

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 8500 Series Secure Router 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 8500 Series Secure Router. 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 8500 Series Secure 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 8500 Series Secure Router.

- Finding feature information in this module, on page 1
- Contents, on page 1
- Software redundancy on the Cisco 8500 Series Secure Router, on page 2
- Stateful switchover, on page 3
- IPsec failover, on page 4
- Bidirectional forwarding detection, on page 4

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.

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 8500 Series Secure Router and contains the following sections:

Software redundancy on the Cisco 8500 Series Secure Router

This section covers the following topics:

Software redundancy overview

On the Cisco 8500 Series Secure 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 8500 Series Secure Routers.

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.

Configuring two Cisco IOS processes

On the Cisco 8500 Series Secure 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.

SUMMARY STEPS

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

DETAILED STEPS

Procedure

	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.

	Command or Action	Purpose
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.

Step 6	reload **Example:** `Router # reload`	Reloads IOS.

Stateful switchover

On the Cisco 8500 Series Secure Routers, Stateful Switchover (SSO) can be used to enable a second IOS process.

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

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 8500 Series Secure Routers 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 8500 Series Secure Routers, BFD for IPv4 Static Routes and BFD for BGP are fully supported.

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