Client(35) seq=261
```

```
<output truncated>
```

This example shows how to display information about the redundancy facility state:

```
Device# show redundancy states

       my state = 13 -ACTIVE
     peer state = 8  -STANDBY HOT
           Mode = Duplex
           Unit = Primary
        Unit ID = 5

Redundancy Mode (Operational) = sso
Redundancy Mode (Configured)  = sso
Redundancy State              = sso
     Maintenance Mode = Disabled
    Manual Swact = enabled
 Communications = Up

   client count = 115
 client_notification_TMR = 30000 milliseconds
           RF debug mask = 0x0

Device#
```

show redundancy config-sync

To display a configuration synchronization failure or the ignored mismatched command list (MCL), if any, use the **show redundancy config-sync** command in EXEC mode.

show redundancy config-sync {**failures** {**bem** | **mcl** | **prc**} | **ignored failures mcl**}

Syntax Description

failures	Displays MCL entries or best effort method (BEM)/Parser Return Code (PRC) failures.
bem	Displays a BEM failed command list, and forces the standby supervisor module to reboot.
mcl	Displays commands that exist in the switch's running configuration but are not supported by the image on the standby supervisor module, and forces the standby supervisor module to reboot.
prc	Displays a PRC failed command list and forces the standby supervisor module to reboot.
ignored failures mcl	Displays the ignored MCL failures.

Command Default

None

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1	This command was introduced.

Usage Guidelines

When two versions of Cisco IOS images are involved, the command sets supported by two images might differ. If any of those mismatched commands are executed on the active supervisor module, the standby supervisor module might not recognize those commands, which causes a configuration mismatch condition. If the syntax check for the command fails on the standby supervisor module during a bulk synchronization, the command is moved into the MCL and the standby supervisor module is reset. To display all the mismatched commands, use the **show redundancy config-sync failures mcl** command.

To clean the MCL, follow these steps:

1. Remove all mismatched commands from the active supervisor module's running configuration.
2. Revalidate the MCL with a modified running configuration by using the **redundancy config-sync validate mismatched-commands** command.
3. Reload the standby supervisor module.

Alternatively, you could ignore the MCL by following these steps:

1. Enter the **redundancy config-sync ignore mismatched-commands** command.

2. Reload the standby supervisor module; the system transitions to SSO mode.

Note If you ignore the mismatched commands, the out-of-synchronization configuration on the active supervisor module and the standby supervisor module still exists.

3. You can verify the ignored MCL with the **show redundancy config-sync ignored mcl** command.

Each command sets a return code in the action function that implements the command. This return code indicates whether or not the command successfully executes. The active supervisor module maintains the PRC after executing a command. The standby supervisor module executes the command and sends the PRC back to the active supervisor module. A PRC failure occurs if these two PRCs do not match. If a PRC error occurs at the standby supervisor module either during bulk synchronization or line-by-line (LBL) synchronization, the standby supervisor module is reset. To display all PRC failures, use the **show redundancy config-sync failures prc** command.

To display best effort method (BEM) errors, use the **show redundancy config-sync failures bem** command.

This example shows how to display the BEM failures:

```
Device> show redundancy config-sync failures bem
BEM Failed Command List
-----------------------

 The list is Empty
```

This example shows how to display the MCL failures:

```
Device> show redundancy config-sync failures mcl
Mismatched Command List
-----------------------

The list is Empty
```

This example shows how to display the PRC failures:

```
Device# show redundancy config-sync failures prc
PRC Failed Command List
-----------------------

 The list is Empty
```

show secure-stackwise-virtual

To view your Secure StackWise Virtual configuration information, use the **showsecure-stackwise-virtual** command in in privileged EXEC mode.

show secure stackwise-virtual { **authorization-key** | **interface***interface-id* | **status**

Syntax Description

authorization-key	Displays the Secure StackWise Virtual authorization key installed on the device.
interface *interface-id*	Displays the Secure StackWise Virtual interface statistics.
status	Displays the Secure StackWise Virtual status of the device.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.x	This command was introduced.

Example:

The following is a sample output of the **show secure-stackwise-virtual authorization key** command

```
Device# show secure-stackwise-virtual authorization-key
SECURE-SVL: Stored key (16) : FACEFACEFACEFACEFACEFACEFACEFACE
```

The following is a sample output of the **show secure-stackwise-virtual interface**command

```
Device# show secure-stackwise-virtual interface fortyGigabitEthernet 1/0/10
Secure-SVL is enabled
  Replay protect       : Strict
  Replay window      : 0
  Cipher                     : GCM-AES-XPN-128
  Session Number    : 0
  Number of Rekeys : 0

 Transmit Secure-SVL Channel
   Encrypt Pkts                      : 80245
   Cumulative Encrypt Pkts : 80245

Receive Secure-SVL Channel
   Valid Pkts                        : 80927
   Invalid Pkts                     : 0
   Delay Pkts                       : 0
   Cumulative Valid Pkts   : 80927

 Port Statistics
   Egress untag pkts    : 0
   Ingress untag pkts   : 0
   Ingress notag pkts   : 0
```

```
   Ingress badtag pkts : 0
   Ingress noSCI pkts   : 0
```

The following is the sample output of the **show secure-stackwise-virtual status** command.

```
Device# show secure-stackwise-virtual status
Switch is running in SECURE-SVL mode
```

standby console enable

To enable access to the standby console supervisor module, use the **standby console enable** command in redundancy main configuration submode. To disable access to the standby console supervisor module, use the **no** form of this command.

standby console enable
no standby console enable

Syntax Description

This command has no arguments or keywords.

Command Default

Access to the standby console supervisor module is disabled.

Command Modes

Redundancy main configuration submode

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1	This command was introduced.

Usage Guidelines

This command is used to collect and review specific data about the standby console. The command is useful primarily for Cisco technical support representatives troubleshooting the device.

This example shows how to enter the redundancy main configuration submode and enable access to the standby console supervisor module:

```
Device(config)# redundancy
Device(config-red)# main-cpu
Device(config-r-mc)# standby console enable
Device(config-r-mc)#
```