Interchassis High Availability

The Interchassis High Availability feature provides geographically dispersed multibox redundancy. The unified session border controller (SBC) and the distributed SBC support the box-to-box high availability.

Interchassis High Availability feature is supported by the Cisco ASR 1001 Series Routers, Cisco ASR 1002 Series Routers, Cisco ASR 1004 Series Routers, Cisco ASR 1006 Series Routers, and Cisco ASR 1013 Series Routers.

Cisco Unified Border Element (SP Edition) was earlier known as Integrated Session Border Controller. It is referred to in this document as the session border controller (SBC).

For a complete description of the commands used in this chapter, refer to the *Cisco Unified Border Element (SP Edition) Command Reference: Unified Model* at:

http://www.cisco.com/en/US/docs/ios/sbc/command/reference/sbcu_book.html

For information about all the Cisco IOS commands, use the Command Lookup Tool at http://tools.cisco.com/Support/CLILookup or a Cisco IOS master commands list.

Feature History for Interchassis High Availability

Release	Modification
Cisco IOS XE Release 3.2S	This feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
Cisco IOS XE Release 3.3S	Added support information pertaining to the Cisco ASR 1006 Series Router, Cisco ASR 1013 Series Router, and interchassis-intrachassis conversion.
Cisco IOS XE Release 3.7S	Added information about upgrading interchassis redundancy.

Contents

This module contains the following sections:

Prerequisites for Interchassis High Availability

Following are the prerequisites pertaining to the Interchassis High Availability feature:

- The interfaces shared by the SBC must have the same redundant interface identifier (RII).
- The active device and the standby device must have the same peripheral configuration as the SBC features such as the SBC interfaces, virtual routing and forwarding (VRF), routes, sbc redundancy groups, and so on. The SBC-specific configuration will be replicated to the standby. Therefore, only the active Cisco ASR 1000 Series Router requires the full SBC-specific configuration.
- The active device and the standby device must run on the identical version of the Cisco IOS XE software.
- The active device and the standby device must be connected through an L2 connection for the control path.
- The Embedded Service Processor must be the same on both the active and standby devices. RP's must also match and have similar physical port adapter configuration.
- Network Time Protocol (NTP) must be configured or the clock must be set identical on both Cisco ASR 1000 Series Routers to allow timestamps and call timers to match.
- The latency times must be minimal on all control and data links to prevent timeouts.
- Physically redundant links, such as Gigabit Ether Channel must be used for control and data path.

Restrictions for Interchassis High Availability

Following are the restrictions pertaining to the Interchassis High Availability feature:

- Clustering of more than two SBCs for redundancy is not supported.
- The failover time for a box-to-box application is higher for a non-box-to-box application.
- LAN and MESH scenarios are not supported.
- If a dual IOS daemon is configured, the device does not support the interchassis high availability configuration.
- Only the SBC Active-Standby mode is supported.
- The SBC interfaces must be used for signaling and media addresses. Physical interface IP addresses must not be used.
- VRF's must be defined in the same order on both active and standby routers for an accurate synchronization of the SBC data.
- When the configuration is replicated to the standby router, it is not committed to the startup configuration, it is in the running configuration. The user must execute the **write memory** command to commit changes on the standby router that have been synchronized from the active router.
- Coexistence of interchassis high availability and intrachassis high availability is not supported.
- In Cisco ASR 1001 Series Routers, Cisco ASR 1002 Series Routers, and Cisco ASR 1004 Series Routers, the interchassis redundancy is not supported with software redundancy.

- In Cisco ASR 1006 Series Routers and Cisco ASR 1013 Series Routers, interchassis redundancy is not supported with intrachassis redundancy. It is supported with a single RP and ESP in the chassis.
- When CUBE-SP is in inter-chassis redundancy mode, customer need to use **sync** command in the active box to sync the configuration file from active box to standby box so that the latest configuration of CUBE-SP will be synchronized in the running configuration file in the standby box.

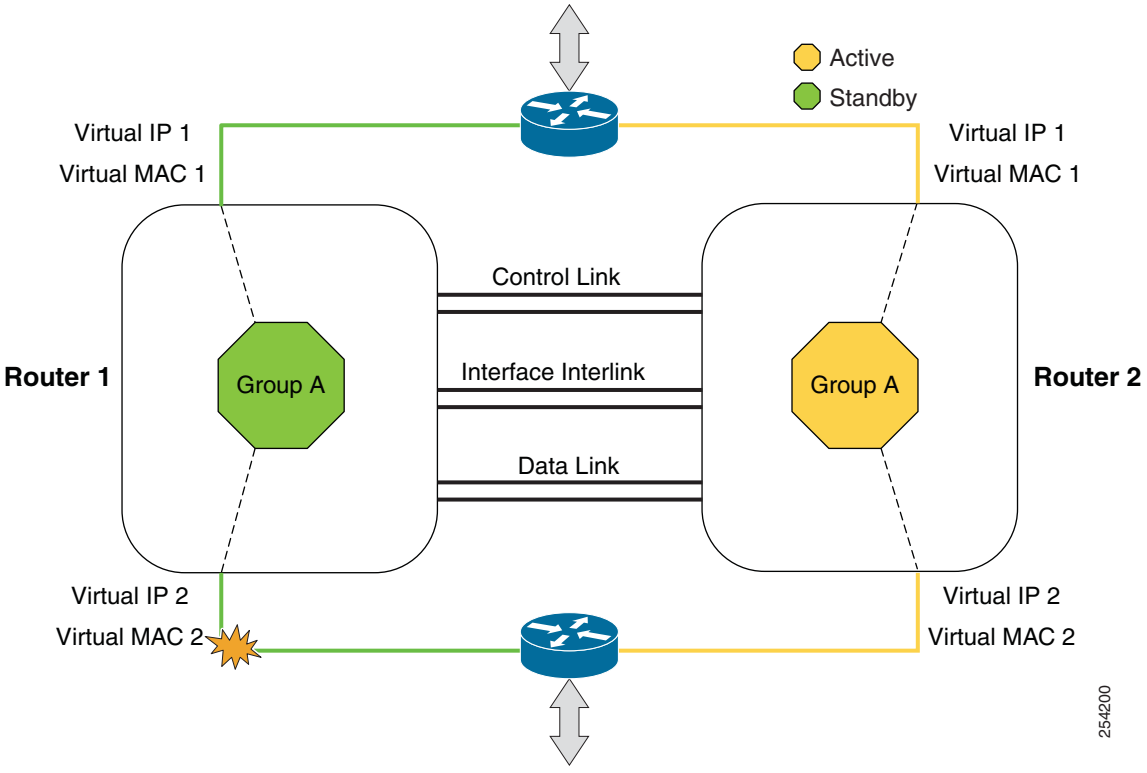
Information About Interchassis High Availability

The Interchassis High Availability feature enables the configuration of pairs of routers to act as backup for each other. This feature can be configured to determine the active router based on a number of failover conditions. When a failover occurs, the standby router seamlessly takes over and starts processing call signaling and performing media forwarding.

Groups of redundant interfaces are known as redundancy groups. Figure 15-1 depicts the active-standby device scenario. It shows how the redundancy group is configured for a pair of routers that have a single outgoing interface.

The routers are joined by a configurable control link and data synchronization link. The control link is used to communicate the status of the routers. The data synchronization link is used to transfer stateful information from the SBC, and to synchronize the stateful database for the calls and media flows. Each pair of redundant interfaces are configured with the same unique ID number, also known as the RII.

Figure 15-1 Redundancy Group Configuration



The status of the redundancy group members is determined through the use of Hello messages sent over the control link. If either of the routers do not respond to a Hello message within the configured amount of time, it is considered that a failure has occurred, and a switchover is initiated. To detect a failure in milliseconds, the control links run the failover protocol integrated with the Bidirectional Forwarding Detection (BFD) protocol. You can configure the following parameters for the Hello messages:

- Active timer
- Standby timer
- Hellotime–The interval at which Hello messages are sent.
- Holdtime–The amount of time before the active or the standby router is declared to be down.

The hellotime defaults to 3 seconds to align with the Hot Standby Router Protocol (HSRP), and the holdtime defaults to 10 seconds. You can also configure these timers in milliseconds by using the **timers hellotime msec** command.

Note B2B HA redundancy holdtime should be at least 3 seconds, and is recommended holdtime is 5 seconds.

Note If you allocate a large amount of memory, for example, 1 GB, to the log buffer, the CPU utilization and memory utilization of the router increases. This issue is compounded if you set small intervals for the hellotime and the holdtime. If you want to allocate a large amount of memory to the log buffer, we recommend that you accept the default values for the hellotime and holdtime. For the same reason, we also recommend that you do not use the **preempt** command.

To determine which pairs of interfaces are affected by the switchover, you must configure the RII for each pair of redundant interfaces.

Priority can be configured in the startup or running configuration, whereas the run-time priority is the priority of the router at any given time. The run-time priority can be similar to the configured priority if no decrements have been made, or it may be lowered based on the interface faults and decrements. The following priority factors can cause a switchover:

- The router with the highest priority value is the active router. If a fault occurs on either the active router or the standby router, the priority of the router is decremented by a configurable amount known as the decrement value. If the priority of the active router falls below the priority of the standby router, a switchover occurs, and the standby router becomes the active router. This default behavior can be overridden by disabling the preemption attribute for the redundancy group. You can also configure each interface to decrease the priority when the L1 state of the interface goes down. This amount overrides the default amount configured for the redundancy group.

  Note By default, preemption is not enabled. It can be enabled using the **preempt** command. When preemption is configured, the standby router initiates the failover. However, if you configure SBC on the router, we recommend that you do not use the **preempt** command. If the **preempt** command has been configured and if a failover occurs, the B2B state changes might not progress in a manner that permits a guaranteed amount of time for SBC synchronization.

  Each failure event that causes a modification of a redundancy group's priority generates a syslog entry that contains a time stamp, information about the redundancy group that was affected, the previous priority, the new priority, and a description of the failure event cause.

- When the priority of a router or interface falls below a configurable threshold level, the active router initiates the failover.

A switchover to the standby router can also occur under the following circumstances:

- Power loss or reload occurs on the active router, including crashes.
- The redundancy group on the active router is reloaded manually using the **redundancy application reload group rg-number self** command.

Two consecutive Hello messages that are missed on any monitored interface forces the interface into testing mode. When this occurs, both the units first verify the link status on the interface, and then execute the following tests:

- Network activity test
- ARP test
- Broadcast ping test

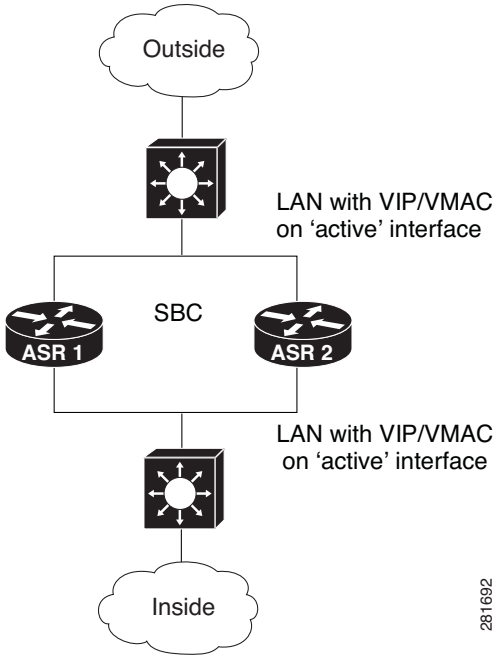
Exclusive Virtual IP and Exclusive Virtual MAC

Virtual IP (VIP) and Virtual MAC are used by the SBC application to control the interfaces that receive traffic. An interface on one device is paired with another interface on another device, and both the interfaces are associated with the same redundancy group. The interface that is associated with an active redundancy group exclusively *owns* the VIP Address and the Virtual MAC. The Address Resolution Protocol (ARP) process on that device sends ARP replies for ARP requests, if any, pertaining to the VIP, and the Ethernet controller for the interface is programmed to receive the packets destined for the Virtual MAC. When a redundancy group failover occurs, the *ownership* of the VIP and Virtual MAC changes. The interface associated with the newly active redundancy group sends a gratuitous ARP, and programs the interface's Ethernet controller to accept the packets destined for the Virtual MAC.

LAN-LAN Topology

The Interchassis High Availability feature supports the LAN-LAN topology. Figure 15-2 shows a LAN-LAN topology. Traffic is often directed to the SBC by configuring static routing in the upstream or downstream routers to an appropriate SBC interface IP address. In addition, the Cisco ASR 1000 Series Routers can participate in dynamic routing with either upstream or downstream routers. The dynamic routing configuration supported on the LAN-facing interfaces can introduce a dependency on routing protocol convergence, thus increasing the failover time.

Figure 15-2 LAN-LAN Topology



WAN-LAN Topology

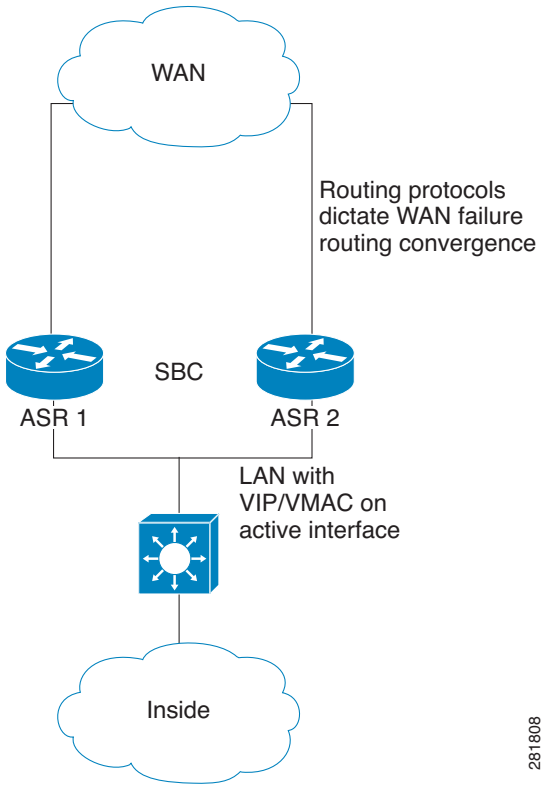
The Interchassis High Availability feature supports the WAN-LAN topology.

Note However, asymmetric routing is not supported in the Interchassis High Availability feature.

Figure 15-3 shows a WAN-LAN topology in which the LAN is similar to that present in the LAN-LAN topology. For the WAN, VIP is not required. The SBC interface network can be distributed on both the Cisco ASR 1000 Series Routers through dynamic routing. Routing protocols, such as OSPF, ISIS, and BGP, can run over the WAN links.

For a traffic failover caused by a WAN-facing router failure, the immediate WAN link or other WAN connectivity is dependent on the routing protocol convergence. Although subsecond failover cannot be achieved in these failure scenarios, fault detection can be minimized by tuning the routing protocol keep-alive timers and using the BFD feature, if available. Using the IOS Track feature and decreasing the redundancy group's priority values on the Cisco ASR 1000 Series Router to trigger failovers when the WAN links have failed, helps minimize the SBC downtime by failing over to a standby router with full connectivity.

Figure 15-3 WAN-LAN Topology



Transport by Redundancy Group and SBC

Redundancy group requires each client to establish a connection between the standby and active devices. The Cisco ASR 1000 Series Router platform implementation for box-to-box uses a connection between the standby and active routers using Stream Control Transmission Protocol (SCTP). This connection is used by the Redundancy Facility client to exchange the events and status used to keep the two boxes in synchronization. The platform also has an MCP client that uses a reliable User Datagram Protocol (UDP) connection for exchanging the platform-specific status and events.

The SBC has its own client, and uses a TCP connection for exchanging status, events, and replication data. These connections can be viewed using the **show redundancy application transport clients** command, and the details of the connections, ports, and IP addresses, can be viewed using the **show redundancy application group** command.

Interchassis-Intrachassis Conversion

From Cisco IOS XE Release 3.3S, Interchassis High Availability feature is also supported on Cisco ASR 1006 Series Routers and Cisco ASR 1013 Series Routers.

Intrachassis high availability occurs when the Cisco ASR 1000 Series Router has two routing processors (RP), with one RP in active mode and the other RP in standby mode. Interchassis high availability occurs when there are two Cisco ASR 1000 Series Router, with one router in active mode and the other in standby mode, and each router has one RP.

The following sections list the steps involved in high availability interchassis-intrachassis conversion:

- Intrachassis to Interchassis Conversion, page 15-8
- Interchassis to Intrachassis Conversion, page 15-10

Intrachassis to Interchassis Conversion

The following steps describe the procedure involved in dual RPs to single RP box-to-box conversion:

Step 1 Configure the Cisco ASR 1006 Series Router and Cisco ASR 1013 Series Router with dual RPs and dual forwarding processors (FPs) in the Stateful Switchover (SSO) mode.

Step 2 Configure the SBC functionality and generate test calls to ensure proper operation.

Step 3 Remove one RP and one FP from a box, using either OIR or CLI shutdown methods.

Step 4 Configure application redundancy:

```
Router(config)# interface GigabitEthernet0/1/1
Router(config-if)# redundancy rii 600
Router(config-if)# redundancy group 1 ip 10.2.3.4 exclusive decrement 200
Router(config-if)# exit
Router(config)# redundancy
Router(config-red)# application redundancy
Router(config-red-app)# group 1
Router(config-red-app-grp)# name SBC
Router(config-red-app-grp)# data GigabitEthernet 0/0/1
Router(config-red-app-grp)# control GigabitEthernet 0/0/2 protocol 1
Router(config-red-app-grp)# timers delay 100 reload 400
Router(config-red-app-grp)# track 1 decrement 1
Router(config-red-app-grp)# track 2 decrement 1
Router(config-red-app-grp)# exit
Router(config-red-app)# protocol 1
Router(config-red-app-prtcl)# name BFD
Router(config-red-app-prtcl)# timers hellotime 4 holdtime 6
Router(config-red-app-prtcl)# authentication md5 key-string 0 n1 100
```

Step 5 Add the SBC application redundancy configuration after the RG is shutdown:

```
Router(config)# redundancy
Router(config-red)# application redundancy
Router(config-red-app)# group 1
Router(config-red-app-grp)# name SBC
Router(config-red-app-grp)# shutdown
Router(config-red-app-grp)# exit
Router(config-red-app)# exit
Router(config-red)# exit
Router(config)# sbc redundancy-group 1 tcp
Router(config)# redundancy
Router(config-red)# application redundancy
Router(config-red-app)# group 1
```

```
Router(config-red-app-grp)# no shutdown
```

Step 6 Save the SBC configuration and use the **no sbc** command to remove the SBC configuration:

```
Router(config)# no sbc ASR1
```

Step 7 Check whether the Cisco ASR 1000 Series Router is in the ACTIVE mode or UNKNOWN mode because another Cisco ASR 1000 Series Router is not yet configured:

```
Router# show redundancy application transport group
```

Step 8 Configure the SBC again using the saved configuration.

```
Router(config)# sbc ASR1
```

Step 9 Place a test call to ensure that the SBC is functioning well.

Step 10 Bring the second Cisco ASR 1000 Series Router online with a single RP and single FP.

Step 11 Configure application redundancy on the second Cisco ASR 1000 Series Router:

```
Router(config)# interface GigabitEthernet0/1/1
Router(config-if)# redundancy group 1 ip 10.1.1.1 exclusive decrement 50
Router(config-if)# redundancy rii 10
Router(config-if)# exit
Router(config)# redundancy
Router(config-red)# application redundancy
Router(config-red-app)# group 1
Router(config-red-app-grp)# name SBC
Router(config-red-app-grp)# data GigabitEthernet 1/0/1
Router(config-red-app-grp)# control GigabitEthernet 0/0/1 protocol 1
Router(config-red-app-grp)# timers delay 100 reload 400
Router(config-red-app-grp)# track 1 decrement 1
Router(config-red-app-grp)# track 2 decrement 1
Router(config-red-app-grp)# exit
Router(config-red-app)# protocol 1
Router(config-red-app-prtcl)# name BFD
Router(config-red-app-prtcl)# timers hellotime 4 holdtime 6
Router(config-red-app-prtcl)# authentication md5 key-string 0 n1 100
```

Step 12 Add the SBC application redundancy configuration to the second Cisco ASR 1000 Series Router after the RG is shut down:

```
Router(config)# redundancy
Router(config-red)# application redundancy
Router(config-red-app)# group 1
Router(config-red-app-grp)# name SBC
Router(config-red-app-grp)# shutdown
Router(config-red-app-grp)# exit
Router(config-red-app)# exit
Router(config-red)# exit
Router(config)# sbc redundancy-group 1 tcp
Router(config)# redundancy
Router(config-red)# application redundancy
Router(config-red-app)# group 1
Router(config-red-app-grp)# no shutdown
```

Step 13 Configure the second Cisco ASR 1000 Series Router such that it is in the STANDBY HOT mode:

```
Router# show redundancy application transport group
```

Step 14 Check whether the first Cisco ASR 1000 Series Router is still in the ACTIVE mode:

```
Router# show redundancy application transport group
```

Step 15 Check whether the SBC configuration is synchronized to the Cisco ASR 1000 Series Router that is in the STANDBY mode:

```
Router# show run
```

Step 16 Place a test call to check whether the SBC is still functioning.

Interchassis to Intrachassis Conversion

The following steps describe the procedure involved in single RP box-to-box to dual RPs conversion:

Step 1 Configure two Cisco ASR 1000 Series Routers with single RP's and single FP's in the box-to-box mode.

Step 2 Generate test calls with multiple failovers to ensure proper box-to-box operation.

Step 3 Shut the RG on both the Cisco ASR 1000 Series Routers:

```
Router(config)# redundancy
Router(config-red)# application redundancy
Router(config-red-app)# group 1
Router(config-red-app-grp)# shutdown
```

Step 4 Remove the SBC redundancy configuration from both the Cisco ASR 1000 Series Routers:

```
Router (config)# no sbc redundancy-group 1 tcp
```

Step 5 Remove the RG configuration from both the Cisco ASR 1000 Series Routers:

```
Router(config-red)# no application redundancy
```

Step 6 Save the SBC configuration, and use the **no sbc** command to remove the SBC configuration:

```
Router(config)# no sbc ASR1
```

Step 7 Add one RP and one FP to the Cisco ASR 1000 Series Router that is in the ACTIVE mode.

Step 8 Configure the SBC again using the saved configuration:

```
Router(config)# sbc ASR1
```

Step 9 Check whether the SBC application of the primary Cisco ASR 1000 Series Router has been activated and is functioning correctly:

```
Router# show redundancy application transport group
```

Step 10 Generate test calls to verify whether the SBC is functioning, and leave this call active in order to be able to perform the subsequent steps.

Step 11 Configure the SSO redundancy:

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

Step 12 Check whether the configuration is synchronized and there are no interruptions in the SBC traffic:

```
Router# show run
```

Step 13 Place a test call to ensure that the SBC is still functioning.

Configuring Interchassis High Availability

To configure Interchassis High Availability, see the following sections in the "Configuring Firewall Stateful Inter-Chassis Redundancy" chapter of *Security Configuration Guide: Zone-Based Policy Firewall Cisco IOS XE Release 3S*:

http://www.cisco.com/en/US/partner/docs/ios-xml/ios/sec_data_zbf/configuration/xe-3s/sec-data-zbf-xe-book.html

This chapter provides information about the following topics:

- Configuring the Redundancy Application Group
- Configuring the Redundancy Group Protocol
- Configuring Virtual IP Address and Redundant Interface Identifier
- Configuring Control and Data Interface

Configuring Static Routing with Interchassis High Availability

When a static route is used in an upstream and downstream router or Layer 3 switch, VIP must be configured on the LAN-facing interface on the Cisco ASR 1000 Series Router. The static route that has an SBC interface IP address as the destination IP address sets the VIP address as the next hop address. Although this scenario offers the best convergence time during a failover, it faces an unicast flooding problem in the LAN between the router or the Layer 3 switch and the Cisco ASR 1000 Series Router.

The default ARP table aging time is 4 hours, while the MAC table aging time is only a couple of minutes. A MAC aging timer, which is greater or equal to the ARP timeout, is required to prevent unicast flooding for both upstream LAN and downstream LAN. After the ARP table is timed out, it sends an ARP request towards the VIP. The active Cisco ASR 1000 Series Router replies to the ARP request with a VMAC. The MAC table is refreshed and the unicast flooding problem is resolved.

To increase the MAC aging timer or decrease the ARP aging timer for the VLAN with the unicast flooding problem, use one of the following commands on the router or the Layer 3 switch:

- The **arp timeout** command on a VLAN interface
- The **mac-address-table aging-time vlan** command

Configuring Dynamic Routing with Interchassis High Availability

The SBC interface must be included as part of the Open Shortest Path First (OSPF) area so that the SBC is advertised when the box becomes active. The following example shows an OSPF configuration, illustrating the SBC box-to-box application with routing:

```
router ospf 200
 router-id 4.4.4.10
 priority 11
 nsf
 network 4.4.0.0 0.0.255.255 area 0

interface SBC1
 ip address 10.2.0.1 255.255.255.0 secondary
 ip address 10.2.0.10 255.255.255.0 secondary
 ip address 10.2.0.100 255.255.255.0
 ip ospf 200 area 0
```

Note To prevent duplicate IP addresses, the SBC interface is held in a down/down state on the standby router.

Assigning a Redundancy Group to the SBC

This task shows how to assign a redundancy group to the SBC:

Note Configuration on the SBC interface is similar on both active and standby routers. However, redundancy group traffic interfaces have different IP addresses and a shared redundancy IP address.
While performing this procedure on the Cisco ASR 1001 Router, Cisco ASR 1002 Router, and Cisco ASR 1004 Router, set the redundancy mode to **NONE**.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **redundancy**
4. **application redundancy**
5. **group** *id*
6. **shutdown**
7. **exit**
8. **exit**
9. **exit**
10. **sbc redundancy-group** ***group-number*** **tcp**
11. **redundancy**
12. **application redundancy**
13. **group** *id*
14. **no shutdown**
15. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enables the global configuration mode.

	Command or Action	Purpose
Step 3	**redundancy** **Example:** `Router(config)# redundancy`	Enters the redundancy configuration mode.
Step 4	**application redundancy** **Example:** `Router(config-red)# application redundancy`	Enters the redundancy application configuration mode.
Step 5	**group** *id* **Example:** `Router(config-red-app)# group 1`	Enters the redundancy application group configuration mode. • *id*—Specifies the redundancy group ID that ranges from 1 to 2.
Step 6	**shutdown** **Example:** `Router(config-red-app-grp)# shutdown`	To assign a redundancy group to the SBC, the redundancy group must be shut down.
Step 7	**exit** **Example:** `Router(config-red-app-grp)# exit`	Exits from the redundancy application group configuration mode and enters the redundancy application configuration mode.
Step 8	**exit** **Example:** `Router(config-red-app)# exit`	Exits from the redundancy application configuration mode and enters the redundancy configuration mode.
Step 9	**exit** **Example:** `Router(config-red)# exit`	Exits from the redundancy configuration mode and enters the global configuration mode.
Step 10	**sbc redundancy-group** *group-number* **tcp** **Example:** `Router(config)# sbc redundancy-group 1 tcp`	Assigns the redundancy group to the SBC in order to track the following: • *group-number*—Specifies the redundancy group number. • **tcp**—Specifies the Transmission Control Protocol TCP), and the redundancy group protocol.
Step 11	**redundancy** **Example:** `Router(config)# redundancy`	Enters the redundancy configuration mode.
Step 12	**application redundancy** **Example:** `Router(config-red)# application redundancy`	Enters the redundancy application configuration mode.

	Command or Action	Purpose
Step 13	**group** *id* **Example:** `Router(config-red-app)# group 1`	Enters the redundancy application group configuration mode: • *id*—Specifies the redundancy group ID that ranges from 1 to 2.
Step 14	**no shutdown** **Example:** `Router(config-red-app-grp)# no shutdown`	The redundancy group gets activated.
Step 15	**end** **Example:** `Router(config)# end`	Exits the redundancy application group configuration mode and enters the Privileged EXEC mode.

Managing and Monitoring Interchassis High Availability

You can manage and monitor the Interchassis High Availability feature as explained in the following sections:

- Managing and Monitoring the Redundancy Group infrastructure, page 15-14
- Managing and Monitoring an SBC Redundancy Group, page 15-15

Managing and Monitoring the Redundancy Group infrastructure

To manage and monitor the redundancy group infrastructure, use the following commands:

- **redundancy application reload group** *group-number* {**peer** | **self**}—Forces an active redundancy group to reload, and a standby redundancy group to become the active redundancy group, without affecting the status of the active redundancy group.
- **show redundancy application** {*group-id* | **all**}—Shows the summary information pertaining to the specified group or all the groups.
- **show redundancy application faults** {*group-id* | **all**}—Shows information about the faults pertaining to the specified group or all the groups.
- **show redundancy application if-mgr** {*group-id* | **all**}—Shows information about the if-mgr pertaining to the specified group or all the groups.
- **show redundancy application interface** *interface*—Shows the interface information associated with the redundancy groups.
- **show redundancy application protocol** *group-id*—Shows the protocol information pertaining to the specified group or all the groups.
- **show redundancy application transport** {*group-id* | **clients**}—Shows transport information pertaining to the specified group or all the groups.

To enable debug logging of the specified type of information associated with redundancy groups, use the following commands:

- **debug redundancy application vp** {**event** | **error**}
- **debug redundancy application transport** {**db** | **trace** | **event** | **error** | **timer**}

- **debug redundancy application media** {**packet** | **event** | **error** | **timer** | **nbr** | **all**}
- **debug redundancy application protocol** {**event** | **error** | **media** | **peer** | **detail** | **all**}
- **debug redundancy application faults** {**event** | **error** | **fault** | **func** | **db** | **all**}
- **debug platform software rg** {**tdl** | **terse** | **detail** | **error**}

Managing and Monitoring an SBC Redundancy Group

To manage and monitor an SBC redundancy group, use the following commands:

- **show sbc** *name* **rg transport**—Shows the transport information pertaining to an SBC redundancy group.
- **show sbc** *name* **rg statistics**—Shows the transport statistics pertaining to an SBC redundancy group.
- **clear sbc** *name* **rg**—Clears the SBC redundancy group box-to-box statistics.
- **monitor event-trace sbc ha—**Configures event tracing pertaining to the SBC in order to include significant redundancy group events for generating the history for bootup and transition logs to assist in debugging.

The following example shows a sample output of the **show sbc** *name* **rg transport** command:

```
Router# show sbc MySBC rg transport
SBC HA RG connection parameters for domain 2
--------------------------------------------
  Application Type        1
  Handler                 53
  My IP address           1.0.0.7
  My L4 Port              1060
  L3 Protocol             1
  L4 Protocol             1
  Peer IP address         1.0.0.6
  Peer L4 Port            1060
  My MTU                  1464
  My L4 Offset            28
```

The following example shows a sample output of the **show sbc** *name* **rg statistics** command:

```
Router# show sbc MySBC rg statistics
SBC HA B2B statistics
---------------------
Number of messages successfully queued           = 407
Number of messages successfully sent             = 407
Number of IPS messages sent                      = 370
Number of messages queue failures                = 0
Number of attempted-send message failures        = 0
Number of message header malloc failures         = 0
Number of no packet available failures           = 0
Number of high watermark of queued messages      = 16
Number of high watermark of recv messages        = 15

Number of messages received                      = 412
Number of received IPS messages                  = 356
Number of received messages discarded            = 0
Number of received messages dropped(no group)    = 0
Number of received large IPS messages            = 37
Number of large message send failures            = 0
Number of large message send total               = 0
Number of large message recv failures            = 0
Number of large message not sent, unsupp by peer = 0
```

The following example shows a sample output of the **show monitor event-trace sbc ha all** command. In this example, all the messages from the SBC high availability events are displayed:

```
Router# show monitor event-trace sbc ha all

*Jan 16 10:21:49.718: RF: Is Active, from boot = 0x1
*Jan 16 10:21:49.720: IPC: Initialised as master
*Jan 16 10:21:49.720: RF: Active reached, from boot = 0x1
*Jan 16 10:21:59.448: ILT: Registered on 48, result = 0x1
*Jan 16 10:21:59.448: RF: Start SM on 48
*Jan 16 10:49:02.523: IPC: Session to peer opened
*Jan 16 10:49:02.605: ISSU: Negotiation starting
*Jan 16 10:49:02.605: RF: Delaying progression at 300
*Jan 16 10:49:02.617: ISSU: Negotiation done
*Jan 16 10:49:02.617: RF: Negotiation result = 0x1
*Jan 16 10:49:02.617: RF: Peer state change, peer state = 0x1
*Jan 16 10:49:02.617: RF: Resuming progression at event 300
*Jan 16 10:50:00.853: ISSU: Transformed transmit message
*Jan 16 10:50:00.853: IPC: Queuing message type SBC_HA_MPF_CAPS_MSG_TYPE
*Jan 16 10:50:00.854: IPC: Queued message type SBC_HA_MPF_CAPS_MSG_TYPE
```

Upgrading Interchassis Redundancy

To upgrade interchassis redundancy, perform the following steps:

Note Two Cisco ASR1000 Series Aggregation Services Routers are required to perform this procedure. While the primary router is the active one, the secondary router is the standby one.

Step 1 In the primary router, use the **show redundancy application group** *RG Group ID* command to display which router is the active one.

Step 2 In the secondary router, use the **show redundancy application group** *RG Group ID* command to display which router is the standby one.

Step 3 Download the latest version of the Cisco ASR 1000 Series Aggregation Services Routers image to both the primary router and the secondary router.

Step 4 On the secondary router, change the boot variable to the new image by using the **boot system bootflash:** *new image* command.

Step 5 On the primary router, synchronize the SBC by using the **sbc** *sbc name* command and the **sync** command.

Wait for five minutes to make sure that the SBC configuration is fully synchronized to the standby router.

Step 6 On the secondary router, save the running configuration by using the **write memory** command.

Step 7 On the primary router, shut down the redundancy group.

The secondary router immediately becomes the active one, and all the active calls are preserved. Note that the router is still in service when switching over to the active router.

Step 8 On the primary router, change the boot variable to the new software image, and save the running configuration.

Step 9 Reload the primary router for upgrading, and wait for this router to come up with the upgraded version. It might take around 10 to 12 minutes from the time the router is reloaded.

Step 10 On the secondary router, shut down the redundancy and execute the **no shutdown** command for the redundancy group on the primary router as soon as possible.

Step 11 The router will be down for around 100 seconds, and the primary router becomes active and in service with the upgraded software.

Step 12 Save the running configuration in the primary router.

Step 13 Reload the secondary router for upgrade. When you are asked whether you want to save the configuration before proceeding with the reload, enter No so that the secondary router will come up in the standby state after the upgrade.

The upgrade is completed.

Configuration Examples for Interchassis High Availability

To view the list of configuration examples pertaining to Interchassis High Availability, see the following sections in the "Configuring Firewall Stateful Inter-Chassis Redundancy" chapter of *Security Configuration Guide: Zone-Based Policy Firewall Cisco IOS XE Release 3S* at:

http://www.cisco.com/en/US/partner/docs/ios-xml/ios/sec_data_zbf/configuration/xe-3s/sec-data-zbf-xe-book.html

- Example: Configuring the Redundancy Application Group
- Example: Configuring the Redundancy Group Protocol
- Example: Configuring Virtual IP Address and Redundant Interface Identifier
- Example: Configuring Control and Data Interface