High Availability Overview

Cisco High Availability (HA) enables network-wide protection by providing fast recovery from faults that may occur in any part of the network. With Cisco High Availability, network hardware and software work together and enable rapid recovery from disruptions to ensure fault transparency to users and network applications.

The unique hardware and software architecture of the Cisco ASR 1000 Series Routers is designed to maximize router uptime during any network event, and thereby provide maximum uptime and resilience within any network scenario.

This guide covers the aspects of High Availability that are unique to the Cisco ASR 1000 Series Routers. It is not intended as a comprehensive guide to High Availability, nor is it intended to provide information on High Availability features that are available on other Cisco routers that are configured and implemented identically on the Cisco ASR 1000 Series Routers. The Cisco IOS feature documents and guides should be used in conjunction with this chapter to gather information about High Availability-related features that are available on multiple Cisco platforms and work identically on the Cisco ASR 1000 Series Routers.

- Finding Feature Information in This Module, on page 1
- Contents, on page 2
- Hardware Redundancy Overview on the Cisco ASR 1000 Series Routers, on page 2
- Software Redundancy on the Cisco ASR 1000 Series Routers, on page 3
- Route Processor Redundancy, on page 6
- Stateful Switchover, on page 6
- IPsec Failover, on page 7
- Bidirectional Forwarding Detection, on page 7
- Additional References, on page 8
- Feature Information for High Availability Overview, on page 9

Finding Feature Information in This Module

Your software release might not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information for High Availability Overview, on page 9.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn . An account on Cisco.com is not required.

Contents

This section discusses various aspects of High Availability on the Cisco ASR 1000 Series Routers and contains the following sections:

Hardware Redundancy Overview on the Cisco ASR 1000 Series Routers

Some models of the Cisco ASR 1000 Series Routers offer hardware redundancy within the same Cisco ASR 1000 Series Router through the following methods:

- Allowing two Route Processors (RPs) in the same Cisco ASR 1000 Series Router
- Allowing two Enhanced Services Processors (ESPs) in the same Cisco ASR 1000 Series Router

No hardware redundancy is supported for the following hardware:

- SPA interface processors (SIPs)—A SIP must be reloaded, and traffic briefly interrupted, for a SIP upgrade to complete.
- Shared port adapters (SPAs)—A SPA must be reloaded, which will briefly interrupt traffic to that SPA, for a SPA software subpackage update to complete.

Hardware redundancy on the Cisco ASR 1000 Series Routers gives users the following benefits:

- A failover option—If a processor fails, the standby processor immediately becomes the active processor with little or no delay. The failover happens completely within the same router, so a second standby router is not needed.
- No downtime upgrades—Using features like ISSU, a software upgrade can be handled on the standby processor while the active processor continues normal operation.

Hardware redundancy is available on the Cisco ASR 1006 Router only at this time.

provides a hardware redundancy overview.

Table 1: Hardware Redundancy Overview

Hardware	Support for Dual Hardware Configuration on Cisco ASR 1001 Router	Support for Dual Hardware Configuration on Cisco ASR 1002 Router	Support for Dual Hardware Configuration on Cisco ASR 1004 Router	Support for Dual Hardware Configuration on Cisco ASR 1006 Router	Failover Behavior
Enhanced Services Processor	No	No	No	Yes	If an active ESP experiences a hardware or software event that makes it unable to forward traffic (such as a hardware failure, an OIR, or a manual switch) and a standby ESP is configured, the standby ESP becomes the active ESP with the possibility of a minor interruption (less than 200 ms).

Hardware	Support for Dual Hardware Configuration on Cisco ASR 1001 Router	Support for Dual Hardware Configuration on Cisco ASR 1002 Router	Support for Dual Hardware Configuration on Cisco ASR 1004 Router	Support for Dual Hardware Configuration on Cisco ASR 1006 Router	Failover Behavior
Route Processor	No	No	No	Yes	If an active RP experiences an event that makes it unable to forward traffic (such as a hardware failure, a software failure, an OIR, or a manual switch) and a standby RP is configured, the standby RP immediately becomes the active RP.
SPA	No	No	No	No	No standby configurations are available for SPAs. If a SPA fails, that particular SPA is down and unable to forward traffic. In the event of a SPA shutdown, all other SIPs and SPAs on the router continue to be fully operational.
SIP	No	No	No	No	No standby configurations are available for SIPs. If a SIP fails, all SPAs in that SIP are down and unable to forward traffic. In the event of a SIP shutdown, all other SIPs and SPAs on the router continue to be fully operational.

Software Redundancy on the Cisco ASR 1000 Series Routers

This section covers the following topics:

Software Redundancy Overview

On the Cisco ASR 1000 Series Routers, IOS runs as one of many processes within the operating system. This is different than on traditional Cisco IOS, where all processes are run within Cisco IOS. See the "IOS as a Process" section on page 2-7 for more information regarding IOS as a process on the Cisco ASR 1000 Series Router.

This architecture allows for software redundancy opportunities that are not available on other platforms that run Cisco IOS software. Specifically, a standby IOS process can be available on the same Route Processor as the active IOS process. This standby IOS process can be switched to in the event of an IOS failure, and can also be used to upgrade subpackage software in some scenarios as the standby IOS process in a software upgrade.

On the Cisco ASR 1006 Router, the second IOS process can run only on the standby Route Processor. Two IOS processes on the same Router Processor are not possible for any Cisco ASR 1000 Series Router that supports dual RP hardware redundancy configurations since the second Route Processor can support a standby IOS process. An overview of software redundancy is shown in Table 2: Software Redundancy Overview, on page 4.

Table 2: Software Redundancy Overview

Router	Support for Two IOS Processes on Same Route Processor	Support for a Second IOS Process on Standby Route Processor	Explanation
Cisco ASR 1001 Router[1]	Yes	N/A	The Cisco ASR 1001 Router only supports one RP, so dual IOS processes run on the lone RP.
Cisco ASR 1002 Router	Yes	N/A	The Cisco ASR 1002 Router only supports one RP, so dual IOS processes run on the lone RP.
Cisco ASR 1004 Router	Yes	N/A	The Cisco ASR 1004 Router only supports one RP, so dual IOS processes run on the lone RP.
Cisco ASR 1006 Router	No	Yes	The Cisco ASR 1006 Router supports a second Route Processor, so the second IOS process can only run on the standby Route Processor.

[1] If a critical process, such as the ESP or the SIP fails on the Cisco ASR 1001 Router, then the entire chassis reloads.

Second IOS Process on a Cisco ASR 1002 or 1004 Router

For Cisco ASR 1002 and 1004 routers, Route Processor Redundancy and Stateful Switchover can be used to switch between IOS processes. RPR and SSO need to be configured by the user, however, because a second IOS process is not available by default on Cisco ASR 1002 and 1004 routers.

Table 2 summarizes the software redundancy opportunities available with the second IOS process for the Cisco ASR 1002 and 1004 routers.

Table 3: Software Redundancy Options for Cisco ASR 1002 and 1004 Routers

Router	Default HA Setting	Options with 2 GB or DRAM	Options with 4 GB or DRAM
Cisco ASR 1002 Router	None	None	None, RPR, SSO
Cisco ASR 1004 Router	None	None	None, RPR, SSO

ISSU cannot be used to upgrade consolidated packages on Cisco ASR 1002 or 1004 Routers, and only a few subpackages can be upgraded individually using ISSU through the use of dual IOS processes on the same Route Processor. See the Route Processor Redundancy, on page 6 for more information on which subpackages can be upgraded using ISSU in a dual RP setup.

Configuring two Cisco IOS process on one RP

On the Cisco ASR 1000 Series Routers, Cisco IOS runs as one of the many processes. This architecture supports software redundancy opportunities. Specifically, a standby Cisco IOS process is available on the same Route Processor as the active Cisco IOS process. In the event of a Cisco IOS failure, the system switches to the standby Cisco IOS process. It also supports software upgrade of subpackages when the standby Cisco IOS process is performing an ISSU upgrade.

This section describes how to configure two Cisco IOS process on one RP.

SUMMARY STEPS

1. enable
2. **configure terminal**
3. redundancy
4. mode SSO
5. **exit**
6. reload

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`	Enters global configuration mode.
Step 3	redundancy **Example:** `Router(config)# redundancy`	Enters redundancy configuration mode.
Step 4	mode SSO **Example:** `Router(config)# mode SSO`	Configures SSO. When this command is entered, the redundant supervisor engine is reloaded and begins to work in SSO mode.

Step 5	**exit**
	Example:
	`Router(config)# exit`
	Example:
	`Router #`
		Exits configuration mode and returns to global configuration mode.

	Command or Action	Purpose
Step 6	reload **Example:** `Router # reload`	Reloads IOS.

Example

```
Router# configure terminal
Router(config)# redundancy
Router(config)# mode SSO
Router(config)# exit
Router# reload
```

Route Processor Redundancy

Route Processor Redundancy (RPR) allows you to configure a standby RP. When you configure RPR, the standby RP loads the Cisco IOS software on bootup and initializes itself in standby mode. In the event of a fatal error on the active RP, the system switches to the standby RP, which reinitializes itself as the active RP. In this event, the entire system is rebooted, so the switchover with RPR is slower than with other High Availability switchover features such as Nonstop Forwarding/Stateful Switchover (NSF/SSO).

On the Cisco ASR 1000 Series Router, RPR can also be used to enable a second IOS process on a single RP for a Cisco ASR 1002 or 1004 Router. See the Second IOS Process on a Cisco ASR 1002 or 1004 Router, on page 4 for additional information on the second IOS process.

For the Cisco ASR 1000 Series Routers, RPR introduces the following functionality:

- Startup configuration synchronization between the active and standby RP or IOS process. It is important to note, however, that changes in the running configuration are not synchronized using RPR.
- Warm Reload—The Warm Reload feature allows users to reload their routers without reading images from storage; that is, the router reboots by restoring the read-write data from a previously saved copy in the RAM and by starting execution without either copying the software from flash to RAM or self-decompression of the image.

It is important to note that in most cases, Stateful Switchover (SSO) requires less downtime for switchover and upgrades than RPR. RPR should only be used when there is a compelling reason to not use SSO.

It is important to note RPR is supported on the Cisco ASR 1000 Series Routers while RPR+ is not.

Stateful Switchover

The Stateful Switchover (SSO) feature takes advantage of processor redundancy by establishing one of the processors as the active processor while the other RP is designated as the standby processor, and then synchronizing critical state information between them. Following an initial synchronization between the two processors, SSO dynamically maintains RP state information between the dual processors.

Stateful Switchover is particularly useful in conjunction with Nonstop Forwarding. SSO allows the dual processors to maintain state at all times, and Nonstop Forwarding lets a switchover happen seamlessly when a switchover occurs.

On the Cisco ASR 1000 Series Router, SSO can also be used to enable a second IOS process on a single RP for a Cisco ASR 1002 or 1004 Router. See the Second IOS Process on a Cisco ASR 1002 or 1004 Router, on page 4 for additional information on the second IOS process.

It is important to note that in most cases, SSO requires less downtime for switchover and upgrades than RPR. RPR should only be used when there is a compelling reason to not use SSO.

For additional information on NSF/SSO, see the Cisco Nonstop Forwarding document.

SSO-Aware Protocol and Applications

SSO-supported line protocols and applications must be SSO-aware. A feature or protocol is SSO-aware if it maintains, either partially or completely, undisturbed operation through an RP switchover. State information for SSO-aware protocols and applications is synchronized from active to standby to achieve stateful switchover for those protocols and applications.

The dynamically created state of SSO-unaware protocols and applications is lost on switchover and must be reinitialized and restarted on switchover.

To see which protocols are SSO-aware on your router, use the following commands **show redundancy client** or **show redundancy history**.

IPsec Failover

IPSec failover is a feature that increases the total uptime (or availability) of a customer's IPSec network. Traditionally, this is accomplished by employing a redundant (standby) router in addition to the original (active) router. If the active router becomes unavailable for any reason, the standby router takes over the processing of IKE and IPSec. IPSec failover falls into two categories: stateless failover and stateful failover.

The IPsec on the Cisco ASR 1000 Series Router supports only stateless failover. Stateless failover uses protocols such as the Hot Standby Router Protocol (HSRP) to provide primary to secondary cutover and also allows the active and standby VPN gateways to share a common virtual IP address.

Bidirectional Forwarding Detection

Bidirectional Forwarding Detection (BFD) is a detection protocol designed to provide fast forwarding path failure detection times for all media types, encapsulations, topologies, and routing protocols. In addition to fast forwarding path failure detection, BFD provides a consistent failure detection method for network administrators. Because the network administrator can use BFD to detect forwarding path failures at a uniform rate rather than the variable rates for different routing protocol hello mechanisms, network profiling and planning is easier, and reconvergence time is consistent and predictable.

On the Cisco ASR 1000 Series Routers, BFD for IPv4 Static Routes and BFD for BGP are supported.

For more information on BFD, see the Bidirectional Forwarding Detection document.

Additional References

Related Documents

Related Topic	Document Title
Bidirectional Forwarding Detection	*IP Routing BFD Configuration Guide, Cisco IOS XE Release 3S*
High Availability Configurations	*High Availability Configuration Guide, Cisco IOS XE Release 3S*
Software Upgrade Process Configurations	Software Upgrade Process Configuration Guide

Standards

Standard	Title
None	—

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at this URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
None	—

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for High Availability Overview

Table 4: Feature Information for High Availability Overview , on page 9 lists the features in this module and provides links to specific configuration information.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn . An account on Cisco.com is not required.

Note Table 4: Feature Information for High Availability Overview , on page 9 lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Table 4: Feature Information for High Availability Overview

Feature Name	Releases	Feature Information
High Availability Overview	Cisco IOS XE 2.1S	In Cisco IOS XE Release 2.1S, this feature was introduced on the Cisco ASR 1000 Series Router.