

## CISCO IOS SOFTWARE RELEASE 12.2(18)SXD NEW FEATURES AND HARDWARE SUPPORT

### 1. CISCO IOS SOFTWARE RELEASE 12.2S INTRODUCTION

Cisco IOS<sup>®</sup> Software Release 12.2S is designed for Enterprise campus and Service Provider edge networks that require world-class IP and Multiprotocol Label Switching (MPLS) services. The Cisco Catalyst<sup>®</sup> Switches and high-end routers in Release 12.2S provide secure, converged network services in the most demanding Enterprise and Service Provider environments, from the wiring closet and data center to the WAN edge.

The infrastructure innovation and technology leadership in Release 12.2S enable advanced Ethernet LAN switching, Metro Ethernet, and Broadband Aggregation services through enhancements in High Availability, Security, MPLS, VPNs, and IP Routing and Services.

Releases 12.2(22)S, 12.2(20)S, 12.2(18)S, and 12.2(14)S are available from Cisco.com. For detailed information about the features and hardware supported in each of these releases, refer to Release 12.2S New Features and Hardware Support, Product Bulletin No. 2216.

Derived from Release 12.2(14)S, Release 12.2SX provides Release 12.2S functionality and new features and hardware support for the Cisco Catalyst 6500 Series Switch and Cisco 7600 Series Router.

In addition to Release 12.2(18)SXD, Releases 12.2(17d)SXB, 12.2(17b)SXA, 12.2(17a)SX, and 12.2(14)SX are available from Cisco.com. For detailed information about the features and hardware supported in each of these releases, please visit:

[http://www.cisco.com/en/US/products/sw/iosswrel/ps5012/prod\\_bulletins\\_list.html](http://www.cisco.com/en/US/products/sw/iosswrel/ps5012/prod_bulletins_list.html)

[http://www.cisco.com/en/US/products/hw/switches/ps708/prod\\_bulletins\\_list.html](http://www.cisco.com/en/US/products/hw/switches/ps708/prod_bulletins_list.html)

#### 1.1 Release 12.2SX Ordering Information, Feature Sets, and Image Names

Refer to the “Feature Sets” section of the Release 12.2SX release notes for information about Release 12.2SX orderable product numbers, feature sets, and image names.

[http://www.cisco.com/en/US/products/hw/switches/ps708/prod\\_release\\_note09186a00801c8339.html](http://www.cisco.com/en/US/products/hw/switches/ps708/prod_release_note09186a00801c8339.html)

[http://www.cisco.com/en/US/products/hw/switches/ps708/prod\\_release\\_note09186a008019e1e9.html](http://www.cisco.com/en/US/products/hw/switches/ps708/prod_release_note09186a008019e1e9.html)

#### 1.2 Additional Information

- Cisco IOS Software Release 12.2S  
<http://www.cisco.com/go/release122s/>
- Cisco IOS Software Release feedback and questions  
<http://www.cisco.com/warp/public/732/feedback/release/>

- Cisco IOS Software Product Lifecycle Dates & Milestones  
[http://www.cisco.com/en/US/products/sw/iosswrel/ps5187/prod\\_bulletin09186a00801a1349.html](http://www.cisco.com/en/US/products/sw/iosswrel/ps5187/prod_bulletin09186a00801a1349.html)
- Cisco IOS Software Center  
<http://www.cisco.com/public/sw-center/>

## 2. RELEASE 12.2(18)SXD HARDWARE AND FEATURE HIGHLIGHTS

Releases 12.2(18)SXD extends the benefits of Cisco IOS High Availability to Enterprise campus, data center, and WAN aggregation networks, and Service Provider edge aggregation networks that run the Cisco Catalyst 6500 Series Switch and Cisco 7600 Series Router. These enhancements provide nonstop application availability for Enterprise business-critical services, including supply-chain management, secure transactions, IP communications, and e-business. They also provide the network resiliency that Service Providers need to extend revenue through robust Service Level Agreements. This increased availability and resiliency reduces the total cost of ownership for Enterprise and Service Provider networks while also improving their overall productivity and efficiency.

Release 12.2(18)SXD adds support for the Cisco Catalyst 6500 Series Wireless LAN Services Module (WLSM), Cisco Nonstop Forwarding with Stateful Switchover, MPLS Traffic Engineering Fast Reroute, and many other additional new features.

Table 1 and the following sections highlight some of the key hardware and software features available in Release 12.2(18)SXD.

**Note:** Unless noted otherwise, the following highlighted features were first supported in Release 12.2SX as of Release 12.2(18)SXD. Subsequent releases of Release 12.2SX also support the highlighted features, and might include additional hardware support for the following highlighted features.

Cisco Feature Navigator, which requires an account on Cisco.com, dynamically updates the list of supported hardware as new hardware support is added for the features in the releases of Release 12.2SX. Cisco Feature Navigator can provide a cumulative list of all new and existing features supported in Release 12.2(18)SXD, including hardware and software image support.

**Table 1** Release 12.2(18)SXD Hardware and Feature Highlights

2.1 Hardware Support	2.2 Cisco IOS Infrastructure
2.1.1 Distributed Forwarding Cards for Cisco CEF256-Based Line Cards	2.2.1 Cisco Nonstop Forwarding with Stateful Switchover
2.1.2 Cisco Catalyst 6500 Series Wireless LAN Services Module	2.2.2 NetFlow Multiple Export Destinations
2.1.3 Cisco 10GBASE-CX4 XENPAK Module	2.2.3 Gateway Load Balancing Protocol
2.1.4 Cisco Receive-Only Wavelength-Division Multiplexing Gigabit Interface Converter	
2.1.5 Cisco 1000BASE-ZX Small Form-factor Pluggable	

**Table 1** Release 12.2(18)SXD Hardware and Feature Highlights (Continued)

2.3 IP Routing	2.4. MPLS and VPNs
2.3.1 IP Event Dampening 2.3.2 Routing Convergence Enhancements 2.3.2.1. Border Gateway Protocol Convergence Optimization 2.3.2.2. Border Gateway Protocol Dynamic Update Peer-Groups 2.3.2.3. Integrated Intermediate System-to-Intermediate System Incremental Shortest Path First Support 2.3.2.4. IS-IS Mechanism to Exclude Connected IP Prefix from LSP Advertisements 2.3.2.5. Open Shortest Path First Incremental Shortest Path First Support 2.3.2.6. Open Shortest Path First Support for Fast Hello Packets 2.3.2.7. Open Shortest Path First Support for Link State Advertisement Throttling	2.4.1. Multiprotocol Label Switching Traffic Engineering and Multiprotocol Label Switching Traffic Engineering Fast Reroute
2.5. Security	2.6 Multicast
2.5.1. Control Plane Policing 2.5.2. Secure Copy	2.6.1 SSM Mapping

## 2.1 Hardware Support

### 2.1.1 Distributed Forwarding Cards for Cisco CEF256-Based Line Cards

The Cisco<sup>®</sup> Catalyst<sup>®</sup> 6500 Series Distributed Forwarding Card 3 (DFC3), is an optional daughter card for CEF256-based line cards. The DFC3 provides localized forwarding decisions for each line card and scales the aggregate system performance. The new DFC3B and DFC3BXL offer enhancements to support Multiprotocol Label Switching (MPLS) and access control entries (ACE) counters on the Cisco Catalyst 65xx and Catalyst 68xx series line cards. The DFC3BXL also has improved scalability to support one million IPv4 routes and 256,000 NetFlow entries.

#### Benefits

- Support all features that WS-F6K-DFC3A currently supports
- Support MPLS and ACE counters
- DFC3BXL supports one million routes
- Deployed in CEF256 line cards such as WS-X6816-GBIC and WSX65XX line cards.

#### Hardware

<b>Routers</b>	Cisco 7600 series, Supervisor Engine 720
<b>Switches</b>	Cisco Catalyst Series, Supervisor Engine 720

#### Considerations

Requires Cisco IOS Software Release 12.2(18)SXD3 or later.

### Additional Information

Detailed information on DFC3

[http://www.cisco.com/en/US/products/hw/switches/ps708/prod\\_bulletins\\_list.html](http://www.cisco.com/en/US/products/hw/switches/ps708/prod_bulletins_list.html)

### Product Management Contact

[c6k-sw-pm@cisco.com](mailto:c6k-sw-pm@cisco.com)

### 2.1.2 Cisco Catalyst 6500 Series Wireless LAN Services Module

The Cisco Catalyst 6500 Series Wireless LAN Services Module (WLSM), part of the Cisco Catalyst 6500 Series of multilayer switches and a key component of the Cisco Structured Wireless-Aware Network (SWAN) framework, is the industry's only enterprise class wireless and wireline switching system, enabling secure, highly available, and easily managed unified networking deployments for enterprises, midsize businesses, universities, and service providers (Figure 1). By integrating wireless awareness into existing networks, customers can provide fast, secure campus-wide wireless Layer 3 roaming and can greatly simplify wireless deployments and ongoing network operations.

**Figure 1**

Cisco Catalyst 6500 Series WLSM



### Benefits

- Simplified management and reduced total cost of ownership
  - No changes to the client devices or underlying network infrastructure are required.
  - Common command-line interface (CLI), management tools, and software are used across wireless and wireline networks.
  - Fast secure roaming tunnels (FSRTs) are dynamically configured between Cisco Aironet Series access points and the Cisco Catalyst 6500 Series Switch equipped with a Cisco Catalyst 6500 Series WLSM.
- Industry's fastest secure Layer 3 mobility solution
  - Wireless users can roam from access point to access point across the campus with no loss of connectivity.
  - Access point to access point handoff times as low as 50 ms are supported (depending upon authentication type and client device capabilities).
  - No wireless traffic is permitted beyond the access point and into the FSRT until after the wireless user has successfully authenticated.

- Industry's most scalable WLAN solution
  - Support for up to 300 access points and 6000 wireless clients per Cisco Catalyst 6500 Series WLSM.
  - Cisco Catalyst 6500 Series Switch performance and bandwidth supports the expansion from pilot to full-scale deployment of hundreds of access points, including IEEE 802.11b and IEEE 802.11a/g dual-band radios that can far exceed the performance and capabilities of other “wireless appliances” or “wireless switches.”
- Secure segmentation of wireless users with up to 16 mobility groups
  - A single management interface on the Cisco Catalyst 6500 Series Switch manages all mobility groups, including up to 300 access points.
  - Security policies, such as IEEE 802.1X authentication types and access control lists (ACLs), can be defined on a per mobility group basis.
- Extends rich Cisco Catalyst 6500 Series features to wireless traffic
  - Layers 2 and 3 Catalyst 6500 Series Supervisor Non-Stop Forwarding/Stateful Switchover (NSF/SSO) extended to wireless traffic is supported.

**A full range of ACLs for traffic inspection, filtering, and rate limiting based on Layer 2 through 4 header information is supported.**

- Quality of Service (QoS) preservation and policy enforcement of all wireless traffic provided on a per mobility group basis.
- Hardware-based denial of service (DoS) protection mechanisms such as control plane rate limiters and Unicast Reverse Path Forwarding (uRPF) are included.
- Interoperability with intrusion detection, network analysis, IPsec VPN, and firewall services modules is supported.

#### Hardware

<b>Switches</b>	Cisco Catalyst 6500 Series, Supervisor Engine 720
-----------------	---

#### Additional Information

<http://www.cisco.com/en/US/products/ps5865/index.html>

#### Product Management Contact

- Vijay Sagar, [vsagar@cisco.com](mailto:vsagar@cisco.com)
- [ask-c6000-pm@cisco.com](mailto:ask-c6000-pm@cisco.com)

#### 2.1.3 Cisco 10GBASE-CX4 XENPAK Module

The range of Cisco 10GBASE XENPAK modules (CISCO XENPAK-10 GD-CX4) offers customers a wide variety of 10 Gigabit Ethernet connectivity options for data center, enterprise wiring closet, and service provider transport applications. The Cisco 10GBASE-CX4 Module provides 10Gb Ethernet connectivity and supports link lengths of up to 15 meters on CX4 cable.

## Benefits

- Optimized for 10 Gigabit Ethernet intra-rack connectivity—lowest cost 10GBASE connectivity option
- IEEE 802.3ak compliant for copper connectivity of up to 15m
- Hot swappable when deployed—the switch does not have to reboot
- Interchangeable—allows users the flexibility to deploy other 10GBASE Modules available from Cisco (including 10GBASE-SR, 10GBASE-LX4, 10GBASE-LR, and 10GBASE-ER)
- Supports the Cisco quality ID feature—users can easily identify whether the XENPAK module is a qualified and supported Cisco XENPAK module

## Hardware

<b>Routers</b>	Cisco 7600 Series, Supervisor Engine 720
<b>Switches</b>	Cisco Catalyst 6500 Series, Supervisor Engine 720

## Considerations

Initial support for the Cisco 10GBASE-CX4 Module is in Release 12.2(17d)SXB1.

## Product Management Contact

- Amy Chan, [camy@cisco.com](mailto:camy@cisco.com)
- [ask-c6000-pm@cisco.com](mailto:ask-c6000-pm@cisco.com)

### 2.1.4 Cisco Receive-Only Wavelength-Division Multiplexing Gigabit Interface Converter

The Cisco Receive-Only Wavelength-Division Multiplexing Gigabit Interface Converter (WDM-GBIC-REC) pluggable allows cable service providers to build optimized transport networks for video-on-demand applications. The Cisco Receive-Only WDM GBIC can be used as a pluggable receiver on any unidirectional link in a CWDM and/or DWDM transport network (Figure 2).

**Figure 2**

Cisco Receive-Only WDM GBIC



## Benefits

- Can be used as receiver for all wavelengths supported by Cisco CWDM and Cisco DWDM pluggable transceivers

- Provides high receive sensitivity
- Cost optimized for unidirectional links (no transmitter)
- Hot-swappable input device that plugs into Gigabit Ethernet GBIC ports or slots of a Cisco switch/router, linking the port with the network
- Can be used and interchanged on a wide variety of Cisco products and can be intermixed in combinations of 1000BASE-SX, 1000BASE-LX/LH, or 1000BASE-ZX on a port-by-port basis

#### Hardware

<b>Routers</b>	Cisco 7600 Series, Supervisor Engine 720, Supervisor Engine 2
<b>Switches</b>	Cisco Catalyst 6500 Series, Supervisor Engine 720, Supervisor Engine 2

#### Considerations

Initial support for the Cisco Receive-Only WDM GBIC is in Release 12.2(17d)SXB1.

#### Product Management Contact

- Amy Chan, [camy@cisco.com](mailto:camy@cisco.com)
- [ask-c6000-pm@cisco.com](mailto:ask-c6000-pm@cisco.com)

### 2.1.5 Cisco 1000BASE-ZX Small Form-factor Pluggable

#### Description

The Cisco industry-standard Small Form-factor Pluggable (SFP) Gigabit Interface Converter is a hot-swappable input/output device that plugs into a Gigabit Ethernet port or slot, linking the port with the network. SFPs can be used and interchanged on a wide variety of Cisco products and can be intermixed in combinations of 1000BASE-SX, 1000BASE-LX/LH, or 1000BASE-ZX on a port-by-port basis. As additional capabilities are developed, these modules make it easy to upgrade to the latest interface technology, maximizing investment protection.

The GLC-ZX-SM, 1000BASE-ZX SFP operates on ordinary single-mode fiber optic link spans of up to 70 kilometers (km) in length. Link spans of up to 100 km are possible using premium single-mode fiber or dispersion-shifted single-mode fiber. The SFP provides an optical link budget of 23 dB—the precise link span length will depend on multiple factors such as fiber quality, number of splices, and connectors.

When shorter distances of single-mode fiber are used, it may be necessary to insert an inline optical attenuator in the link, to avoid overloading the receiver. A 5-decibel (dB) or 10-dB inline optical attenuator should be inserted between the fiber optic cable plant and the receiving port on the GLC-ZX-SM at each end of the link whenever the fiber optic cable span is less than 25 km.

#### Hardware

<b>Switches</b>	Cisco Catalyst 6500 Series, Supervisor Engine 720
-----------------	---

#### Considerations

Initial support for the Cisco 1000BASE-ZX SFP is in Release 12.2(17d)SXB1.

### Additional Information

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122sx/index.htm>

### Product Management Contact

- Amy Chan, [camy@cisco.com](mailto:camy@cisco.com)
- [ask-c6000-pm@cisco.com](mailto:ask-c6000-pm@cisco.com)

## 2.2 Cisco IOS Infrastructure

### 2.2.1 Cisco Nonstop Forwarding with Stateful Switchover

Cisco Nonstop Forwarding (NSF) with Stateful Switchover (SSO) delivers seamless Supervisor Engine switchover and nonstop application availability for business-critical services in Enterprise campus, data center, and WAN aggregation networks, and Service Provider aggregation networks. SSO protects from hardware or software faults on an active Supervisor Engine by synchronizing Layer 2 protocol and state information with a standby Supervisor Engine. This ensures zero interruption of L2 connections in the event of a switchover (from the active to the standby Supervisor Engine). Network operators are informed of the cause of the switchover; however, applications and services are not reset (Figure 3).

**Figure 3**  
Cisco NSF with SSO for Supervisor Engine Switchover

#### Eliminates service disruptions

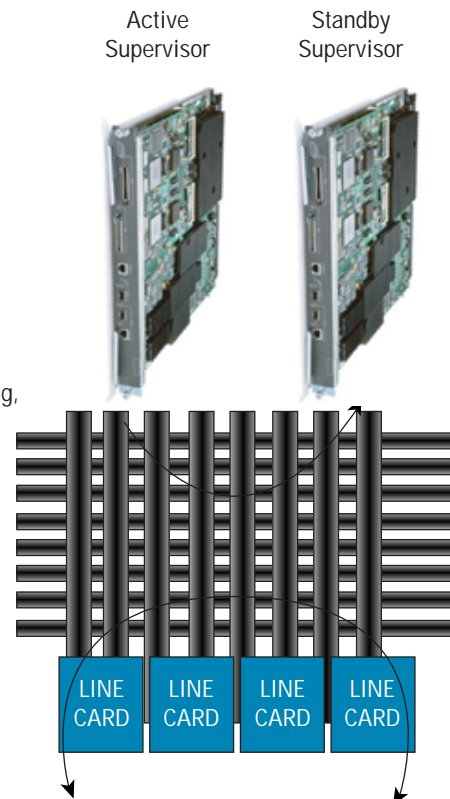
- Preserves user sessions and mitigates impacts of service outage on network users
- Increases network availability

#### Reduces costs

- Minimizes the costs associated with network downtime, such as loss of revenue, loss of productivity, damage to reputation, emergency network expenditures, and Service Level Agreement (SLA) penalties

#### Increases operational efficiency

- Reduces network administration, troubleshooting, and maintenance costs through increased network availability



SSO is particularly useful at the network edges. Traditionally, the core of the network is protected against network faults through the use of redundant devices and mesh connections that allow traffic to bypass failed network elements. SSO provides protection for network edge devices (with redundant Supervisor Engines or Route Processors) that represent a single point of failure in the network design, and where an outage might result in a loss of service for customers. SSO takes advantage of the redundant processors in a dual processor system by establishing one of the processors as active and the other as standby, and then synchronizing critical state information between them. After initial synchronization, SSO dynamically maintains state information between the active and standby processors. A switchover from the active to the standby processor occurs when the active processor fails, is removed from the networking device, or is manually taken down for maintenance. Since the standby processor has the Layer 2 protocol state information, it can communicate to its neighboring network devices after it takes control and becomes the active processor. Packet forwarding continues using known routes while routing protocol convergence is completed on the newly active processor. This continuous forwarding of packets is accomplished through Cisco NSF.

Cisco NSF works with SSO to minimize the amount of time a network is unavailable to its users following a switchover. Without Cisco NSF with SSO, when a networking device restarts, all routing peers of that device usually detect that the device went down and then came back up. This down-to-up transition results in what is called a “routing flap,” which could spread across multiple routing domains. Routing flaps caused by routing restarts create routing instabilities, which are detrimental to the overall network performance. Cisco NSF helps to suppress routing flaps due to processor restart or failure, 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 processor following a switchover. With Cisco NSF, peer networking devices do not experience routing flaps. Data traffic is forwarded through intelligent line cards, while the standby processor assumes control from the failed active processor during a switchover.

### Benefits

- Automatic fault detection and seamless recovery—SSO automatically detects a hardware or software fault in the active Supervisor Engine and allows the standby Supervisor Engine, which knows the state of the Layer 2 LAN as well as WAN connectivity protocols (eg: ATM, Frame Relay, Point-to-Point Protocol (PPP), and Cisco High-Level Data Link Control (HDLC)), to take control. Cisco NSF allows packet forwarding to continue with minimal or no packet loss while routing peer relationships are re-established and without requiring network-wide reconvergence for Border Gateway Protocol (BGP), Open Shortest Path First (OSPF), Intermediate System-to-Intermediate System (IS-IS), and Extended Interior Gateway Routing Protocol (EIGRP).
- No service disruption—By preserving user sessions, Cisco NSF with SSO mitigates the impact of service outages on network users and delivers increased network uptime.
- Reduced costs—Cisco NSF with SSO minimizes the costs associated with network downtime, such as loss of revenue, loss of productivity, damage to reputation, and reputation, emergency network expenditures, and Service Level Agreement (SLA) penalties.
- Increased operational efficiency—The enhanced availability and resiliency that Cisco NSF with SSO delivers helps to increase operational efficiency by reducing network troubleshooting and maintenance costs.

### Hardware

#### Routers

Cisco 7600 Series, Supervisor Engine 720, Supervisor Engine 2

### Considerations

Cisco NSF requires that layer 3 peer devices be NSF-aware, which means the peers are able to support dynamic protocol routing extensions or graceful restart capabilities.

### Additional Information

<http://www.cisco.com/go/grip/>

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122sx/index.htm>

### Product Management Contact

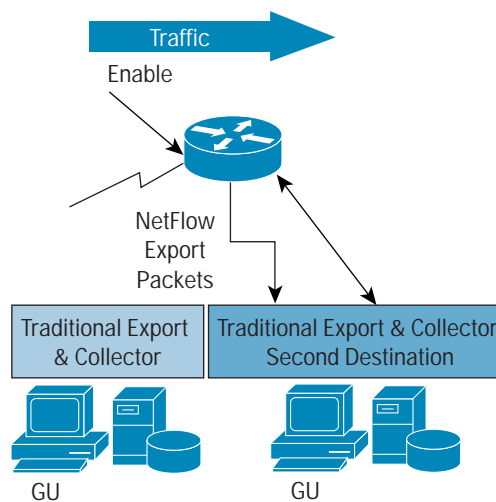
- Rohit Shrivastava, roshriva@cisco.com

### 2.2.2 NetFlow Multiple Export Destinations

Understanding who is using the network and for how long, what protocols and applications are being utilized, and where the network data is flowing is a necessity for today's IP networks managers. IP network managers rely on exported NetFlow data for a variety of purposes, including network management and planning, enterprise accounting, troubleshooting, security monitoring and departmental charge back billing, data warehousing, and data mining for marketing purposes.

The NetFlow Multiple Export Destinations feature enables configuration of multiple destinations of the NetFlow data. With this feature enabled, two identical streams of NetFlow data are sent to different destination hosts. Currently, the maximum number of export destinations allowed is two. The NetFlow Multiple Export Destinations feature helps assure high availability of NetFlow data export information (Figure 4).

**Figure 4**  
NetFlow Multiple Export Destinations



### Benefits

The NetFlow Multiple Export Destinations feature improves the chances of receiving complete NetFlow data by providing redundant streams of data. By sending the exact same export data to more than one NetFlow collector, fewer packets will be lost.

#### Hardware

<b>Routers</b>	Cisco 7600 Series, Supervisor Engine 2
<b>Switches</b>	Cisco Catalyst 6500 Series, Supervisor Engine 2

#### Additional Information

- <http://www.cisco.com/go/netflow/>
- [http://cisco.com/en/US/products/hw/switches/ps708/products\\_configuration\\_guide\\_chapter09186a008007e6f0.html](http://cisco.com/en/US/products/hw/switches/ps708/products_configuration_guide_chapter09186a008007e6f0.html)

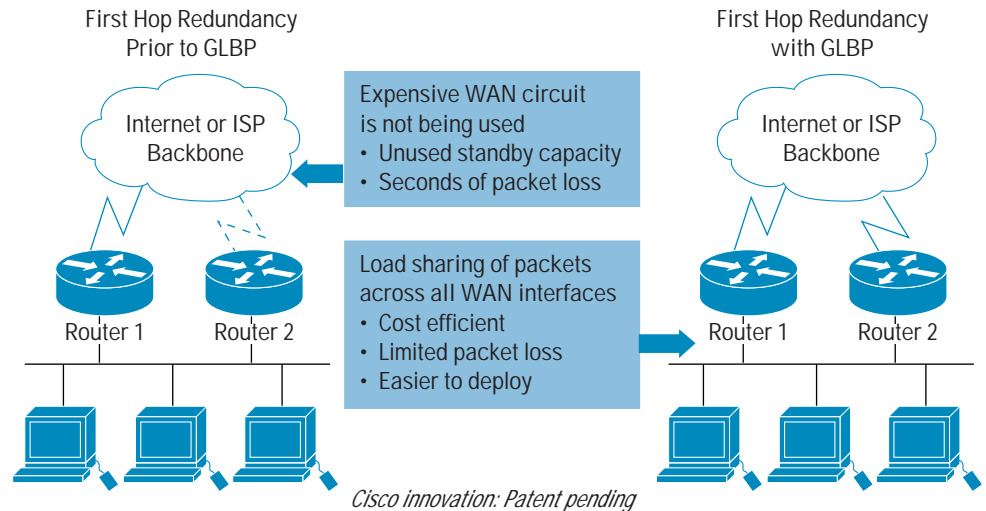
#### Product Management Contact

- Tom Zingale, [tomz@cisco.com](mailto:tomz@cisco.com)
- Martin McNealis, [mmcneali@cisco.com](mailto:mmcneali@cisco.com)

### 2.2.3 Gateway Load Balancing Protocol

Gateway Load Balancing Protocol (GLBP) is a Cisco innovation that uses available network bandwidth effectively by load sharing packets over all available paths while protecting the first hop router (Figure 5). Previously, first hop redundancy features only forwarded packets over the backup WAN paths if the primary router or primary path became unavailable. GLBP load balances IP traffic across multiple routers in the enterprise edge, thus improving network efficiency. Resilience and throughput are increased, as the enterprise backbone is no longer required to maintain standby routers in back-up mode with un-utilized WAN links. Customers that use Hot Standby Routing Protocol (HSRP) may find they double their site's available bandwidth without increasing their costs by enabling GLBP.

**Figure 5**  
Gateway Load Balancing Protocol



### Benefits

- Reduced costs—GLBP does not require a backup router on a dedicated data link, so enterprises no longer incur regular monthly costs for an unused backup data link or the one-time cost for the extra backup router.
- Efficient resource utilization—GLBP makes it possible for any router in a group to serve as a backup if needed. This eliminates the need for a dedicated backup router since all available routers can be used to support network traffic.
- Decreased administrative burden—Achieving similar performance is possible without GLBP, but it requires supporting multiple client gateway configurations. With GLBP, all clients are configured for the same gateway.

### Hardware

<b>Routers</b>	Cisco 7600 Series, Supervisor Engine 720, Supervisor Engine 2
<b>Switches</b>	Cisco Catalyst 6500 Series, Supervisor Engine 720, Supervisor Engine 2

### Considerations

GLBP was introduced into Release 12.2SX in Release 12.2(17d)SXB.

### Additional Information

<http://www.cisco.com/go/grip/>

### Product Management Contact

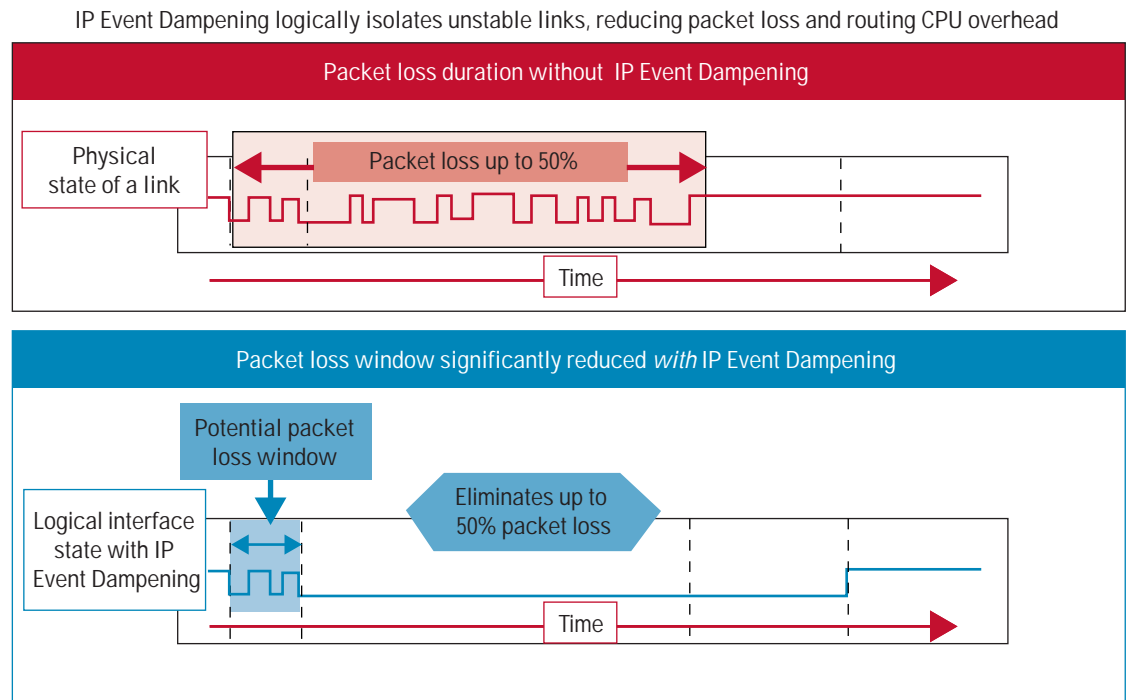
- Mark Denny, [mdenny@cisco.com](mailto:mdenny@cisco.com)
- Amir Khan, [akhan@cisco.com](mailto:akhan@cisco.com)

## 2.3 IP Routing

### 2.3.1 IP Event Dampening

IP Event Dampening allows a router to police itself on each network interface, to ensure that only stable circuits and connections remain active (Figure 6). Sometimes faulty fibers, poor connections, or other problems can force a network circuit to temporarily break connectivity then quickly gain connectivity again. This is called a “link flap”. A routing device responds by finding an alternate path for its packet flows. When availability appears to be restored, the routing device may try to use the circuit again. This “flapping” can cause unnecessary packet loss and network jitter. If “flapping” continues, a Cisco router with IP Event Dampening will take the interface out of operation until the interface indicates it is behaving appropriately. This creates a more stable environment for the entire network, reduces network jitter, and can reduce packet loss by 50%.

**Figure 6**  
IP Event Dampening



#### Benefits

- IP Event Dampening delivers resiliency improvements.
- Faster convergence. Routers that are not experiencing link flap reach convergence sooner, as routing tables are not rebuilt each time the offending router leaves and enters service.

- Increased network stability. A router with data-link problems removes itself from service until the data link is consistently stable, so other routers simply redirect traffic around the affected router until data-link issues are resolved, thus ensuring that the router loses no data packets.

#### Hardware

<b>Routers</b>	Cisco 7600 Series, Supervisor Engine 720, Supervisor Engine 2
<b>Switches</b>	Cisco Catalyst 6500 Series, Supervisor Engine 720, Supervisor Engine 2

#### Additional Information

<http://www.cisco.com/go/grip/>

#### Product Management Contact

- Rohit Shrivastava, roshriva@cisco.com

### 2.3.2 Routing Convergence Enhancements

Convergence is the speed and ability of a group of internetworking devices running a specific routing protocol to agree on the topology of an internetwork after a change in that topology. Sections 2.2.2.2.1 through 2.2.2.2.7 highlight the routing convergence enhancements in Release 12.2(18)SXD1.

#### 2.3.2.1. Border Gateway Protocol Convergence Optimization

Border Gateway Protocol (BGP) Convergence Optimization is a new algorithm for update generation that reduces the amount of time that is required for BGP convergence. Neighbor update messages are optimized before they are forwarded to neighbors. Updates are optimized and forwarded based on peer groups and per-individual neighbors. This enhancement improves BGP convergence, router boot time, and transient memory usage. This enhancement is not user configurable.

#### Hardware

<b>Routers</b>	Cisco 7600 Series, Supervisor Engine 720, Supervisor Engine 2
<b>Switches</b>	Cisco Catalyst 6500 Series, Supervisor Engine 720, Supervisor Engine 2

#### Additional Information

<http://www.cisco.com/warp/public/732/Tech/routing/>

#### Product Management Contact

- Chetan Khetani, cpk@cisco.com
- Pepe Garcia, pepe@cisco.com

#### 2.3.2.2. Border Gateway Protocol Dynamic Update Peer-Groups

The Border Gateway Protocol (BGP) Dynamic Update Peer-Groups feature introduces a new algorithm that dynamically calculates and optimizes update-groups of neighbors that share the same outbound policies and can share the same update messages. In previous versions of Cisco IOS Software, BGP update messages were grouped

together based on peer-group configurations. This method of grouping updates limited outbound policies and specific-session configurations. The BGP Dynamic Update Peer-Groups feature separates update-group replication from peer-group configuration, which improves convergence time and flexibility of neighbor configuration.

#### Hardware

<b>Routers</b>	Cisco 7600 Series, Supervisor Engine 720, Supervisor Engine 2
<b>Switches</b>	Cisco Catalyst 6500 Series, Supervisor Engine 720, Supervisor Engine 2

#### Additional Information

<http://www.cisco.com/warp/public/732/Tech/routing/>

#### Product Management Contact

- Chetan Khetani, [cpk@cisco.com](mailto:cpk@cisco.com)
- Pepe Garcia, [pepe@cisco.com](mailto:pepe@cisco.com)

#### **2.3.2.3. Integrated Intermediate System-to-Intermediate System Incremental Shortest Path First Support**

Integrated Intermediate System-to-Intermediate System (IS-IS) Incremental SPF allows the system to recalculate only the affected part of the shortest path tree. Recalculating only a portion of the tree rather than the entire tree results in faster IS-IS convergence and saves CPU resources.

#### Hardware

<b>Routers</b>	Cisco 7600 Series, Supervisor Engine 720, Supervisor Engine 2
<b>Switches</b>	Cisco Catalyst 6500 Series, Supervisor Engine 720, Supervisor Engine 2

#### Additional Information

<http://www.cisco.com/warp/public/732/Tech/routing/>

#### Product Management Contact

- Chetan Khetani, [cpk@cisco.com](mailto:cpk@cisco.com)
- Pepe Garcia, [pepe@cisco.com](mailto:pepe@cisco.com)

#### **2.3.2.4. IS-IS Mechanism to Exclude Connected IP Prefix from LSP Advertisements**

In order to speed up IS-IS convergence, the number of IP prefixes carried in LSPs needs to be limited. Configuring interfaces as unnumbered limits the prefixes. However, for network management reasons, one might want to have numbered interfaces and also want to prevent advertising interface addresses into IS-IS. The IS-IS Mechanisms to Exclude Connected IP Prefixes from LSP Advertisements feature provides two methods to avoid the overpopulation of routing tables and thereby reduce IS-IS convergence time.

#### Hardware

<b>Routers</b>	Cisco 7600 Series, Supervisor Engine 720, Supervisor Engine 2
<b>Switches</b>	Cisco Catalyst 6500 Series, Supervisor Engine 720, Supervisor Engine 2

#### Additional Information

<http://www.cisco.com/warp/public/732/Tech/routing/>

#### Product Management Contact

- Chetan Khetani, [cpk@cisco.com](mailto:cpk@cisco.com)
- Pepe Garcia, [pepe@cisco.com](mailto:pepe@cisco.com)

#### **2.3.2.5. Open Shortest Path First Incremental Shortest Path First Support**

The Open Shortest Path First (OSPF) Incremental SPF Support feature allows the system to recalculate only the affected part of the shortest path tree. Recalculating only a portion of the tree, rather than the entire tree, results in faster OSPF convergence and saves CPU resources.

#### Hardware

<b>Routers</b>	Cisco 7600 Series, Supervisor Engine 720, Supervisor Engine 2
<b>Switches</b>	Cisco Catalyst 6500 Series, Supervisor Engine 720, Supervisor Engine 2

#### Additional Information

<http://www.cisco.com/warp/public/732/Tech/routing/>

#### Product Management Contact

- Chetan Khetani, [cpk@cisco.com](mailto:cpk@cisco.com)
- Pepe Garcia, [pepe@cisco.com](mailto:pepe@cisco.com)

#### **2.3.2.6. Open Shortest Path First Support for Fast Hello Packets**

The Open Shortest Path First (OSPF) Support for Fast Hello Packets feature provides a way to configure the sending of hello packets in intervals less than one second. Such a configuration results in faster convergence in an OSPF network. Fast hellos are especially useful in LAN segments.

#### Hardware

<b>Routers</b>	Cisco 7600 Series, Supervisor Engine 720, Supervisor Engine 2
----------------	---

## Switches

Cisco Catalyst 6500 Series, Supervisor Engine 720, Supervisor Engine 2

### Additional Information

<http://www.cisco.com/warp/public/732/Tech/routing/>

### Product Management Contact

- Chetan Khetani, [cpk@cisco.com](mailto:cpk@cisco.com)
- Pepe Garcia, [pepe@cisco.com](mailto:pepe@cisco.com)

#### 2.3.2.7. Open Shortest Path First Support for Link State Advertisement Throttling

The OSPF Link-State Advertisement (LSA) Throttling feature provides a dynamic mechanism to slow down LSA updates in OSPF during times of network instability. It also allows faster OSPF convergence by providing LSA rate limiting in milliseconds.

### Hardware

## Routers

Cisco 7600 Series, Supervisor Engine 720, Supervisor Engine 2

## Switches

Cisco Catalyst 6500 Series, Supervisor Engine 720, Supervisor Engine 2

### Additional Information

<http://www.cisco.com/warp/public/732/Tech/routing/>

### Product Management Contact

- Chetan Khetani, [cpk@cisco.com](mailto:cpk@cisco.com)
- Pepe Garcia, [pepe@cisco.com](mailto:pepe@cisco.com)

## 2.4. MPLS and VPNs

### 2.4.1. Multiprotocol Label Switching Traffic Engineering and Multiprotocol Label Switching Traffic Engineering Fast Reroute<sup>1</sup>

Cisco IOS Multiprotocol Label Switching (MPLS) fuses the intelligence of routing with the performance of switching, providing significant benefits to networks with a pure IP architecture as well as those with IP, ATM or a mixture of other Layer 2 technologies.

MPLS Traffic Engineering was initially envisioned as technology that would enable Service Providers to better utilize available network bandwidth by using alternate paths (i.e. other than the shortest path). It has evolved to provide multiple benefits, including connectivity protection using Fast Reroute (FRR).

With MPLS Traffic Engineering FRR, Service Providers can now reroute MPLS label switched paths around any link or node failure with full traffic recovery rates as fast as 50 milliseconds. FRR protects primary tunnels by using pre-provisioned backup tunnels. These backup tunnels protect MPLS label-switched paths (LSPs) from link and node failures by locally repairing the LSPs at the point of failure, allowing data to continue to flow on them while their head-end routers attempt to establish new end-to-end LSPs as replacements.

1. Support is planned for a future update to Release 12.2(18)SXD

## Benefits

- **Node Protection**—Backup tunnels that terminate at the next-next hop protect both the downstream link and node. This provides protection for link and node failures.
- **Multiple Backup Tunnels Can Protect the Same Interface**—In addition to being required for Node Protection, this enhancement provides the following benefits:
  - **Redundancy**—If one backup tunnel is down, other backup tunnels protect LSPs.
  - **Increased backup capacity**—If the protected interface is a high-capacity link and no single backup path exists with an equal capacity, multiple backup tunnels can protect that one high-capacity link.
- **Bandwidth Protection**—Rerouted LSPs not only have their packets delivered during a failure, but the quality of service can also be maintained.
- **Scalability**—A backup tunnel can protect multiple LSPs. Furthermore, a backup tunnel can protect multiple interfaces. This is called many-to-one (N:1) protection. N:1 protection has significant scalability advantages over one-to-one (1:1) protection, where a separate backup tunnel must be used for each LSP needing protection. N:1 protection is not new with Node Protection; it existed with Link Protection.
- **Support for RSVP Hellos**—RSVP Hello allows a router to detect when its neighbor has gone down but its interface to that neighbor is still operational. When Layer 2 link protocols are unable to detect that the neighbor is unreachable, Hellos provide the detection mechanism; this allows the router to switch LSPs onto its backup tunnels and avoid packet loss.

## Hardware

<b>Routers</b>	Cisco 7600 Series, Supervisor Engine 720
<b>Switches</b>	Cisco Catalyst 6500 Series, Supervisor Engine 720

## Additional Information

<http://www.cisco.com/go/mpls/>

### Product Management Contact

Azhar Sayeed, [asayeed@cisco.com](mailto:asayeed@cisco.com)

## 2.5. Security

### 2.5.1. Control Plane Policing

Even the most robust software implementations and hardware architectures are vulnerable to Denial of Service (DoS) attacks. DoS attacks are malicious acts designed to cause failures in a network infrastructure by flooding it with worthless traffic camouflaged as specific types of control packets directed at the control plane processor. By involving hundreds of sources, distributed DoS attacks multiply the amount of worthless IP traffic, sometimes by as much as many gigabytes per second. These IP streams contain packets that are destined for processing by the control plane of Cisco route processors. Based on the high rate of rogue packets presented to the route processor, the control plane must spend an inordinate amount of time processing and discarding the DoS traffic.

Control Plane Policing provides users with a mechanism to control the type and rate of traffic that hits the control-plane of the device, and thereby helps to maintain packet forwarding and protocol states while the router is under attack. Control Plane Policing leverages Modular Quality of Service (QoS) CLI (MQC) to provide a programmable policing functionality on routers that filter and rate limit (or police) traffic destined to the control plane. This policing functionality can be used in conjunction with Cisco IOS QoS classification mechanisms to identify and limit certain traffic types completely, or to target only those that exceed a specified threshold level.

### Benefits

- Streamlines incoming rate of traffic destined to the control plane
- Protects against attacks targeted towards the network infrastructure
- Easily defines global policy commands to address the aforementioned security goals using the Cisco MQC infrastructure

### Hardware

Routers	Cisco 7600 Series Router
Switches	Cisco Catalyst 6500 Series Switch

### Additional Information

[http://www.cisco.com/en/US/products/ps6642/products\\_ios\\_protocol\\_group\\_home.html](http://www.cisco.com/en/US/products/ps6642/products_ios_protocol_group_home.html)

### Product Management Contact

IOS-Security-PM@cisco.com

### 2.5.2. Secure Copy

#### Description

The Secure Copy (SCP) feature provides a secure and authenticated method for copying router configuration or router image files.

#### Benefits

SCP allows a user who has appropriate authorization to copy any file that exists in the Cisco IOS File System (IFS) to and from a router by using the copy command. An authorized administrator may also perform this action from a workstation.

### Hardware

Routers	Cisco 7600 Series, Supervisor Engine 720, Supervisor Engine 2
Switches	Cisco Catalyst Series, Supervisor Engine 720, Supervisor Engine 2

### Additional Information

<http://www.cisco.com/go/iossecurity/>

#### **Product Management Contact**

IOS-Security-pm@cisco.com

## **2.6 Multicast**

### **2.6.1 SSM Mapping**

The Source Specific Multicast (SSM) Mapping feature extends the Cisco IOS suite of SSM transition tools which also includes URL Rendezvous Directory (URD) and Internet Group Management Protocol v3lite. SSM Mapping supports SSM transition in cases where neither URD nor IGMPv3lite are available, or when supporting SSM on the end system is impossible or unwanted due to administrative or technical reasons. SSM mapping enables you to leverage SSM for video delivery to legacy Set Top Boxes that do not support SSM.

#### **Benefits**

SSM mapping enables you to leverage SSM for video delivery to legacy Set Top Boxes that do not support SSM. In addition to the SSM benefits which are largely shared when using SSM mapping, full SSM provides the benefit of avoiding the need for IP Multicast address management. The SSM Mapping feature provides the same level of protection from denial of service (DoS) attacks as SSM.

#### **Hardware**

<b>Routers</b>	Cisco 7600 series, Supervisor Engine 720
<b>Switches</b>	Cisco Catalyst 6500 Series, Supervisor Engine 720

#### **Considerations**

In Cisco IOS Software Release 12.2(18)SXD3, SSM Mapping feature has the following limitations:

1. IGMPv1, IGMPv2 and IGMPv3 hosts have to be put in separate vlans.
2. Safe-reporting will not interact with SSM Mapping.

#### **Additional Information (URLs)**

Detailed information on SSM mapping

[http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products\\_feature\\_guide09186a00801a6d6f.html#1077274](http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_feature_guide09186a00801a6d6f.html#1077274)

#### **Product Management Contact**

c6k-sw-pm@cisco.com

## CISCO SYSTEMS



Corporate Headquarters  
Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
[www.cisco.com](http://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](http://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](http://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](http://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](http://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

All contents are Copyright © 1992-2004 Cisco Systems, Inc. All rights reserved. Cisco, Cisco IOS, Cisco Systems, and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company.  
(0403R) ETMG\_203032.3\_SH\_12.04