WHITE PAPER

CISCO IOS HIGH AVAILABILITY
CURBS DOWNTIME WITH FASTER RELOADS AND UPGRADES

For Single Processor Routing and Switching Systems

Cisco IOS® Software has been enhanced to meet demand for higher network service availability. Two features, Warm Reload and Warm Upgrade, improve system reboot times and lower the impact of upgrades and software faults.

Cisco continually enhances Cisco IOS Software to eliminate or reduce the impact of potential causes of downtime and to meet customers' requirement for access to applications, systems, and data from anywhere, anytime

The recent introduction of the Warm Reload capability and the release of Warm Upgrade capability are examples of Cisco IOS Software enhancements that improve network service availability in non-redundant systems, particularly for network products with a single processor.

This document provides a brief overview of these features.

COLD/WARM/HOT

Before discussing these features themselves, it is helpful to describe the terminology used throughout the Cisco IOS High Availability program.

The adjectives 'Cold', 'Warm', or 'Hot' are used to denote the readiness of the system and its components to assume the network services functionality and the job of forwarding packets to their destination. These terms will appear in conjunction with Cisco Nonstop Forwarding (NSF) with Stateful Switchover (SSO), within output from Cisco IOS Software 'show' commands, such as 'sh redundancy states', and with many high availability feature descriptions. Each term is used to convey the technical underpinnings, which surround the amount of internal state information saved to allow increasingly faster switchover or even continuous packet forwarding. The terms are generally defined as:

- **Cold**: Cold redundancy refers to the degree of resiliency that has been traditionally provided by a redundant system. A redundant system is 'cold' when no state information is maintained between the backup or standby system and the system it offers protection to.
- **Warm**: Warm redundancy refers to a degree of resiliency beyond cold standby system. In this case, the redundant system has been partially prepared, but does not have all of the state information known by the primary system, so that it can take over immediately. Some additional information must be determined or gleaned from the traffic flow or the peer network devices to handle packet forwarding.
- **Hot**: Hot redundancy refers to a degree of resiliency where the redundant system is fully capable of handling the traffic of the primary system id. Substantial state information has been saved, so the network service is continuous, and the traffic flow is minimally or not affected.

In the case of a single-processor, non-redundant system the term *warm* refers to the fact that Cisco IOS Software is preloaded and partially prepared to resume packet forwarding. However, the system is reinitialized, so all software state pertaining to network services must be reacquired and prepared as with a 'cold' reboot. A more detailed description of each feature follows.

WARM RELOAD

The Cisco IOS Software Warm Reload feature allows Cisco IOS Software to reload without Read Only Memory Monitor (ROMMON) intervention. Essentially, the image restores the read-write data from a previously saved copy in the RAM and restarts execution of the Cisco IOS Software. A significant reduction in downtime is achieved because this avoids the lengthy time for a flash to RAM copy and image self-decompression.

The benefit of this method is realized for situations in which it might be necessary or beneficial to reload the router or switch. This might involve some instance where a software problem has rendered the system non-functional or sub-optimal.

Warm Reload works by saving the initialized Cisco IOS Software data segment at the 'cold' boot-up before it is changed. When an exception occurs or when a Warm Reload is requested via command-line interface (CLI), the saved data segment is restored and control is passed (jump) to the start of the Cisco IOS Software text segment.

The major gain from Warm Reload is its ability to bypass the image copy from flash to the RAM and the subsequent software image decompression step. Enabling the feature causes the text and read-only data segments to remain in the memory, the read-write data segment is restored upon request or software crash, the bss and heap are rebuilt, and processing is restarted. The network then reconverges and traffic resumes as with any reload.

The difference between a cold reboot and Warm Reload is illustrated in Figures 1 and 2. Figure 1 shows the traditional cold boot process. Execution is halted, the image is loaded (read in from flash to RAM) and decompressed, the system is booted, initialized, and execution begins.

The red line around the outside of the figure denotes the network service downtime, which extends from the time execution is first halted to the time execution is resumed.

Figure 1. Reload Process prior to the introduction of Warm Reload

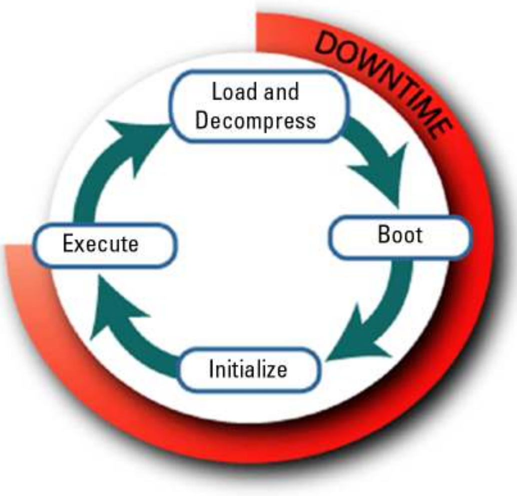


Figure 2. Reload Process subsequent to the introduction of Warm Reload

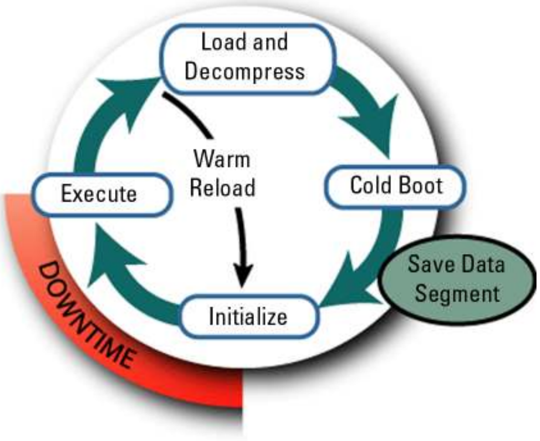


Figure 2 has an added step: "Save Data Segment". Following a cold boot, the data segment is retained in the memory. When a Warm Reload is triggered, the system is halted and reinitialized using the in-memory data segment. The system takes a 'short-cut' to initialization, and the load and compress step is bypassed.

Note: Prior to invoking a Warm Reload, a 'cold' reboot must happen with the Warm Reload feature configured, so that the "Save Data Segment" step has occurred.

An added benefit is protection from the case where the system has been configured to load an image from removable media (i.e. ATA flash disk), and the media is subsequently removed. Without Warm Reload, the system might fail and would not come back to a fully operational state if it cannot locate the image it needs to load. With Warm Reload, there is less chance for an error in this situation. In most cases, the system will re-initialize using the in-memory data segment.

Table 1 shows a comparison of the time taken to cold boot versus the time taken to perform a Warm reload. A significant reduction in downtime can be attained.

Table 1. Sample Warm Reload Times

	Cold Reboot Time	Warm Reload Time	Reduction in Downtime	% Improvement
Cisco 7206 NPE G1 Router	3 minutes, 43 seconds (0:223s)	32 seconds	3 minutes, 11 seconds	86%
Cisco 7204 NPE 400 Router	2 minutes, 4 seconds (0:124s)	21 seconds	1 minute, 43 seconds	83%

*Times vary for each configuration

Warm Reload Details

The Warm Reload feature has been designed and engineered to accommodate and anticipate problems that may be encountered by enabling such a feature. To guard against any possibility of ROMMON state corruption due to software anomaly, an internal hard limit is placed on the number of consecutive Warm Reload attempts. If reached, the system falls back to a ‘cold’ reboot. In addition, timers are maintained to detect software crash conditions that occur within a specified time after a Warm Reload. This acts as another safeguard and, if triggered, the system falls back to a ‘cold’ reboot. The integrity of the saved data segment is verified and/or protected prior to invoking the Warm Reload. Finally, the software conditions that result in a Warm Reload are only those that are software-induced anomalies. When appropriate, a crash info file and core are saved as with the current ‘cold’ reboot. Other conditions that may be caused by a hardware-related fault result in a ‘cold’ reboot.

Memory Use

Enabling Warm Reload will have an impact on the available memory. The available memory for the hardware will be reduced by the size of the reserved Warm Reload storage area. The amount of memory required will depend upon the size of the read-write initialized data for the image plus the space necessary for Warm Reload control structures. On average, this will equal 1–2MB.

If the user disables Warm Reload later, the memory taken by the Warm Reload storage will be released and made available to the Cisco IOS Software memory manager.

Warm Reload Feature Availability

Cisco IOS Warm Reload has been available in the Cisco IOS Software Release 12.2S and 12.3T families since Releases 12.2(18)S and 12.3(2)T, respectively. For additional information, please visit:
http://www.cisco.com/go/ios

Cisco IOS Software is packaged in feature sets that support specific hardware. For updated information on hardware support, please visit Cisco Feature Navigator at:
http://www.cisco.com/go/fn/.

This application dynamically updates the list of supported hardware, when hardware support is added for the feature.

Warm Reload Configuration Example

```
Router#(config) warm-reboot count 10 uptime 10
Router#(config) exit
!
Router# show warm-reboot
Warm Reboot is enabled
```

If the reload command is issued after configuration of the warm-reboot global command, a 'cold' reboot will occur. Thus, to reload the system without overriding the warm-reboot functionality, specify the warm keyword with the reload command. Use this task to perform a Warm Reload.

```
Router# reload warm at 10:30
```

WARM UPGRADE

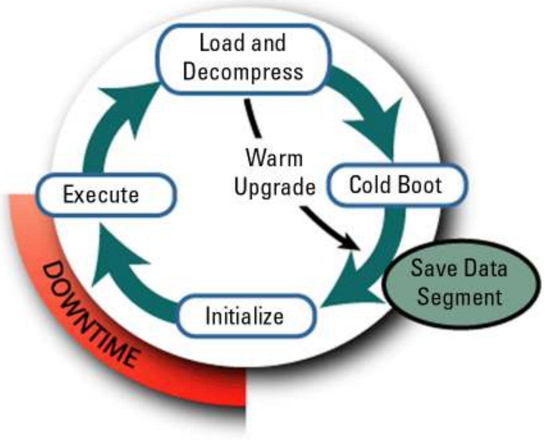
Faster upgrades can be achieved by extending the strategy used by Warm Reload. For Warm Upgrade the Cisco IOS Software image should be preloaded, then existing operation halted, and control transferred to the new, in-memory Cisco IOS Software version.

Cisco IOS Warm Upgrade builds on the capability set forth with Warm Reload. It introduces an optional parameter to the reload CLI command to allow the network administrator to specify the name of the Cisco IOS Software image to load.

For example:

```
Router# reload warm file disk2:c7200-js-mz.122-18.S3
```

Figure 3. Warm upgrade process



After this command is issued, the router will continue to forward packets and load the new image into memory. As illustrated in Figure 3, the system does not halt nor perform a cold reboot, but instead loads and then decompresses the new Cisco IOS Software image, while packet forwarding continues. After the new image is fully loaded and prepared, execution is halted, and control is transferred to the new image for initialization and execution.

Again, Warm Upgrade results in less downtime to upgrade the Cisco IOS Software than a traditional reboot. This means less impact on network services, end users, and business planned software upgrades. With Warm Upgrade the downtime associated with Cisco IOS Software upgrade can be reduced from 3–4 minutes to approximately 30 seconds.

TEST RESULTS

To illustrate the difference in downtime and the positive effect Warm Upgrade can have in a network, Cisco ran tests to demonstrate the time required for an upgrade and for traffic forwarding to resume. The results of the tests are shown in Table 2.

A network test bed simulated a headend router with 500 OSPF routing destinations. Traffic was sent to each of the routed subnets, and the headend router under test was upgraded to a newer version of Cisco IOS Software. Table 2 illustrates the times at various stages of recovery.

Table 2. Warm Upgrade Test Results

	Without Warm Upgrade	With Warm Upgrade
Reload start	0:00	0:00
Packet loss seen	0:00	0:27
Reload complete	2:50	1:00
OSPF adjacency restored	3:20	1:30
Traffic flow restored to all 500 destinations	3:35	1:35

*Cumulative times

As seen in Table 1, traffic loss with Warm Upgrade is not seen until 27 seconds after the upgrade command is issued and the **downtime as a result of the upgrade is decreased from 3:35 seconds to 1 minute, 8 seconds** (1:35 - 0:27 = 1:08). **The impact to service is reduced by 2 minutes, 27 seconds or 68%**.

SUMMARY

Cisco recognizes that reduction of any and all potential sources of network service downtime is important to customers. Therefore, Cisco IOS High Availability strategy is very simple: innovate and enhance Cisco IOS Software to eliminate or reduce the impact of all potential causes of downtime. This strategy has given rise to the Warm Reload and Warm Upgrade features which improve availability of single-processor, non-redundant systems.

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on **the Cisco Web site at www.cisco.com/go/offices.**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland
Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland
Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe