High Availability on Cisco 4000 Series Integrated Services Routers

The High Availability (HA) feature allows you to benefit from the failover capability of Cisco Unified Border Element (Cisco UBE) on two routers, one active and one standby. When the active router goes down for any reason, the standby router takes over seamlessly, preserving and processing your calls.

Figure 1: Cisco UBE High Availability

- About Cisco UBE High Availability on Cisco 4000 Series ISR, on page 1
- How to Configure Cisco UBE High Availability on Cisco 4000 Series ISR, on page 5
- Verify Your Configuration, on page 11
- Troubleshoot High Availability Issues, on page 19

About Cisco UBE High Availability on Cisco 4000 Series ISR

Cisco UBE supports Box-to-box redundancy on Cisco 4000 Series Integrated Services Router (Cisco 4000 Series ISR) and uses Redundancy Group Infrastructure to provide High Availability.

Box-to-Box Redundancy

Box-to-box redundancy enables configuring a pair of routers to act as back up for each other. In the router pair, the active router is determined based on the failover conditions. The router pair continuously exchange status messages. Cisco UBE session information is checkpointed across the active and standby router. This enables the standby router to immediately take over all Cisco UBE call processing responsibilities when the active router becomes unavailable.
Redundancy Group (RG) Infrastructure

A group of redundant interfaces form a Redundancy Group. The active and standby routers are connected by a configurable control link and data synchronization link. The control link is used to communicate the redundancy state for each router. The data synchronization link is used to transfer stateful information to synchronize the stateful database for the calls and media flows. Each pair of redundant interfaces is configured with the same unique ID number, also known as the Redundancy Interface Identifier (RII).

A Virtual IP address (VIP) is configured on interfaces that connect to the external network. All signaling and media is sourced from and sent to the Virtual IP address. External devices such as Cisco Unified Communication Manager, uses VIP as the destination IP address for the calls traversing through Cisco UBE.

The following figure shows the redundancy group configured for a pair of routers with a single outgoing interface.

**Figure 2: Redundancy Group Configuration**

Network Topology

This section describes how to configure the following network topology, in which an active and standby pair of routers is used in a SIP trunk deployment between a Cisco Unified Communications Manager (Unified CM) and a service provider (SP) SIP trunk for PSTN access.
In this topology, both active and standby routers have the same configuration and both platforms are connected through a physical switch across same interfaces. This is required for Cisco UBE HA to work. For example, the CUBE-1 and CUBE-2 interface towards WAN must terminate on the same switch. Multiple interfaces or sub-interfaces can be used on either LAN or WAN side. Also, one Cisco UBE has a lower IP address across all three interfaces on the same Cisco UBE platform.

We recommend that you keep the following in mind when configuring this topology:

- Use a dedicated interface that is connected through a switch for checkpointing the RG control and data traffic across the two routers.
- A keepalive interface that is used for check-pointing RG control and data traffic must be in a different subnet or VLAN if the redundancy group ID is the same for the two different Cisco UBE HA pairs.
- You can configure a maximum of two redundancy groups. Hence, there can be only two active and standby pairs within the same network.
- Source all signaling and media from and to the Virtual IP address.
- Always save the running configuration to avoid losing it due to router reload during a failover.
- Virtual Routing and Forwarding
  - Define Virtual Router Forwarding (VRF) in the same order on both active and standby routers for an accurate synchronization of data.
  - You can configure VRFs only on Traffic interfaces (SIP and RTP). Do not configure VRF on RG Control and Data interface.
  - VRF configurations on both the active and standby router must be identical. VRF IDs are checkpointed for the calls before and after switchover (includes VRF-based RTP port range).
- Manually copy the configurations from one router to the other.
- When the configuration is replicated on the standby router, it is not committed to the startup configuration; it is in the running configuration. You must run the **write memory** command to commit the changes that are synchronized from the active router on the standby router.

**Considerations and Restrictions**

The following is a list of further considerations and restrictions you should know before configuring this topology:
Considerations

- Only active calls are checkpointed (Calls that are connected with 200 OK or ACK transaction completed).
- When you apply and save the configuration for the first time, the platform must be reloaded.
- For H.323, and TCP-based calls, media preservation is supported after the failover, but session signaling is not preserved.
- If you have Cisco Unified Customer Voice Portal (CVP) in your network, we recommend that you configure TCP session transport for the SIP trunk between CVP and Cisco UBE.
- Upon failover, the previously active Cisco UBE reloads by design.
- Cisco UBE uses the primary IP address to communicate Smart Licensing information.
- For SIP-SIP TLS calls (using Cisco IOS XE Release 3.11 or later), configure both the active and standby Cisco UBE as trust points to a common external CA Server.
- TCP sessions are not preserved during the failover. Remote user agents are expected to reestablish TCP sessions (using port 5060) before sending subsequent messages.
- Call Admission Control (CAC) continues to work after switchover. After stateful switchover, no calls are allowed if the CAC limit is reached before the switchover.
- Up to 6 multimedia lines in the SDP are checkpointed for Cisco UBE HA. From Cisco IOS XE Release 3.17 onwards, SDP Passthru (up to 2 m-lines) calls are also checkpointed.
- Survivability.tcl preservation is supported from Cisco IOS XE Release 3.17 onwards for Unified Customer Voice Portal (CVP) deployments.
- SRTP-RTP, SRTP-SRTP, and SRTP Passthru are supported.
- Port channel is supported for both RG control data and traffic interfaces only from Cisco IOS XE 16.3.1 onwards.

Figure 4: Additional Supported Options for Cisco UBE HA

- LTI-based transcoder call flow preservation is supported from Cisco IOS XE Release 3.15 onwards and requires same DSP module capacity on both active and standby in the same slot or subslot.
Restrictions

- IPv6 is not supported.
- All SCCP-based media resources (Conference bridge, Transcoding, Hardware MTP, and Software MTP) are not supported.
- Cisco Unified Survivable Remote Site Telephony (Unified SRST) or TDM Gateway co-location on Cisco UBE HA is not supported.
- Routers connected through Metropolitan Area Network (MAN) Ethernet regardless of latency are not supported.
- Out-of-band DTMF (Notify or KPML) is not supported post switchover. Only rtp-n te to rtp-n te and voice-inband to voice-inband DTMF works after the switchover.
- Media-flow around and UC Services API (Cisco Unified Communications Manager Network-Based Recording) are not supported.
- Signaling and media preservation are not supported over a crossover cable connection for the RG-control or data link.
- You cannot terminate Wide Area Network (WAN) on Cisco UBE directly or Data HA on either side. Both active and standby routers must be in the same Data Center and connected to the same physical switch.
- The Courtesy Callback (CCB) feature is not supported if a callback was registered with Cisco Unified Customer Voice Portal (CVP) and then a switchover was done on Cisco UBE.
- You cannot configure a secondary IP address for the interfaces.
- If the redundancy group ID is same for the two different Cisco UBE HA pairs, then the keepalive interface that is used for checkpointing RG control and data traffic must be in a different subnet or VLAN.
- Call Progress Analysis (CPA) calls (before transferred to the agent), SCCP-based media resources, Noise Reduction, Acoustic Shock Protection (ASP), and transrating calls are not supported.
- The failover time for a Box-to-box application is higher than the Inbox application.

How to Configure Cisco UBE High Availability on Cisco 4000 Series ISR

Before You Begin

- Use Cisco IOS-XE Release 3.11 and or later on both active and standby routers.
- Ensure that you have the required licenses for configuring high availability. For detailed information, see Cisco Unified Border Element Data Sheet.
- Connect the active and the standby router through a layer 2 connection for the control path.
Configure the Network Time Protocol (NTP) or set the clock to be identical on both active and standby 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 EtherChannel, must be used for the control and data paths.

**Configure High Availability**

**SUMMARY STEPS**

1. Configure the Redundancy Group (RG).
2. Configure interface tracking.
3. Configure the interfaces.
4. Configure SIP Binding.
5. (Optional) If H.323 calls are involved, enable H.323 binding.
6. Configure the Punt Policing feature.
7. Configure the RG group under voice service voip. This enables Box-to-box Cisco UBE HA.
8. Configure the Media Inactivity timer.
9. Reload the router.
10. Configure the peer router.
11. Point the attached devices to the Cisco UBE Virtual IP (VIP) address.

**DETAILED STEPS**

**Step 1** Configure the Redundancy Group (RG).

a) Enter application redundancy mode.

**Example:**

```
Router>enable
Router#configure terminal
Router(config)#redundancy
Router(config-r)#mode none
Router(config-red)#application redundancy
Router(config-red-app)#group 1
```

b) Configure a name for the redundancy group.

**Example:**

```
Router(config-red-app-grp)#name cube-ha
```

where `cube-ha` is the name of the redundancy group.

c) Specify the initial priority and failover threshold for a redundancy group.

**Example:**

```
Router(config-red-app-grp)#priority 100 failover threshold 75
```

where 100 is priority value and 75 is the threshold value. The router with highest priority and threshold value among the HA pair acts as the active router.
d) Configure the timers for delay and reload.

   **Example:**
   
   ```
   Router(config-red-app-grp)#timers delay 30 reload 60
   ```

   Delay timer which is the amount of time to delay the RG group’s initialization and role negotiation after the interface comes up.
   
   Default: 30 seconds. Range is 0-10000 seconds.

   Reload timer is the amount of time to delay RG group initialization and role-negotiation after a reload.
   
   Default: 60 seconds. Range is 0-10000 seconds.

e) Configure the interface used to exchange keepalive and hello messages between the router pair.

   **Example:**
   
   ```
   Router(config-red-app-grp)#control GigabitEthernet0/0/2 protocol 1
   ```

   where GigabitEthernet0/0/2 is the interface and protocol 1 is the protocol instance that is attached to the interface.

f) Configure the interface that is used for checkpointing of data traffic.

   **Example:**
   
   ```
   Router(config-red-app-grp)#data GigabitEthernet0/0/2
   ```

g) Configure RG group tracking.

   **Example:**
   
   ```
   Router(config-red-app-grp)#track 1 shutdown
   Router(config-red-app-grp)#track 2 shutdown
   ```

h) Specify the protocol instance that will be attached to a control interface and enters redundancy application protocol configuration mode.

   **Example:**
   
   ```
   Router(config-red-app-grp)#protocol 1
   ```

i) Configure the two timers for hellotime and holdtime.

   **Example:**
   
   ```
   Router(config-red-app-grp)#timers hellotime 3 holdtime 10
   ```

   hellotime—Interval between successive hello messages.
   
   Default is 3 seconds. Range is 250 milliseconds-254 seconds.

   holdtime—The interval between the receipt of a hello message and the presumption that the sending router has failed. This duration has to be greater than the hellotime.
   
   Default is 10 seconds. Range is 750 milliseconds-255 seconds.

   We recommend that you configure the holdtime timer configured to be at least 3 times the value of the hellotime timer.

**Step 2** Configure interface tracking.

The **track** command is used in RG to track the voice traffic interface state so that the active router initiates switchover after the traffic interface is down.

Configure the following commands at the global level to track the status of the interface.
Step 3  Configure the interfaces.

a) Configure the redundancy interface identifier for the redundancy group.

Required for generating a Virtual MAC (VMAC) address. You must use the same rii ID value on the interface of each router (active and standby) that has the same Virtual IP address.

If there is more than one Box-to-box HA pair on the same LAN, each pair MUST have unique rii IDs on their respective interfaces (to prevent collision). show redundancy application group all must indicate the correct local and peer information.

Example:

Router(config)#interface GigabitEthernet0/0/0
Router(config-if)#ip address 203.0.113.10 255.255.0.0
Router(config-if)#negotiation auto
Router(config-if)#redundancy rii 1

b) Associate the interface with the redundancy group created.

Example:

Router(config-if)#redundancy group 1 ip 203.0.113.12 exclusive

c) Configure interface for RG control and data.

Example:

Router(config)#interface GigabitEthernet0/0/2
Router(config-if)#ip address 192.51.100.1 255.255.255.0
Router(config-if)#media-type rj45
Router(config-if)#negotiation auto

Step 4  Configure SIP Binding.

Configure Cisco UBE to bind SIP messages to the interface that is configured with a Virtual IP address (VIP) for the RG group employed.

Example:

Router(config)#dial-peer voice 1 voip
Router(config-dial-peer)#session protocol sipv2
Router(config-dial-peer)#incoming called-number 2000
Router(config-dial-peer)#voice-class sip bind control source-interface GigabitEthernet0/0/0
Router(config-dial-peer)#voice-class sip bind media source-interface GigabitEthernet0/0/0
Router(config-dial-peer)#codec g711ulaw
Router(config-dial-peer)#!

Router(config)#dial-peer voice 2 voip
Router(config-dial-peer)#destination-pattern 2000
Router(config-dial-peer)#session protocol sipv2
Router(config-dial-peer)#session target ipv4:203.0.113.13
Router(config-dial-peer)#voice-class sip bind control source-interface GigabitEthernet0/0/1
Router(config-dial-peer)#voice-class sip bind media source-interface GigabitEthernet0/0/1
Router(config-dial-peer)#codec g711ulaw
**Step 5**  
(Optional) If H.323 calls are involved, enable H.323 binding.  
Under the interface used by H.323, configure voip-bind with its source address equal to the interface’s VIP for the RG group employed.

**Example:**

```
Router#voice service voip
Router(config-voi-serv)#h323
Router(config-serv-h323)#call preserve limit-media-detection
Router(config-serv-h323)#no h225 timeout keepalive

Router(config)#interface GigabitEthernet0/0/0
Router(config-if)#ip address 203.0.113.10 255.255.0.0
Router(config-if)#media-type rj45
Router(config-if)#negotiation auto
Router(config-if)#redundancy rii 1
Router(config-if)#redundancy group 1 ip 9.13.25.123 exclusive
Router(config-if)#h323-gateway voip interface
Router(config-if)#h323-gateway voip bind srcaddr 203.0.113.12

Router(config)#interface GigabitEthernet0/0/1
Router(config-if)#ip address 192.0.2.1 255.255.255.0
Router(config-if)#media-type rj45
Router(config-if)#negotiation auto
Router(config-if)#redundancy rii 2
Router(config-if)#redundancy group 1 ip 192.0.2.3 exclusive
Router(config-if)#h323-gateway voip interface
Router(config-if)#h323-gateway voip bind srcaddr 192.0.2.3
```

**Step 6**  
Configure the Punt Policing feature.

SIP packets towards the virtual IP address and physical IP address match different punt-cause codes. The punt-rate of the virtual IP address with a punt-cause of 60, is lower than the punt-rate of the physical IP address.

To ensure that the behaviour of the SIP packets towards virtual and physical IP address remains the same, you must increase the punt-rate of the virtual IP address by using the `platform punt-policer` command in global configuration mode.

**Example:**

```
Router(config)#platform punt-policer 60 40000
```

In the preceding example, the punt-rate of the virtual IP address (punt-cause 60) is increased from the default value of 2000 to 40000.

The following table provides details of the fields of the CLI.

<table>
<thead>
<tr>
<th><strong>Keyword</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><code>platform punt-policer</code></td>
<td>Configures the Punt Policing feature.</td>
</tr>
<tr>
<td><code>60</code></td>
<td><code>punt-cause</code>—Punt cause. Range is 1–107. Punt cause of the virtual interface is 60.</td>
</tr>
<tr>
<td><code>40000</code></td>
<td><code>punt-rate</code>—Rate limit in packets per second. Range is 10–146484.</td>
</tr>
</tbody>
</table>

**Note**  
The default punt rate value of the virtual IP address and the physical IP address varies with the router platform.
Step 7  Configure the RG group under **voice service voip**. This enables Box-to-box Cisco UBE HA.

**Example:**

```
Router#voice service voip
Router(conf-voi-serv)#redundancy-group 1
```

Step 8  Configure the Media Inactivity timer.

The Media Inactivity Timer enables the active and standby router pair to monitor and disconnect calls if no Real-Time Protocol (RTP) packets are received within a configurable time period.

For the SIP calls, the switched over calls are cleared with signaling (as signaling information is preserved for switched calls).

The Media Inactivity Timer releases TCP-based and H.323-based calls. This is used to guard against any hung sessions resulting from the failover when a normal call disconnect does not clear the call.

You must configure the same duration for the Media Inactivity Timer on both routers. The default value is 30 seconds for SIP and H.323 calls. The sample configuration is as follows:

**Example:**

```
Router(config)#ip rtcp report interval 9000
Router(config)#gateway
Router(config-gateway)#media-inactivity-criteria all
Router(config-gateway)#timer receive-rtp 1200
Router(config-gateway)#timer receive-rtcp 5
```

SIP and H.323 call legs are cleared once the RTCP timer expires.

Step 9  Reload the router.

Once all the preceding configurations are completed, you must save the configurations, and reload the router.

**Example:**

```
Router>enable
Router#reload
```

Step 10  Configure the peer router.

Follow the preceding steps to configure the standby router. Make sure that you use the correct IP addresses.

Step 11  Point the attached devices to the Cisco UBE Virtual IP (VIP) address.

The IP-PBX, Unified SIP Proxy, or service provider must route the calls to Cisco UBE’s Virtual IP address.

HA configuration does not handle SIP and H.323 messages to the Cisco UBE’s physical IP addresses.

For H.323 calls, you must disable the keepalive messages in Unified CM configuration.

a. Go to **System** menu, and choose **Service Parameters**. At the bottom of the Service Parameters, enable **Advanced**.

b. Set the **Allow TCP KeepAlives for H323** to False.

c. After this setting is saved, restart the CallManager Services.
Configuration Examples

Example: Control Interface Protocol Configuration

Router#configure terminal
Router(config)#redundancy
Router(config-red)#mode none
Router(config-red)#application redundancy
Router(config-red-app)#protocol 4
Router(config-red-app-prot)#name rgl
Router(config-red-app-prot)#timers hellotime 3 holdtime 10
Router(config-red-app-prot)#authentication text password

Example: Redundancy Group Protocol Configuration

Router#configure terminal
Router(config)#redundancy
Router(red)#application redundancy
Router(config-red-app)#protocol 1
Router(config-red-app-prtcl)#name RG1
Router(config-red-app-prtcl)#timers hellotime 1 holdtime 3
Router(config-red-app-prtcl)#end
Router#configure terminal
Router(config)#redundancy
Router(red)#application redundancy
Router(config-red-app)#protocol 2
Router(config-red-app-protcl)#name RG1
Router(config-red-app-protcl)#end

Example: Redundant Traffic Interface Configuration

Router#configure terminal
Router(config)#interface GigabitEthernet 0/0/2
Router(config-if)#ip address 198.51.100.1 255.0.0.0
Router(config-if)#ip nat outside
Router(config-if)#ip virtual-reassembly
Router(config-if)#negotiation auto
Router(config-if)#redundancy rii 200
Router(config-if)#redundancy group 1 ip 198.51.100.50 exclusive decrement 10

Verify Your Configuration

All configuration commands in this task are optional. You can use the `show` commands in any order.

SUMMARY STEPS

1. `show redundancy application group [group-id | all]`
2. `show redundancy application transport {clients | group [group-id]}`
3. `show redundancy application protocol {protocol-id | group [group-id]}`
4. `show redundancy application faults group [group-id]`
5. `show redundancy application if-mgr group [group-id]`
6. `show redundancy application control-interface group [group-id]`
7. `show redundancy application data-interface group [group-id]`

**DETAILED STEPS**

**Step 1**

`show redundancy application group [group-id | all]`

**Example:**

```
Router#show redundancy application group
Group ID Group Name State
-------- ---------- -----  
1        Generic-Redundancy-1 STANDBY
2        Generic-Redundancy2 ACTIVE
```

The following example shows the details of redundancy application group 1:

```
Router#show redundancy application group 1
Group ID:1
Group Name:Generic-Redundancy-1

Administrative State: No Shutdown
Aggregate operational state : Up
My Role: STANDBY
Peer Role: ACTIVE
Peer Presence: Yes
Peer Comm: Yes
Peer Progression Started: Yes

RF Domain: btob-one
RF state: STANDBY HOT
Peer RF state: ACTIVE
```

The following example shows the details of redundancy application group 2:

```
Router#show redundancy application group 2
Group ID:2
Group Name:Generic-Redundancy2

Administrative State: No Shutdown
Aggregate operational state : Up
My Role: ACTIVE
Peer Role: STANDBY
Peer Presence: Yes
Peer Comm: Yes
Peer Progression Started: Yes

RF Domain: btob-two
RF state: ACTIVE
Peer RF state: STANDBY HOT
```

**Step 2**

`show redundancy application transport {clients | group [group-id]}`

**Example:**

```
Router#show redundancy application transport client
Client Conn# Priority Interface L3 L4
( 0)RF 0 1 CTRL IPV4 SCTP
( 1)MCP_HA 1 1 DATA IPV4 UDP_REL
```
The following example shows configuration details for the redundancy application transport group:

Router#show redundancy application transport group

Transport Information for RG (1)
Client = RF
TI conn_id my_ip my_port peer_ip peer_por intf L3 L4
0 0 1.1.1.1 59000 1.1.1.2 59000 CTRL IPV4 SCTP
Client = MCP_HA
TI conn_id my_ip my_port peer_ip peer_por intf L3 L4
1 1 9.9.9.2 53000 9.9.9.1 53000 DATA IPV4 UDP_REL
Client = AR
TI conn_id my_ip my_port peer_ip peer_por intf L3 L4
2 0 0.0.0.0 0 0.0.0.0 0 NONE_IN NONE_L3 NONE_L4
Client = CF
TI conn_id my_ip my_port peer_ip peer_por intf L3 L4
3 0 9.9.9.2 59001 9.9.9.1 59001 DATA IPV4 SCTP

Transport Information for RG (2)
Client = RF
TI conn_id my_ip my_port peer_ip peer_por intf L3 L4
8 0 1.1.1.1 59004 1.1.1.2 59004 CTRL IPV4 SCTP
Client = MCP_HA
TI conn_id my_ip my_port peer_ip peer_por intf L3 L4
9 1 9.9.9.2 53002 9.9.9.1 53002 DATA IPV4 UDP_REL
Client = AR
TI conn_id my_ip my_port peer_ip peer_por intf L3 L4
10 0 0.0.0.0 0 0.0.0.0 0 NONE_IN NONE_L3 NONE_L4
Client = CF
TI conn_id my_ip my_port peer_ip peer_por intf L3 L4
11 0 9.9.9.2 59005 9.9.9.1 59005 DATA IPV4 SCTP

The following example shows the configuration details of redundancy application transport group 1:

Router#show redundancy application transport group 1

Transport Information for RG (1)
Client = RF
TI conn_id my_ip my_port peer_ip peer_por intf L3 L4
0 0 1.1.1.1 59000 1.1.1.2 59000 CTRL IPV4 SCTP
Client = MCP_HA
TI conn_id my_ip my_port peer_ip peer_por intf L3 L4
1 1 9.9.9.2 53000 9.9.9.1 53000 DATA IPV4 UDP_REL
Client = AR
TI conn_id my_ip my_port peer_ip peer_por intf L3 L4
2 0 0.0.0.0 0 0.0.0.0 0 NONE_IN NONE_L3 NONE_L4
Client = CF
TI conn_id my_ip my_port peer_ip peer_por intf L3 L4
3 0 9.9.9.2 59001 9.9.9.1 59001 DATA IPV4 SCTP

The following example shows configuration details of redundancy application transport group 2:

Router#show redundancy application transport group 2

Transport Information for RG (2)
Client = RF
TI conn_id my_ip my_port peer_ip peer_por intf L3 L4
8 0 1.1.1.1 59004 1.1.1.2 59004 CTRL IPV4 SCTP
Client = MCP_HA
TI conn_id my_ip my_port peer_ip peer_por intf L3 L4
9 1 9.9.9.2 53002 9.9.9.1 53002 DATA IPV4 UDP_REL
Client = AR
TI conn_id my_ip my_port peer_ip peer_por intf L3 L4
10 0 0.0.0.0 0 0.0.0.0 0 NONE_IN NONE_L3 NONE_L4
Client = CF
TI conn_id my_ip my_port peer_ip peer_por intf L3 L4
11 0 9.9.9.2 59005 9.9.9.1 59005 DATA IPV4 SCTP
Step 3

show redundancy application protocol \{protocol-id| group [group-id]\}

Example:

Router#show redundancy application protocol group

RG Protocol RG 1
----------------
Role: Standby
Negotiation: Enabled
Priority: 50
Protocol state: Standby-hot
Ctrl Intf(s) state: Up
Active Peer: address 1.1.1.2, priority 150, intf Gi0/0/0
Standby Peer: Local
Log counters:
role change to active: 0
role change to standby: 1
disable events: rg down state 1, rg shut 0
ctrl intf events: up 2, down 1, admin_down 1
reload events: local request 0, peer request 0

RG Media Context for RG 1
------------------------
Ctx State: Standby
Protocol ID: 1
Media type: Default
Control Interface: GigabitEthernet0/0/0
Current Hello timer: 3000
Configured Hello timer: 3000, Hold timer: 10000
Peer Hello timer: 3000, Peer Hold timer: 10000
Stats:
Pkts 117, Bytes 7254, HA Seq 0, Seq Number 117, Pkt Loss 0
Authentication not configured
Authentication Failure: 0
Reload Peer: TX 0, RX 0
Resign: TX 0, RX 0
Active Peer: Present. Hold Timer: 10000
Pkts 115, Bytes 3910, HA Seq 0, Seq Number 1453975, Pkt Loss 0

RG Protocol RG 2
----------------
Role: Active
Negotiation: Enabled
Priority: 135
Protocol state: Active
Ctrl Intf(s) state: Up
Active Peer: Local
Standby Peer: address 1.1.1.2, priority 130, intf Gi0/0/0
Log counters:
role change to active: 1
role change to standby: 1
disable events: rg down state 1, rg shut 0
ctrl intf events: up 2, down 1, admin_down 1
The following example shows configuration details for the redundancy application protocol group 1:

Router# show redundancy application protocol group 1

RG Protocol RG 1
------------------
Role: Standby
Negotiation: Enabled
Priority: 50
Protocol state: Standby-hot
Ctrl Intf(s) state: Up
Active Peer: address 1.1.1.2, priority 150, intf Gi0/0/0
Standby Peer: Local
Log counters:
role change to active: 0
role change to standby: 1
disable events: rg down state 1, rg shut 0
ctrl intf events: up 2, down 1, admin_down 1
reload events: local request 0, peer request 0

RG Media Context for RG 1
--------------------------
Ctx State: Standby
Protocol ID: 1
Media type: Default
Control Interface: GigabitEthernet0/0/0
Current Hello timer: 3000
Configured Hello timer: 3000, Hold timer: 10000
Peer Hello timer: 3000, Peer Hold timer: 10000
Stats:
Pkts 120, Bytes 7440, HA Seq 0, Seq Number 120, Pkt Loss 0
Authentication not configured
Authentication Failure: 0
Reload Peer: TX 0, RX 0
Resign: TX 0, RX 0
Active Peer: Present. Hold Timer: 10000
Pkts 102, Bytes 3468, HA Seq 0, Seq Number 1453977, Pkt Loss 0

The following example shows configuration details for the redundancy application protocol group 2:

Router# show redundancy application protocol group 2

RG Protocol RG 2
Role: Active
Negotiation: Enabled
Priority: 135
Protocol state: Active
Ctrl Intf(s) state: Up
Active Peer: Local
Standby Peer: address 1.1.1.2, priority 130, intf Gi0/0/0
Log counters:
role change to active: 1
role change to standby: 1
disable events: rg down state 1, rg shut 0
ctrl intf events: up 2, down 1, admin_down 1
reload events: local request 0, peer request 0

RG Media Context for RG 2

Ctx State: Active
Protocol ID: 2
Media type: Default
Control Interface: GigabitEthernet0/0/0
Current Hello timer: 3000
Configured Hello timer: 3000, Hold timer: 10000
Peer Hello timer: 3000, Peer Hold timer: 10000
Stats:
Pkts 123, Bytes 7626, HA Seq 0, Seq Number 123, Pkt Loss 0
Authentication not configured
Authentication Failure: 0
Reload Peer: TX 0, RX 0
Resign: TX 0, RX 1
Standby Peer: Present. Hold Timer: 10000
Pkts 107, Bytes 3638, HA Seq 0, Seq Number 1453982, Pkt Loss 0

The following example shows configuration details for the redundancy application protocol 1:

Router#show redundancy application protocol 1
Protocol id: 1, name: rg-protocol-1
Hello timer in msecs: 3000
Hold timer in msecs: 10000

OVLD-1#show redundancy application protocol 2
Protocol id: 2, name: rg-protocol-2
Hello timer in msecs: 3000
Hold timer in msecs: 10000

Step 4

```
show redundancy application faults group [group-id]
```

Example:

Router#show redundancy application faults group
Faults states Group 1 info:
Runtime priority: [50]
RG Faults RG State: Up.
Total # of switchovers due to faults: 0
Total # of down/up state changes due to faults: 2
Faults states Group 2 info:
Runtime priority: [135]
RG Faults RG State: Up.
Total # of switchovers due to faults: 0
Total # of down/up state changes due to faults: 2
The following example shows configuration details specific to redundancy application faults group 1:

Router#show redundancy application faults group 1

Faults states Group 1 info:
Runtime priority: [50]
RG Faults RG State: Up.
Total # of switchovers due to faults: 0
Total # of down/up state changes due to faults: 2

The following example shows configuration details specific to redundancy application faults group 2:

Router#show redundancy application faults group 2

Faults states Group 2 info:
Runtime priority: [135]
RG Faults RG State: Up.
Total # of switchovers due to faults: 0
Total # of down/up state changes due to faults: 2

Step 5 show redundancy application if-mgr group [group-id]

Example:

Router#show redundancy application if-mgr group

RG ID: 1
---------
interface GigabitEthernet0/0/3.152
---------------------------------------
VMAC 0007.b421.4e21
VIP 55.1.1.255
Shut shut
Decrement 10

interface GigabitEthernet0/0/2.152
---------------------------------------
VMAC 0007.b421.5209
VIP 45.1.1.255
Shut no shut
Decrement 10

RG ID: 2
---------
interface GigabitEthernet0/0/3.166
---------------------------------------
VMAC 0007.b422.14d6
VIP 4.1.255.254
Shut no shut
Decrement 10

interface GigabitEthernet0/0/2.166
---------------------------------------
VMAC 0007.b422.0d06
VIP 3.1.255.254
Shut no shut
Decrement 10

The following examples shows configuration details for redundancy application interface manager group 1 and group 2:
Router#show redundancy application if-mgr group 1

RG ID: 1
---------

interface GigabitEthernet0/0/3.152
---------------------------------------
VMAC 0007.b421.4e21
VIP 55.1.1.255
Shut shut
Decrement 10

interface GigabitEthernet0/0/2.152
---------------------------------------
VMAC 0007.b421.5209
VIP 45.1.1.255
Shut shut
Decrement 10

Router#show redundancy application if-mgr group 2

RG ID: 2
---------

interface GigabitEthernet0/0/3.166
---------------------------------------
VMAC 0007.b422.14d6
VIP 4.1.255.254
Shut no shut
Decrement 10

interface GigabitEthernet0/0/2.166
---------------------------------------
VMAC 0007.b422.0d06
VIP 3.1.255.254
Shut no shut
Decrement 10

Step 6  show redundancy application control-interface  group [group-id]

Example:

Router#show redundancy application control-interface group

The control interface for rg[1] is GigabitEthernet0/0/0
Interface is Control interface associated with the following protocols: 2 1
Interface Neighbors:
Peer: 1.1.1.2 Active RGs: 1 Standby RGs: 2

The control interface for rg[2] is GigabitEthernet0/0/0
Interface is Control interface associated with the following protocols: 2 1
Interface Neighbors:
Peer: 1.1.1.2 Active RGs: 1 Standby RGs: 2

The following example shows configuration details of the redundancy application control-interface group 1:

Router#show redundancy application control-interface group 1

The control interface for rg[1] is GigabitEthernet0/0/0
Interface is Control interface associated with the following protocols: 2 1
Interface Neighbors:
Peer: 1.1.1.2 Active RGs: 1 Standby RGs: 2
The following example shows configuration details of the redundancy application control-interface group 2:

Router#show redundancy application control-interface group 2

The control interface for rg[2] is GigabitEthernet0/0/0
Interface is Control interface associated with the following protocols: 2 1
Interface Neighbors:
Peer: 1.1.1.2 Active RGs: 1 Standby RGs: 2

Step 7 show redundancy application data-interface group [group-id]

Example:

Router#show redundancy application data-interface group

The data interface for rg[1] is GigabitEthernet0/0/1
The data interface for rg[2] is GigabitEthernet0/0/1

The following examples show configuration details specific to redundancy application data-interface group 1 and group 2:

Router#show redundancy application data-interface group 1
The data interface for rg[1] is GigabitEthernet0/0/1

Router#show redundancy application data-interface group 2
The data interface for rg[2] is GigabitEthernet0/0/1

---

Troubleshoot High Availability Issues

Use the following show and debug commands to troubleshoot any issues:

- show redundancy state
- show redundancy inter-device
- show standby brief
- show standby internal
- show sip-ua status
- show sip-ua statistics
- show voice high-availability summary
- show voip rtp connection | include connection
- show arp
- debug voip ccap all
- debug voip ccap error
- debug voip rtp session
- debug voip rtcp session
Troubleshoot High Availability Issues

- debug voip rtp error
- debug voip rtcp error
- debug voice high-availability all
- debug voice high-availability error
- debug ccsip info
- debug ccsip messages
- debug ccsip media
- debug ccsip error
- debug standby terse

Note

Do not turn on a large number of debugs on a system carrying high volume of active call traffic.