CISCO SYSTEMS

Data Sheet

Cisco IOS Software High-Availability Enhancements for IP/MPLS Provider Edge

This data sheet provides an overview of the new Cisco IOS® Software high-availability enhancements aimed at maximizing service availability for the IP/Multiprotocol Label Switching (MPLS) provider edge. These capabilities are first being delivered on the Cisco® 10000 Series edge routing platform.

Product Overview

Converged IP/MPLS network infrastructure requires the highest level of availability for meeting critical service-level agreements (SLAs) and providing continuous network operations during network and service upgrades. The high-availability needs are especially critical at the network edge – convergence point for terminating customer connections and deploying new services – and, therefore, it is often a single point of failure. As a result, there is a keen focus on application and service continuity at the network edge. To meet the demands of the next-generation IP/MPLS networks and ensure optimal service delivery, high-availability capabilities for the edge devices must ensure continuous operations during network upgrades and service enhancements. They must also minimize the effect of hardware and software failures and deliver the ability to meet stringent SLAs to provide always-available network services, while scaling as required. The combination of new Cisco IOS Software high-availability enhancements on the Cisco 10000 Series router maximizes service availability at the IP/MPLS edge and provides the resiliency service providers need to meet critical evolving network and service demands. This increased availability and resiliency minimizes network downtime and enables service providers to improve service, increase revenue, and reduce operational costs.

The new Cisco IOS Software enhancements include:

- **Cisco IOS In-Service Software Upgrades (ISSU)** – Industry's first, comprehensive, seamless software upgrade capability for the IP/MPLS edge router. Cisco IOS ISSU supports the entire range of software upgrade needs from applying bug fixes to deploying new features and services through in-service upgrade of the complete Cisco IOS Software image. This complete Cisco IOS ISSU capability extends Cisco's high-availability innovations for minimizing planned downtime delivered earlier in Cisco IOS XR Software for Service Provider Networks and in Cisco IOS Software Modularity for Enterprise Campus and Data Center Networks.

- **Border Gateway Protocol (BGP) nonstop routing (NSR)** – This unique, self-contained routing high-availability solution extends IP high-availability capability and benefits to the entire edge. BGP NSR enables Service Providers to "maintain all necessary" BGP routing and session information with customer edge (CE) routers during a processor switchover or during a planned ISSU software upgrade for a provider edge (PE) router. CE routers do not need to be NSF-capable or NSF-aware to benefit from BGP NSR capability on PE routers.

- **MPLS nonstop forwarding with stateful switchover (NSF/SSO)** – This feature extends proven NSF/SSO high-availability technology to MPLS forwarding, MPLS Label Distribution Protocol (LDP), and MPLS VPN (including inter-autonomous system and carrier supporting carrier [CSC]), mitigating service disruptions, reducing downtime costs, and increasing operational efficiency.

- **Line-Card Redundancy with Y-cables** – This seamless line-card failover solution takes advantage of the Cisco 10000 Series 4-Port Channelized T3 Half-Height Line Card hardware support for Y-cables to mitigate service disruptions and reduce network outages for line-card hardware and software failures.

Integration and delivery of these high-availability enhancements on the Cisco 10000 edge routing platform provides a comprehensive solution that, as a combined feature set, optimizes service and network performance and delivers:

- **Improved service and increased revenue potential** – These enhancements deliver critical, differentiated SLAs by mitigating user and service disruptions from software and hardware failures, and facilitating rapid, nondisruptive deployment of new features and services.

- **Reduced operational expenses** – These enhancements minimize the costs associated with planned and unplanned downtime, including SLA penalties, network administration, and troubleshooting and maintenance costs, thereby increasing operational efficiency.

- **Investment protection** – These high-availability enhancements deliver advanced IP/MPLS edge performance on existing flexible-edge routing platform.

Cisco IOS In-Service Software Upgrade

Cisco IOS ISSU is the industry's first, comprehensive in-service upgrade solution for the IP/MPLS edge, mitigating network downtime due to software upgrades and maintenance activities. This solution allows customers to upgrade or downgrade complete Cisco IOS Software images with no effect on the control plane and minimal effect on system packet forwarding. ISSU takes advantage of proven Cisco NSF/SSO technology and implements powerful message versioning capability in Cisco IOS Software to help enable true in-service upgrade across Cisco IOS Software release versions. To perform an in-service upgrade, the standby route processor in a dual-route-processor-based platform is first loaded with the desired Cisco IOS Software release. The standby route processor then comes up as a hot-standby route processor with an upgraded version of the software, and a switchover is performed to transfer control to it and run the upgraded image. During the ISSU procedure, supported SSO protocols and features maintain their session states and, as a result, there is no disruption of the Layer 2 protocol sessions. Furthermore, Cisco NSF technology is used to continue packet forwarding during the software upgrade procedure while the routing information is recreated on the newly active route processor. The net result is a seamless software upgrade for an IP/MPLS provider edge router with no disruptions to Layer 2 protocol sessions and minimal effect on packet forwarding.

This comprehensive Cisco IOS ISSU capability addresses the entire spectrum of software upgrade needs, from applying a set of bug fixes through Cisco IOS Software maintenance rebuild releases to deploying new features and services through Cisco IOS Software feature releases. ISSU capability is further complemented with extensive tooling support and information on Cisco Feature Navigator and Cisco IOS Software Selector Websites to assist customers in obtaining ISSU software version and feature compatibility information across Cisco IOS Software releases.

Benefits

Primary benefits for ISSU include:

- **Rapid, nondisruptive feature deployment** – By preserving user sessions and minimizing packet loss during software upgrades, ISSU helps enable rapid, nondisruptive deployments for new features and services at the IP/MPLS provider edge.

- **Comprehensive solution for planned downtime** – ISSU addresses the entire spectrum of software upgrade needs, from applying bug fixes to deploying new features and services, and delivers a comprehensive solution for addressing planned network downtime.

- **Increased operational efficiencies** – ISSU minimizes and streamlines planned downtime and helps enable operational process changes for software deployment, significantly decreasing planned downtime effort and expenses and increasing operational efficiency.

BGP Nonstop Routing

BGP NSR is a unique, self-contained routing high-availability solution that extends IP high-availability deployments and benefits to the entire edge. Currently BGP supports NSF (through BGP Graceful Restart) as part of the NSF/SSO high-availability offering in Cisco IOS Software. BGP NSR extends the routing high-availability capabilities to the next level by "maintaining all necessary" BGP routing and session information across a route-processor switchover.

Cisco IOS Software support for NSR allows service providers to maintain BGP routing information from customer routers during a switchover process from an active route processor to a standby route processor without having to require resynchronization from the remote customer edge router. The customer edge routers do not need to have NSF-awareness support in order to benefit from Cisco BGP NSR capabilities on the provider edge, allowing NSR to be interoperable with all types of customer edge routers from Cisco as well as other vendors and simplifying NSF/SSO deployment at the edge.

Ultimately, the BGP NSR feature delivers a high-availability solution with no effect on routing and with minimal effect on traffic forwarding to and from the customer sites during a route-processor switchover or a planned ISSU software upgrade of a provider edge router. Furthermore, only the provider edge router needs to be upgraded to support NSR – no customer edge router upgrades are required.

Benefits

BGP NSR provides a routing high-availability solution with the following benefits:

- **Minimizes service disruptions** – This feature reduces impact on customer traffic during route-processor switchovers (scheduled or unscheduled events), extending high-availability deployments and benefits at the edge.

- **Enhances high-availability NSF/SSO deployment at the edge** – This feature allows incremental deployment by upgrading the provider edge with new NSR capability so that customer-facing edge routers are synchronized automatically and no coordination or NSF awareness is needed with the customer-side Cisco and third-party customer edge routers. The BGP NSR feature dynamically detects NSF-aware peers and runs Graceful Restart with those customer edge routers.

- **Provides transparent route convergence** – BGP eliminates route flaps between BGP peers by keeping BGP state on both active and standby route processors and ensures continuous packet forwarding with minimal packet loss during route-processor switchovers.

MPLS NSF/SSO

MPLS NSF/SSO enhancements extend the proven Cisco NSF/SSO high-availability technology to MPLS forwarding, MPLS LDP, and MPLS VPNs (including inter-autonomous system and CSC). With these new enhancements, NSF/SSO delivers seamless route-processor switchover and helps ensure nonstop VPN services availability at the IP/MPLS provider edge. SSO protects from hardware or software faults on an active route processor by synchronizing protocol and state information for supported features with a standby route processor, helping ensure no interruption of sessions or connections if a switchover occurs. The SSO feature takes advantage of route-processor redundancy by establishing one of the route processors as the active processor, designating the other route processor as the standby processor, and then synchronizing critical state information between them. Following an initial synchronization between the two processors, SSO dynamically maintains route-processor state information between them. A switchover from the active to the standby processor occurs when the active route processor fails, when it is removed from the networking device, or when it is manually taken down for maintenance. The standby route processor then takes control and becomes the active route processor, preserving the sessions and connections for the supported features. At this time, packet forwarding continues while route convergence is completed on the newly active route processor. This continuous forwarding technique is accomplished through the Cisco NSF feature.

Cisco NSF works with SSO to minimize the amount of time a network is unavailable to its users following a switchover; it helps suppress routing flaps, thus improving network stability. Cisco NSF allows for the forwarding of data packets to continue along known routes while the routing protocol information is being restored on the newly active route processor following a switchover through IETF Graceful Restart extensions for the routing protocols. With Cisco NSF, peer networking devices do not experience routing flaps.

MPLS NSF/SSO feature enhancements follow:

- **NSF/SSO – MPLS LDP and LDP Graceful Restart** – This feature works with LDP sessions between directly connected peers as well as with peers that are not directly connected (targeted sessions) and allows a router to recover during a route-processor switchover without losing its MPLS forwarding state and with minimal packet loss. This capability is invoked under two conditions:

  - **LDP restart** – An LDP restart occurs because of a route-processor failure in a redundant system. If the system is configured with this feature, the standby route processor retains the MPLS forwarding state and reestablishes communication with the LDP neighbors and recovers the LDP bindings.

  - **LDP session reset** – An LDP session reset occurs because of an LDP session failure on a route processor. The LDP session might have been interrupted because of a TCP or User Datagram Protocol (UDP) communication problem. If the system is configured with this feature, the route processor associates a new session with the previously interrupted session. The LDP bindings and MPLS forwarding states are recovered when the new session is established.

- **NSF/SSO – MPLS VPN** – This feature allows a router to recover during a route-processor switchover without losing its VPN prefix information and with minimal packet loss. The following VPN types are supported:

  - **Basic MPLS VPNs**
  - **MPLS VPN** – CSC
  - **MPLS VPN** – Inter-autonomous systems

    MPLS VPN NSF/SSO works with BGP Graceful Restart, preserving BGP sessions between BGP peers during a route-processor switchover. Without MPLS VPN NSF/SSO support, all BGP sessions (including BGP sessions on provider edge routers) are reset. The provider edge router restarts all sessions, repopulates all the routes in its routing table, and then reconverges. This process can take several seconds to minutes, during which time traffic is lost. With MPLS VPN NSF/SSO, BGP sessions restart gracefully and state information is recovered from neighbors while the line cards continue to forward VPN traffic, taking advantage of the NSF capability.

Benefits

MPLS NSF/SSO provides a route-processor protection solution with the following benefits:

- **Provides automatic fault detection and seamless recovery** – MPLS NSF/SSO enhancements allow continuous forwarding for MPLS LDP and Layer 3 VPN (L3VPN) traffic during a route-processor switchover scenario. The control plane recovers gracefully, delivering faster LDP and MPLS VPN convergence.

- **Eliminates service disruption** – By preserving user sessions and minimizing packet loss, MPLS NSF/SSO reduces the effect of service outages on network users and delivers increased network uptime at the IP/MPLS provider edge.

- **Reduces costs and increases operational efficiency** – MPLS NSF/SSO decreases downtime expenses, including SLA penalties, lost revenue opportunities, user and administrative productivity costs, and emergency network expenditures, thereby increasing operational efficiency.

Line-Card Redundancy with Y-Cables

Line-Card Redundancy with Y-cables on the Cisco 10000 4-Port, Half-Height CT3 Line Card delivers seamless failover to a standby Y-cable-connected line card if a currently active line card fails. The new 4-port Channelized T3 (CT3) module provides enhanced hardware support for Y-cable connectivity. The Line-Card Redundancy feature uses this hardware redundancy capability to establish an active-standby CT3 line-card configuration whereby all ports of active line cards are connected with corresponding ports of standby line cards through Y-cables. Complete protection from a line-card failure can then be provided such that if any hardware or software fails on the active line card, the standby Y-cabled line-card ports take over from the failed line-card ports, with no disruption to any higher-layer protocols and applications and minimal disruption to traffic forwarding in the system.

Benefits

Line-Card Redundancy with Y-cables provides a router high-availability solution with the following benefits:

- **Reduced downtime and lower operational costs** – The line-card redundancy feature allows significant reduction in mean time to recovery for line-card failure (from minutes to less than a few seconds). Operational cost savings can be realized by further optimizing emergency dispatch and repair operations and reducing network troubleshooting and maintenance costs.

- **Incremental revenue through improved SLAs** – Coupled with NSF/SSO and ISSU, the line-card redundancy feature offers enhanced SLA capabilities at the IP/MPLS edge, providing incremental revenue opportunities.

- **Higher customer satisfaction** – By preserving user connectivity during line-card failures in scenarios that have hitherto been single points of failure, the line-card redundancy feature reduces the effect of service outages on network users and delivers increased network uptime at the IP/MPLS provider edge.

Availabilty Information

Table 1 gives availability information about the high-availability technology.

Table 1. Feature Availability

High-Availability Technology	Availability
Cisco IOS ISSU	Cisco 10000 – Since Cisco IOS Software Release 12.2(28)SB
BGP Nonstop Routing	Cisco 10000 – Since Cisco IOS Software Release 12.2(28)SB
MPLS NSF/SSO – MPLS LDP and LDP Graceful Restart	Cisco 10000 – Since 12.2(28)SB
MPLS NSF/SSO – MPLS VPN (including inter-autonomous system and CSC)	Cisco 7500 Series – Since 12.2(25)S
	Cisco 7304 Series – Since 12.2(25)S3
Line-Card Redundancy with Y-cables	Cisco 10000 4-Port, Half-Height, Channelized T3 Line Card – Since 12.2(28)SB

For More Information

For more information about Cisco IOS Software high-availability innovations, visit http://www.cisco.com/go/ or contact your local Cisco Systems® account representative.

CISCO 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 Website 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