



Cisco Globally Resilient IP Overview and Applications

Version History

Version Number	Date	Notes
Initial	July 2002	This document was created.

Overview

Cisco Globally Resilient IP in Cisco IOS software addresses resiliency as a network-wide challenge that must be solved both at the device level and across the network as a whole, with resiliency built into multiple IP services.

Cisco Globally Resilient IP is a portfolio of technologies in Cisco IOS software that enables network-wide resilience to increase IP network availability. Users can select the best Globally Resilient IP features from this portfolio in order to achieve maximum redundancy and scalability on their networks.

Network application traffic must cross different segments, from the enterprise backbone, enterprise edge, and service provider (SP) edge through the SP core. All segments must be resilient enough to recover quickly from faults and to prevent faults from affecting user activities and network applications. A fault anywhere in the network can result in termination, interruption, or violation of Service Level Agreements (SLAs) for business-critical applications.

With Cisco Globally Resilient IP, network hardware and software work together and enable rapid recovery from disruptions to ensure fault transparency to users and network applications. These features are offered on existing Cisco IOS platforms and currently deployed hardware.

This document describes the following key Cisco Globally Resilient IP features in the initial release, and it also provides high-level examples showing how to deploy these features in different network environments:

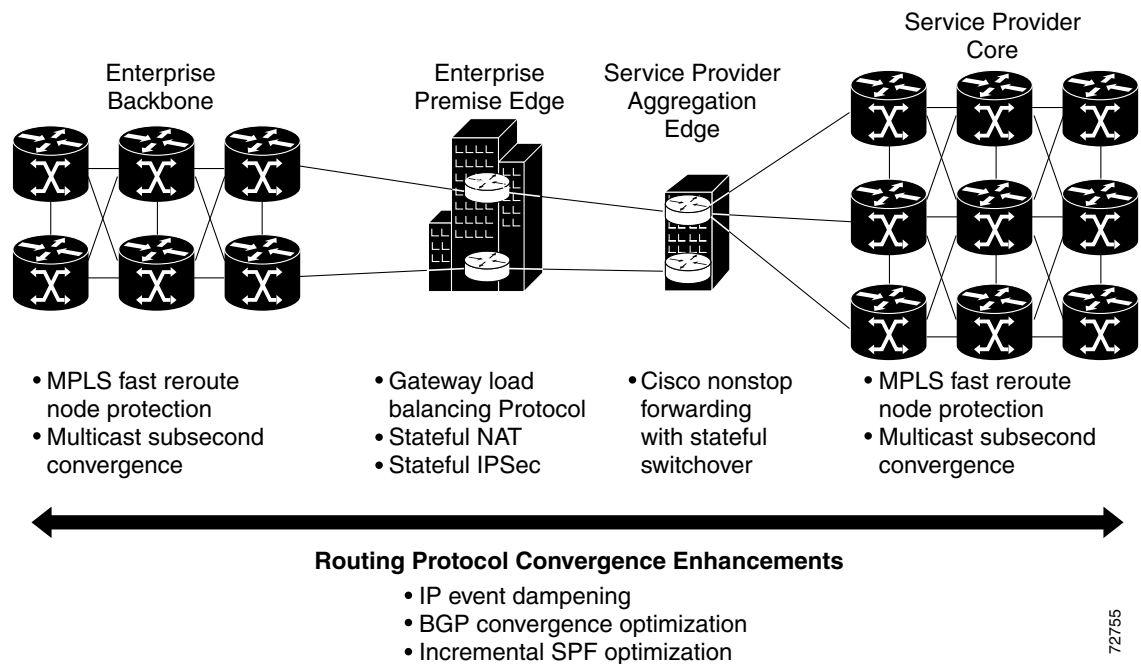
- Cisco nonstop forwarding (NSF) with stateful switchover (SSO)
- IP event dampening
- Border Gateway Protocol (BGP) convergence optimization
- Multicast subsecond convergence
- Multiprotocol Label Switching (MPLS) fast reroute node protection

FINAL DRAFT - CISCO CONFIDENTIAL

Cisco nonstop forwarding (NSF) with stateful switchover (SSO) enables continuous packet forwarding during a Route Processor (RP) takeover and route convergence. SSO allows a backup RP to take immediate control from the active RP while maintaining WAN connectivity protocols. The MPLS fast reroute node protection and multicast subsecond convergence features work on the enterprise backbone and the SP core, and IP event dampening and BGP convergence optimization provide routing protocol convergence enhancements to the Cisco Globally Resilient IP network.

Figure 1 provides a high-level look at how Globally Resilient IP features are applied in global network environments.

Figure 1 Cisco IP Technology Solutions for Globally Resilient IP



Edge Resiliency Features

Cisco NSF with SSO enables the fastest time to recovery for IP networks from hardware or software faults in an RP in the industry. Cisco IOS provides zero IP packet loss for an instantaneous RP switchover on a Cisco 12000 series Internet router, eliminating the aggregation router of an SP as a single point of failure. This breakthrough is highly important because a loss of connectivity at the aggregation edge, which often terminates hundreds of customers and thousands of sessions, has a direct impact on customer SLAs.

Network Resiliency Features

Incremental enhancements to routing protocols improve convergence times, reduce network overhead, and increase resiliency end-to-end across the network. Globally Resilient IP has several key network resiliency enhancements, which are described in the following sections:

- [IP Event Dampening](#)

FINAL DRAFT - CISCO CONFIDENTIAL

- [Border Gateway Protocol Convergence Optimization](#)

IP event dampening improves convergence times and stability throughout the network by isolating faults so that disturbances are not propagated.

New BGP convergence optimization improves convergence time 40 percent for the largest BGP production environments.

Enterprise Backbone and Service Provider Core Features

The multicast subsecond convergence feature enhances the enterprise backbone, and the MPLS fast reroute node protection feature enhances the SP core.

For both enterprise and SP networks, multicast subsecond convergence provides almost instantaneous recovery of multicast paths after unicast routing recovery.

For MPLS traffic engineering environments, MPLS fast reroute now provides a node protection solution to rapidly reroute traffic in case of node (MPLS label switch router) fault, joining existing fast reroute link protection capability, to provide recovery times competitive with SONET.

Cisco Globally Resilient IP

Cisco Globally Resilient IP addresses resiliency as a network-wide challenge that must be solved both at the device level and across the network as a whole, with resiliency built into multiple IP services.

SP and enterprise customers with large IP networks benefit from increased resiliency in the backbone or core and at the network edge, which is often a single point of failure for network connectivity. Further optimization of IP routing protocols improves efficiency and stability across the network.

The rest of this document describes the features in the following sections in detail by closely examining the various network topologies in which they are deployed:

- [Edge Resiliency](#)
- [Network-Wide Resiliency](#)
- [Enterprise Backbone and Service Provider Core Resiliency](#)

Edge Resiliency

An edge access device represents the first hop in a customer network connection. Often, customers have a single circuit between their customer premise router and the edge access router. If an edge router fails, many customer connections become unavailable until the access router recovers. By contrast, core networks include routers configured in dual, mesh configurations, so traffic can take an alternate route if one transmission path is disrupted.

Traditionally, core routers protect against network faults using router redundancy and mesh connections that allow traffic to bypass failed network elements. SSO provides protection for network edge devices with redundant processors that represent a single point of failure in the network design, and where an outage might result in loss of service for customers.

SSO is used in conjunction with Cisco NSF. Cisco NSF allows for the forwarding of data packets to continue along known routes while the routing protocol information is being restored during a switchover. The Cisco NSF and SSO features are described in the following sections:

- [Cisco Nonstop Forwarding](#)

FINAL DRAFT - CISCO CONFIDENTIAL

- [Stateful Switchover](#)

Cisco Nonstop Forwarding

A component of Cisco Globally Resilient IP is Cisco NSF, which is a complementary feature to the SSO feature in Cisco IOS software. Cisco NSF works with SSO to minimize the amount of time a network is unavailable to its users following a switchover. The main objective of Cisco NSF is to ensure that IP packets continue to be forwarded following an RP switchover.

All routing peers of a device that restarts detect that the device went down and then came back up. This 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 with SSO reduces and, on the Cisco 12000 series Internet router, eliminates packet loss caused by either hardware or software faults on an RP.

Cisco NSF allows for the forwarding of data packets to continue along known routes while the routing protocol information is being restored following a switchover. With Cisco NSF, peer networking devices do not experience routing flaps. Data traffic is forwarded through intelligent line cards or dual forwarding processors (FPs) while the standby RP takes control from a compromised active RP through an RP switchover. The ability of line cards and FPs to remain up through a switchover is key to Cisco NSF operation.

**Note**

Cisco NSF always runs together with SSO. For further information on SSO, see the section “[Stateful Switchover](#).”

Cisco NSF Routing and Forwarding Operation

Cisco NSF supports BGP, Open Shortest Path First (OSPF), and Intermediate System-to-Intermediate System (IS-IS) protocols for routing and Cisco Express Forwarding (CEF) for forwarding. Routers running these protocols can detect a switchover and take the necessary actions to continue forwarding network traffic and to recover route information from the peer devices. The IS-IS protocol is also configurable to use state information that has been synchronized between the active and the standby RP to recover route information following a switchover instead of information received from peer devices. In this document, a networking device is said to be Cisco-NSF-aware if it is running Cisco-NSF-compatible software; a device is said to be Cisco-NSF-capable if it has been configured to support Cisco NSF.

Each protocol depends on CEF to continue forwarding packets during switchover while the routing protocols rebuild the routing information base (RIB) tables. Once the routing protocols have converged, CEF updates the forwarding information base (FIB) table and removes stale route entries. CEF, in turn, updates the line cards with the new FIB information.

Cisco Express Forwarding

A key element of Cisco NSF is packet forwarding. In a Cisco networking device, packet forwarding is provided by CEF. CEF maintains the FIB, and uses the FIB information that was current at the time of the switchover to continue forwarding packets during a switchover. This feature reduces any traffic interruption during the switchover.

FINAL DRAFT - CISCO CONFIDENTIAL

During normal Cisco NSF operation, CEF on the active RP synchronizes its current FIB and adjacency databases with the FIB and adjacency databases on the standby RP. Upon switchover of the active RP, the standby RP initially has FIB and adjacency databases that are mirror images of those that were current on the active RP. For platforms with intelligent line cards, the line cards will maintain the current forwarding information over a switchover; for platforms with forwarding engines, CEF will keep the forwarding engine on the standby RP current with changes that are sent to it by CEF on the active RP. In this way, the line cards or forwarding engines will be able to continue forwarding after a switchover as soon as the interfaces and a data path are available.

As the routing protocols start to repopulate the RIB on a prefix-by-prefix basis, the updates in turn cause prefix-by-prefix updates to CEF, which CEF then uses to update the FIB and adjacency databases. Existing and new entries will receive the new version (“epoch”) number, indicating that they have been refreshed. The forwarding information is updated on the line cards or forwarding engine during convergence. The RIB signals when the routing protocols have converged, and CEF removes all FIB and adjacency entries that have an epoch older than the current switchover epoch. The FIB now represents the newest routing protocol forwarding information.

Routing Protocols

The routing protocols run only on the active RP, and they receive routing updates from their neighbor routers. Routing protocols do not run on the standby RP. Following a switchover, the routing protocols request that the Cisco-NSF-aware neighbor devices send state information to help rebuild the routing tables. Alternately, the IS-IS protocols can be configured to synchronize state information from the active to the standby RP to help rebuild the routing table on the Cisco-NSF-capable device in environments where neighbor devices are not Cisco-NSF aware.

**Note**

For Cisco NSF operation, the routing protocols depend on CEF to continue forwarding packets while the routing protocols rebuild the routing information.

BGP Operation

When a Cisco-NSF-capable router begins a BGP session with a BGP peer, it sends an OPEN message to the peer. Included in the message is a declaration that the Cisco-NSF-capable device has “graceful restart” capability. Graceful restart is the mechanism by which BGP routing peers avoid a session routing flap following a switchover. If the BGP peer has received this capability, it is aware that the device sending the message is Cisco-NSF-capable.

If the BGP session is lost during the RP switchover, the Cisco-NSF-aware BGP peer marks all the routes associated with the Cisco-NSF-capable router as stale; however, it continues to use these routes to make forwarding decisions for a set period of time. This functionality means that no packets are lost while the newly active RP is waiting for convergence of the routing information with the BGP peers.

After an RP switchover occurs, the Cisco-NSF-capable router reestablishes the session with the BGP peer. In establishing the new session, it sends a new graceful restart message that identifies the Cisco-NSF-capable router as having restarted, as opposed to establishing a new BGP session.

At this point, the routing information is exchanged between the two BGP peers. Once this exchange is complete, the Cisco-NSF-capable device uses the network information to update the RIB and the FIB with the new forwarding information. The Cisco-NSF-aware device uses the network information to remove stale routes from its BGP table. The BGP protocol is then fully converged.

FINAL DRAFT - CISCO CONFIDENTIAL

If a BGP peer does not support the graceful restart capability, it will ignore the graceful restart capability in an OPEN message but will establish a BGP session with the Cisco-NSF-capable device. This capability will allow interoperability with non-Cisco-NSF-aware BGP peers (and without Cisco NSF functionality).

**Note**

BGP NSF requires that neighbor networking devices be Cisco-NSF aware and Cisco-NSF capable. If a Cisco-NSF-capable router discovers that a particular BGP neighbor does not have Cisco NSF capability, it will not establish a Cisco-NSF-capable session with that neighbor. All other neighbors that have BGP NSF capability will continue to have Cisco-NSF-capable sessions with this Cisco-NSF-capable networking device.

The following example shows NSF for BGP in the running configuration:

Configuration Example 1: NSF for BGP

```
router bgp 101
  bgp graceful-restart restart-time 120
  bgp graceful-restart stalepath-time 360
  bgp graceful-restart
  neighbor 172.16.10.1 remote-as 100
  neighbor 172.16.10.3 remote-as 200
```

In this example, the Cisco NSF feature is enabled for BGP. The router will advertise graceful restart capability to neighbor 172.16.10.1 on a remote AS100 and 172.16.10.3 on a remote AS200. The restart-time value is set to 120 seconds, which is the default value (the restart-time value indicates how long peers will wait to delete all stale routes before receiving an OPEN message from the restarting router).

The stalepath-time value is set to 360 seconds, which is the default value. The stalepath-time value indicates how long a router will wait before it deletes all stale routes after an end of record (EOR) message is received from the restarting router.

OSPF Operation

When an OSPF NSF-capable router performs an RP switchover, it must perform two tasks in order to resynchronize its link-state database with its OSPF neighbors. First, it must relearn the available OSPF neighbors on the network without causing a reset of the neighbor relationship. Second, it must reacquire the contents of the link-state database for the network.

As quickly as possible after an RP switchover, the Cisco-NSF-capable router sends an OSPF NSF signal to neighboring Cisco-NSF-aware devices. Neighbor networking devices recognize this signal as a cue that the neighbor relationship with this router should not be reset. As the Cisco-NSF-capable router receives signals from other routers on the network, it can begin to rebuild its neighbor list.

Once neighbor relationships are reestablished, the Cisco-NSF-capable router begins to resynchronize its database with all of its Cisco-NSF-aware neighbors. At this point, the network information is exchanged between the OSPF neighbors. Once this exchange is complete, the Cisco-NSF-capable device uses the adjacency information to remove stale routes, update the RIB, and update the FIB with the new forwarding information. The OSPF protocols are then fully converged.

FINAL DRAFT - CISCO CONFIDENTIAL**Note**

OSPF NSF requires that all neighbor networking devices be Cisco-NSF aware. If a Cisco-NSF-capable router discovers that it has non-Cisco-NSF-aware neighbors on a particular network segment, it will disable Cisco NSF capabilities for that segment. Other network segments composed entirely of Cisco-NSF-capable or Cisco-NSF-aware routers will continue to provide NSF capabilities.

The following example shows NSF for OSPF in the running configuration:

Configuration Example 2: NSF for OSPF

```
router ospf 1
 log-adjacency-changes
 nsf
 network 10.102.0.0.0.255 255 area 0
```

This configuration enables the Cisco NSF feature for OSPF.

IS-IS Operation

When an IS-IS NSF-capable router performs an RP switchover, it must perform two tasks in order to resynchronize its link-state database with its IS-IS neighbors. First, it must relearn the available IS-IS neighbors on the network without causing a reset of the neighbor relationship. Second, it must reacquire the contents of the link-state database for the network.

The IS-IS NSF feature offers two options when configuring Cisco NSF:

- IETF IS-IS
- Cisco IS-IS

If neighbor routers on a network segment are Cisco-NSF-aware, meaning that neighbor routers are running a software version that supports the IETF Internet draft for router restartability, you can configure IS-IS NSF for Internet Engineering Task Force (IETF). With IETF, neighbor routers provide adjacency and link state information to help rebuild the routing information following a switchover. A benefit of IETF IS-IS configuration is standards-based operation between peer devices.

**Note**

If you configure IETF on the networking device, but neighbor routers are not IETF-compatible, Cisco NSF will not abort following a switchover; however, user connections supported by incompatible devices will experience routing flaps.

If the neighbor routers on a network segment are not Cisco-NSF aware, you must use the Cisco configuration option. The Cisco IS-IS configuration transfers both protocol adjacency and link-state information from the active to the standby RP. A benefit of Cisco configuration is that it does not rely on Cisco-NSF-aware neighbors.

IETF IS-IS Configuration

Using the IETF IS-IS configuration, as quickly as possible after an RP switchover, the Cisco-NSF-capable router sends IS-IS NSF restart requests to neighboring Cisco-NSF-aware devices. Neighbor networking devices recognize this restart request as a cue that the neighbor relationship with this router should not be reset, but that they should initiate database resynchronization with the restarting router. As the restarting router receives restart request responses from routers on the network, it can begin to rebuild its neighbor list.

FINAL DRAFT - CISCO CONFIDENTIAL

Once this exchange is complete, the Cisco-NSF-capable device uses the link-state information to remove stale routes, update the RIB, and update the FIB with the new forwarding information. IS-IS is then fully converged.

The switchover from one RP to the other happens within seconds. IS-IS reestablishes its routing table and resynchronizes with the network within a few additional seconds. At this point, IS-IS waits for a specified interval before it will attempt a second Cisco NSF restart. During this time, the new standby RP will boot up and synchronize its configuration with the active RP. The IS-IS NSF operation waits for a specified interval time to ensure that connections are stable before attempting another restart of IS-IS NSF. This function prevents IS-IS from attempting back-to-back Cisco NSF restarts with stale information.

Cisco IS-IS Configuration

Using the Cisco configuration option, full adjacency and link-state packet (LSP) information is saved, or “checkpointed,” to the standby RP. Following a switchover, the newly active RP maintains its adjacencies using the checkpointed data, and can quickly rebuild its routing tables.

**Note**

Following a switchover, Cisco IS-IS NSF has complete neighbor adjacency and LSP information; however, it must wait for all interfaces that had adjacencies prior to the switchover to come up. If an interface does not come up within the allocated interface wait time, the routes learned from these neighbor devices are not considered in routing table recalculation. Cisco IS-IS NSF provides a command to extend the wait time for interfaces that, for whatever reason, do not come up in a timely fashion.

Cisco NSF Benefits

- Prevents routing flaps—Because SSO continues forwarding network traffic in the event of a switchover, routing flaps are avoided.
- No loss of user sessions—User sessions established prior to the switchover are maintained.
- Neighboring routers do not detect a link flap—Because the interfaces remain up across a switchover, neighboring routers do not detect a link flap (the link does not go down and come back up).
- Improved network stability—Network stability may be improved with the reduction in the number of route flaps that are created if routers in the network fail and lose their routing tables.

Cisco NSF Ramifications

To run OSPF, BGP NSF, or IETF IS-IS, all neighboring network devices must be running a Cisco-NSF-aware software image. If you have a mixed environment, you may need to switch to a homogeneous environment to gain the maximum benefit from these protocols.

Cisco NSF Application

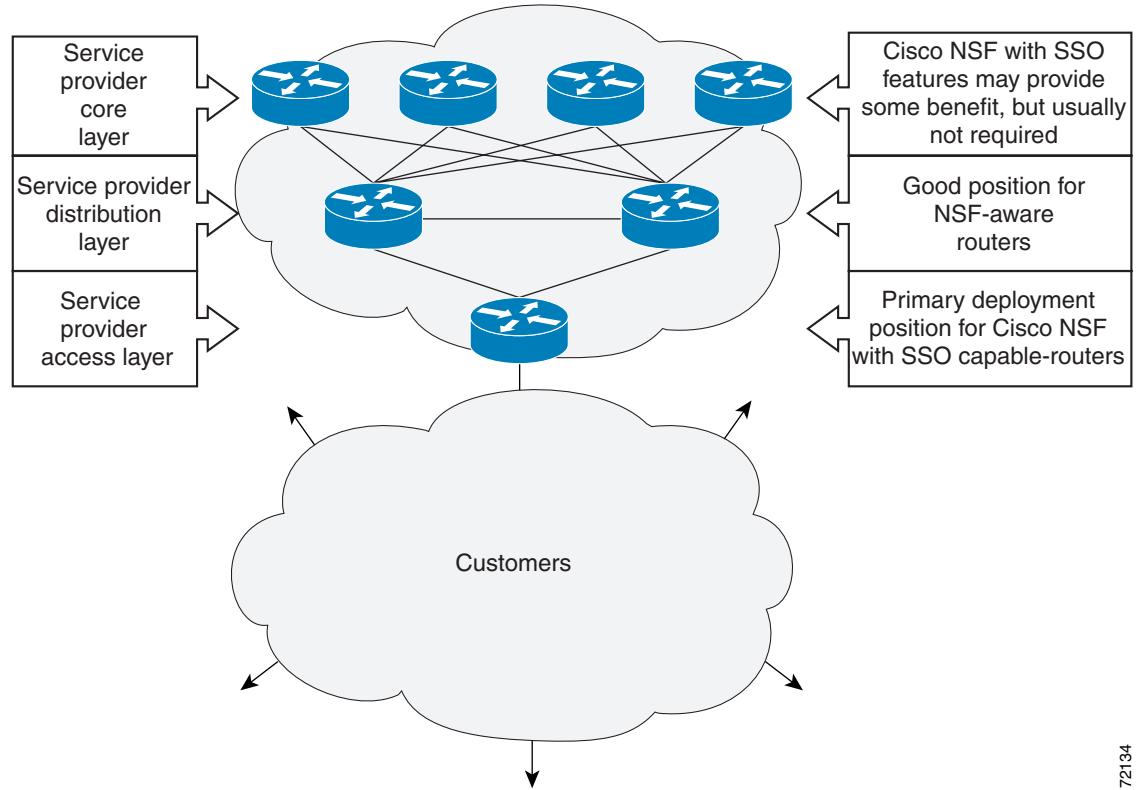
Using Cisco NSF with SSO is particularly useful at the network edge. The routers on the network edge are responsible for many WAN connections and often represent a single point of failure. Keeping these connections alive is necessary to protect against hardware or software RP fault.

FINAL DRAFT - CISCO CONFIDENTIAL

Figure 2 illustrates how SSO is typically deployed in SP networks. In this example, SSO and Cisco NSF are primarily at the access layer (edge) of the SP network. A fault at this point could result in loss of service for enterprise customers requiring access to the SP network.

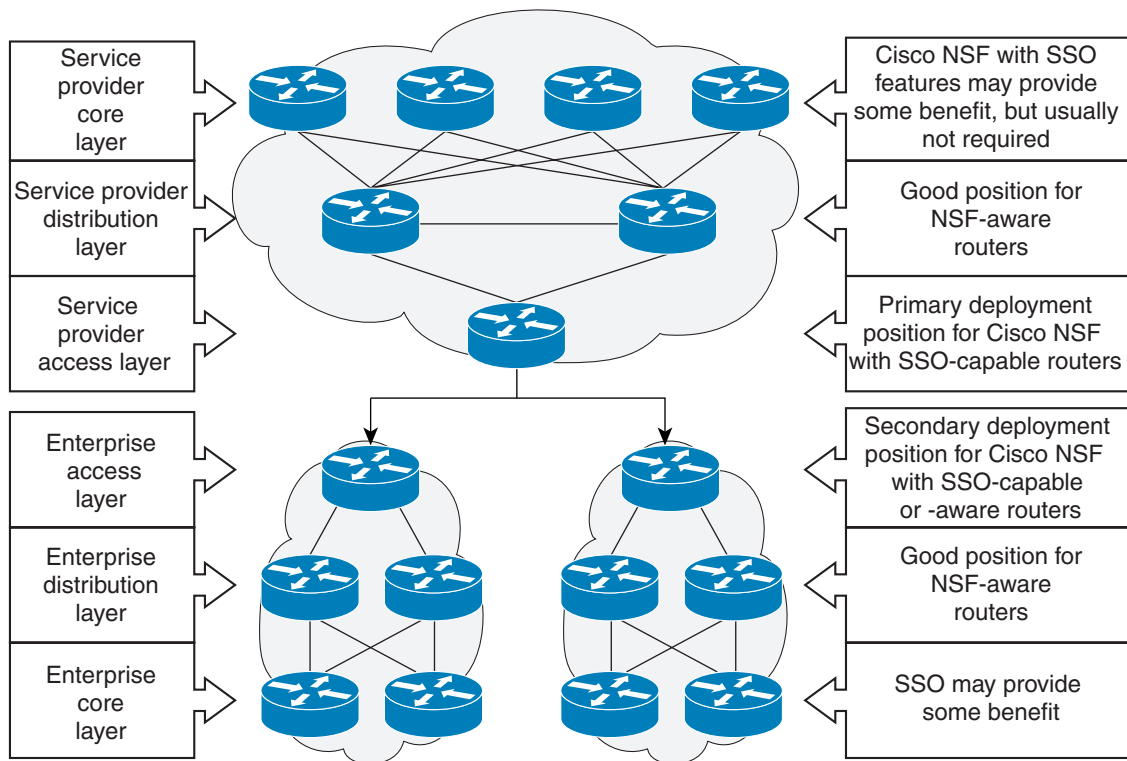
Notice that Figure 2 shows that neighbor routers must be NSF-aware in order for NSF to work. If the neighbor routers are not NSF-aware, the connection is broken.

Figure 2 Cisco NSF with SSO Network Deployment—Service Provider Network



For Cisco NSF protocols that require neighboring devices to participate in Cisco NSF, Cisco-NSF-aware software images must be installed on those neighboring distribution layer devices. Additional network availability benefits might be achieved by applying Cisco NSF with SSO features at the core layer of your network; consult your network design engineers to evaluate your specific site requirements.

Additional levels of availability may be gained deploying SSO and Cisco NSF at other points in the network where a single point of failure exists. Figure 3 illustrates an optional deployment strategy that applies SSO and Cisco NSF at the enterprise network access layer. In this example, each access point in the enterprise network represents another single point of failure in the network design. In the event of a switchover or a planned software upgrade, enterprise customer sessions would continue uninterrupted through the network.

FINAL DRAFT - CISCO CONFIDENTIAL**Figure 3 Cisco NSF with SSO Network Deployment Option—Enterprise Network**

Stateful Switchover

The SSO feature in Cisco Globally Resilient IP works with Cisco NSF in Cisco IOS software on Cisco networking device platforms. The main objective of SSO is to improve the availability of networks constructed with Cisco IOS routers.

Using Cisco NSF with SSO is particularly useful at the network edge. Traditionally, core routers protect against network faults using router redundancy and mesh connections that allow traffic to bypass failed network elements. SSO provides protection for network edge devices with RPs that represent a single point of failure in the network design, and where an outage might result in loss of service for customers.

In specific Cisco networking devices that support dual RPs, SSO takes advantage of RP redundancy to increase network availability. The SSO feature takes advantage of RP redundancy by establishing one of the RPs 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 them.

A switchover from the active to the standby processor occurs when the active RP fails, is removed from the networking device, or is manually taken down for maintenance.

Figure 2 illustrates how SSO is typically deployed in SP networks. In this example, SSO and Cisco NSF are primarily at the access layer (edge) of the SP network. A fault at this point could result in loss of service for enterprise customers requiring access to the SP network.

FINAL DRAFT - CISCO CONFIDENTIAL

For Cisco NSF protocols that require neighboring devices to participate in Cisco NSF, Cisco-NSF-aware software images must be installed on those neighboring distribution layer devices. Additional network availability benefits might be achieved by applying Cisco NSF with SSO features at the core layer of your network; consult your network design engineers to evaluate your specific site requirements.

Additional levels of availability may be gained deploying SSO and Cisco NSF at other points in the network where a single point of failure exists. [Figure 3](#) illustrates an optional deployment strategy that applies SSO and Cisco NSF at the enterprise network access layer. In this example, each access point in the enterprise network represents another single point of failure in the network design. In the event of a switchover or a planned software upgrade, enterprise customer sessions would continue uninterrupted through the network.

Synchronization

In networking devices running SSO, the configuration is synchronized so that the standby RP is always ready to assume control if the active RP fails.

To achieve the benefits of SSO, synchronize the configuration information from the active RP to the standby RP at startup and whenever changes to the active RP configuration occur. This synchronization occurs in two separate phases:

- While the standby RP is booting, the configuration information is synchronized in bulk from the active RP to the standby RP.
- When configuration or state changes occur, an incremental synchronization from the active RP to the standby RP is conducted.

Bulk Synchronization During Initialization

When a system with SSO is initialized, the active RP performs a chassis discovery (discovery of the number and type of line cards and fabric cards, if available, in the system) and parses the startup configuration file. The active RP then synchronizes this data to the standby RP and instructs the standby RP to complete its initialization. This method ensures that both RPs contain the same configuration information.

Incremental Synchronization

After both RPs are fully initialized, any further changes to the running configuration or active RP states are synchronized to the standby RP as they occur. Active RP states are updated as a result of processing protocol information, external events (such as the interface becoming up or down), or user configuration commands (using command-line interface [CLI] commands or Simple Network Management Protocol [SNMP]) or other internal events.

Switchover Operation

During switchover, system control and routing protocol execution are transferred from the active to the standby RP. Switchover may be due to a manual operation (CLI-invoked) or to a software- or hardware-initiated operation (hardware or software fault induced).

FINAL DRAFT - CISCO CONFIDENTIAL

SSO-Supported Protocols 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 high-availability-aware protocols and applications (such as PPP, Frame Relay, ATM, and SNMP) 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.

SSO-aware applications are either platform-independent, such as in the case of line protocols (Frame Relay, ATM, and PPP) or platform-dependent (such as line card drivers). Enhancements to the routing protocols (CEF, OSPF, and BGP) have been made in the SSO feature to prevent loss of peer adjacency through a switchover. These enhancements are platform-independent.

Line Protocols

SSO-aware line protocols synchronize session state information between the active and standby RPs to keep session information current for a particular interface. In the event of a switchover, session information need not be renegotiated with the peer. During a switchover, SSO-aware protocols also check the line card state to learn if it matches the session state information. SSO-aware protocols use the line card interface to exchange messages with network peers in an effort to maintain network connectivity.

SSO is supported in ATM, Frame Relay, PPP, and high-level data link control (HDLC).

Line Card Drivers

Platform-specific line card device drivers are bundled with the Cisco IOS software image for SSO and are correct for a specific image, meaning they are designed to be SSO-aware.

Line cards used with the SSO feature periodically generate status events that are forwarded to the active RP. Information includes the line up or down status, and the alarm status. This information helps SSO support bulk synchronization after standby RP initialization and support state reconciliation and verification after a switchover.

Line cards used with the SSO feature have the following requirements:

- Line cards must not reset.
- Line cards must not be reconfigured.
- Subscriber sessions may not be lost.
- Line cards must clear statistics to zero.

The standby RP communicates only with the active RP, never with the line cards. This function helps to ensure that the active and standby RP always have the same information.

SSO Benefits

- Improved network availability—Because SSO maintains protocol and application state information, user session information is maintained after a switchover, meaning that line cards continue to forward network traffic with no loss of sessions.

FINAL DRAFT - CISCO CONFIDENTIAL

- Improved switchover time—SSO provides a faster switchover relative to high system availability (HSA), Route Processor Redundancy (RPR), and Route Processor Redundancy Plus (RPR+) by fully initializing and fully configuring the standby RP, and by synchronizing state information, which can reduce the time required for routing protocols to converge.
- Zero interruption—SSO provides zero interruption of Layer 2 connections from virtually any hardware or software fault.
- Improved continuity—SSO provides enhanced continuity for ATM, Frame Relay, PPP, Multilink PPP, HDLC, and Ethernet.

SSO Ramifications

SSO need not be configured on neighboring devices. However, Cisco NSF requires that all neighboring network devices be running a Cisco-NSF-aware software image. If you have a mixed environment, you may need to switch to a homogeneous environment to run any of these protocols.

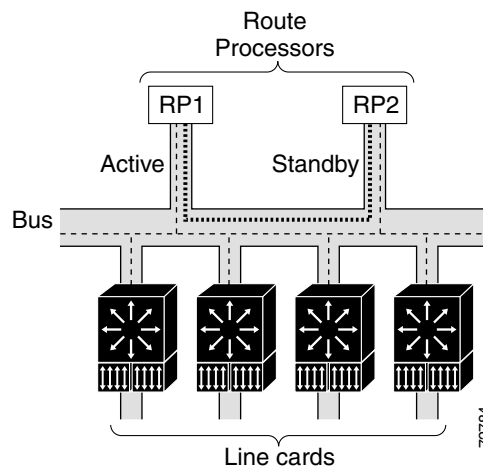
SSO Application

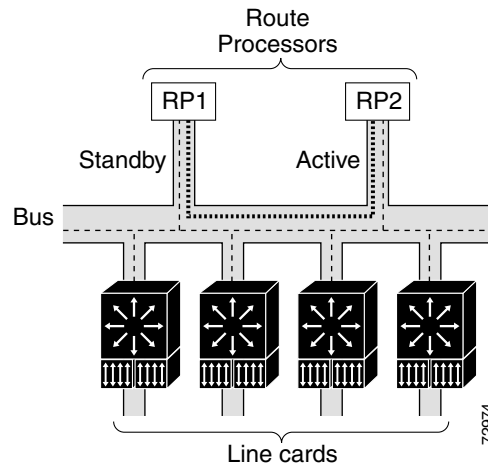
The use of the Cisco Globally Resilient IP SSO feature is critical for routers on the network edge. The routers on the network edge are responsible for many WAN connections and are often a single point of failure. Keeping these connections alive is necessary to protect against hardware or software RP fault and to support Cisco NSF.

On the Cisco 12000 series Internet router, Cisco NSF provides zero packet loss for the edge and the core. It provides protection from hardware or software faults and prevents route flaps from occurring between participating neighbor routers. This feature allows peering relationships to be reestablished, and it allows transparent route convergence to occur.

Figure 4 and Figure 5 illustrate how Cisco NSF with SSO work together to provide resilient routing. SSO enables zero interruption to Layer 2 sessions and packet forwarding. The active RP synchronizes information with the standby RP. The standby RP immediately takes control when the active RP is compromised in some way, at which point the standby RP becomes the active RP.

Figure 4 Resilient Routing: Stateful Switchover Before a Switchover Occurs



FINAL DRAFT - CISCO CONFIDENTIAL**Figure 5** Resilient Routing: Stateful Switchover After a Switchover—Standby Is Now Active

The following example shows SSO in the running configuration:

Configuration Example 3: Stateful Switchover

```

redundancy
 mode sso

```

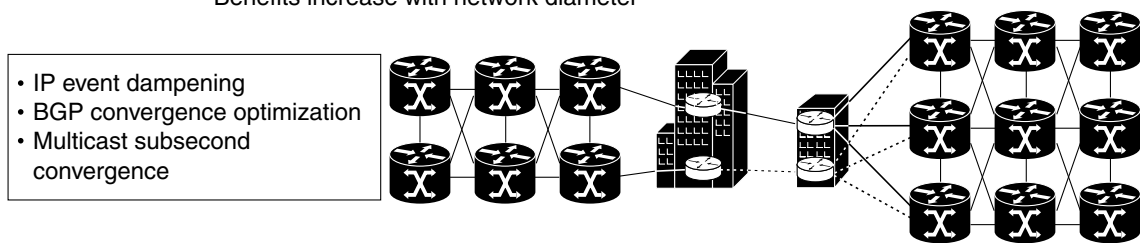
Network-Wide Resiliency

Resilient routing allows routing protocols to recover quickly from a network fault such as a failed router or circuit. The goal is to recover instantaneously from faults without network disruption. Service providers cannot afford to have real-time applications and business services wait for the network to fix itself using existing methods.

Figure 6 shows Globally Resilient IP features that enhance fast network convergence.

FINAL DRAFT - CISCO CONFIDENTIAL**Figure 6 Fast Network Convergence**

- Ability of a network to quickly converge is critical to the delivery of uninterrupted real-time services
- Cisco has pioneered routing protocol enhancements to achieve fast convergence:
 - Event handling
 - BGP — Batched updates
 - OSPF and IS-IS — Localizing updates
 - Multicast — Fast convergence
- Benefits for both unicast and multicast routing
- Benefits increase with network diameter



The Cisco Globally Resilient IP features described in the following sections enhance network recovery, allowing instant recovery on network systems that use Cisco Globally Resilient IP:

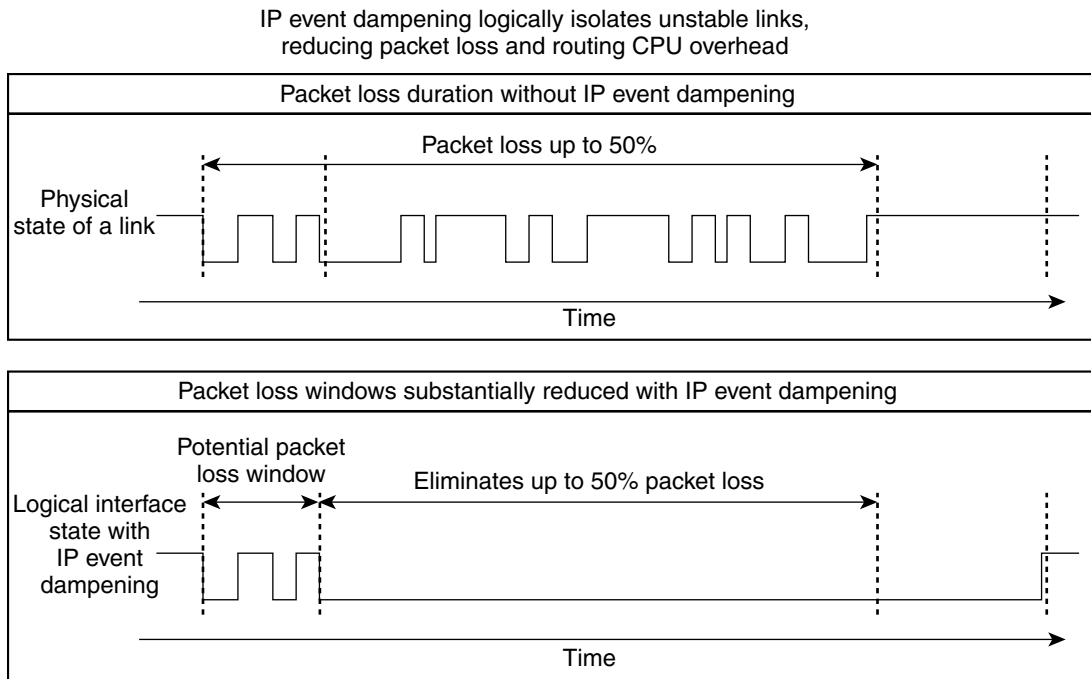
- [IP Event Dampening](#)
- [Border Gateway Protocol Convergence Optimization](#)

IP Event Dampening

Currently, a router with an unstable data link (“link flap”) may remove itself and return to service several times in a matter of seconds, requiring all other routers to rebuild their routing tables with each event. IP event dampening enables a router experiencing link flap to selectively remove itself from network routing tables until a return to data-link stability is ensured. This function ensures that only stable circuits and connections remain active. In order for IP event dampening to work, an alternate path must be provided in case of a fault.

A Cisco router with IP event dampening takes the affected interface out of operation until it resumes normal behavior. The Cisco router first waits a predefined period of time to see if the data link remains stable before removing itself from service. After the router removes itself from service, it waits another predefined period of time after the data link is restored to ensure that the link is stable before returning to service. Administrators may set the thresholds at which the router removes itself from and returns itself to service.

[Figure 7](#) provides a comparison of packet loss information on routers that have the IP event dampening feature and those routers that do not.

FINAL DRAFT - CISCO CONFIDENTIAL**Figure 7 IP Event Dampening**

IP Event Dampening Benefits

- Faster convergence—Routers that are not experiencing link flap reach convergence sooner, because routing tables are not rebuilt each time the offending router leaves and enters service.
- Increased network stability—A router with data-link problems removes the affected routes from service until the data link is consistently stable, so other routers simply redirect traffic using alternative routes until data-link issues are resolved, thus minimizing packet loss.

IP Event Dampening Ramifications

The following protocols will work with IP event dampening:

- IP routing protocols, including static route, Routing Information Protocol (RIP), OSPF, IS-IS, Interior Gateway Routing Protocol (IGRP), Enhanced IGRP (EIGRP), and BGP
- Connectionless Network Protocol (CLNS) routing protocol (which is IS-IS; IS-IS supports both IP and CLNS)
- Cisco Hot Standby Routing Protocol (HSRP)

IP Event Dampening Application

The IP event dampening Cisco Globally Resilient IP feature is necessary because service providers cannot afford to have real-time applications and business services wait long periods of time for the network to fix itself after a fault.

FINAL DRAFT - CISCO CONFIDENTIAL

The following example shows IP event dampening in the running configuration:

Configuration Example 4: IP Event Dampening

```
interface Serial 3/0
dampening 2 500 5000 10
```

In this example, IP event dampening is enabled on serial interface 3/0. The interface is suppressed after five quick consecutive flappings.

Border Gateway Protocol Convergence Optimization

BGP is the routing protocol used to communicate among all the global Internet networks. Because of its importance in the Internet, BGP is a major focus for scaling and convergence work.

As an Internet routing table grows, SPs and large enterprise customers are noticing a dramatic increase in the length of time BGP takes to converge. Networks that once converged in 10 or 15 minutes may now take up to 1 hour and even longer in extreme situations.

Several BGP enhancements have been made to improve convergence and basic scaling properties. These enhancements include using peer groups, configuring TCP path Maximum Transmission Unit (MTU) discovery, and creating larger input queues.

BGP Convergence Optimization Benefits

- Faster convergence—Given the current number of routing table entries, BGP converges up to 40 percent faster with Cisco Globally Resilient IP enhancements.
- Increased scalability—BGP enhancements and configuration recommendations allow users to handle greater numbers of routing table entries within the same convergence time frame.
- Benefits are maximized if a large number of updates needs to be sent and a peer group is used.

BGP Convergence Optimization Ramifications

A new algorithm to improve BGP convergence needs approximately 15 MB of available memory for performing caching and formatting of BGP update messages. These memory requirements should not be a problem for most high-end routers. If a router does not have enough memory, the router will use the old algorithm to send BGP update messages.

BGP Convergence Optimization Application

This Cisco Globally Resilient IP feature is necessary because service providers cannot afford to have real-time applications and business services wait long periods of time for the network to fix itself after a fault.

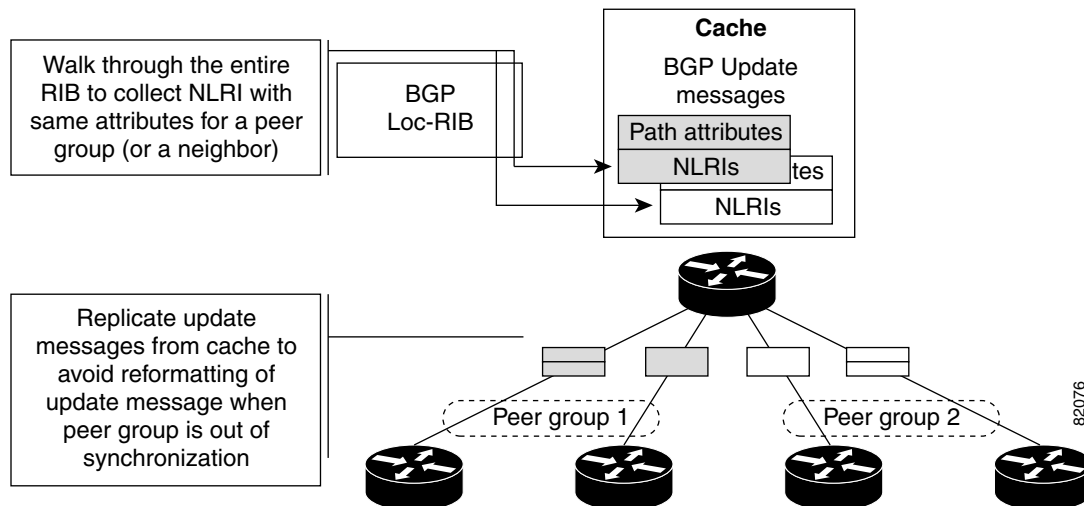
This feature does not require configuration; it is included with the Cisco IOS 12.0(22)S software release. However, TCP MTU discovery needs to be enabled. The following example enables TCP path MTU discovery for the router:

FINAL DRAFT - CISCO CONFIDENTIAL**Configuration Example 5: TCP MTU Discovery**

```
ip tcp path-mtu-discovery
```

Figure 8 shows how this feature works.

Figure 8 BGP Boot Convergence Time



Enterprise Backbone and Service Provider Core Resiliency

SP and enterprise customers with large IP networks benefit from increased resiliency in the backbone and core and at the network edge. Further optimization of IP routing protocols through Globally Resilient IP features improves efficiency and stability across the network.

In Cisco Globally Resilient IP, the multicast subsecond convergence feature enhances the enterprise backbone, and the MPLS fast reroute node protection feature enhances the SP core.

Multicast Subsecond Convergence

The Multicast Subsecond Convergence feature in Cisco IOS Release 12.0(22)S comprises a comprehensive set of features and protocol enhancements that provide for improved scalability and convergence in multicast-based services. This feature set provides for the ability to scale to larger services levels and to recover multicast forwarding after service failure in subsecond time frames.

Multicast subsecond convergence allows you to send Protocol Independent Multicast (PIM) router-query messages (PIM hellos) every few milliseconds. In previous releases, you could send the PIM hellos every few seconds. By enabling a router to send PIM hello messages more often, this feature allows the router to discover unresponsive neighbors more quickly. As a result, the router can implement failover or recovery procedures more efficiently.

FINAL DRAFT - CISCO CONFIDENTIAL

The Multicast Subsecond Convergence feature set enhances both enterprise and service provider network backbones by providing almost instantaneous recovery of multicast paths after unicast routing recovery. Forwarding performance is unaffected by this new feature and is comparable to previous releases of Cisco IOS software.

Because PIM relies on the unicast routing table to calculate its Reverse Path Forwarding (RPF) when a change in the network topology occurs, unicast protocols first need to calculate options for the best paths for traffic, and then multicast can determine the best path.

Multicast subsecond convergence allows multicast protocol calculations to finish almost immediately after the unicast calculations are completed. As a result, multicast traffic forwarding is restored substantially faster after a topology change.

The scalability enhancements improve on the efficiency of handling increases (or decreases) in service users (receivers) and service load (sources or content). Scalability enhancements in this release include the following:

- Improved Internet Group Management Protocol (IGMP) and PIM state maintenance through new timer management techniques
- Improved scaling of the Multicast Source Discovery Protocol (MSDP) Source-Active (SA) cache

The scalability enhancements provide the following benefits:

- Increased potential PIM multicast route (mroute), IGMP, and MSDP SA cache state capacity
- Decreased CPU usage

Multicast subsecond convergence provides the ability to trigger a check of RPF changes for mroute states. This check is triggered by unicast routing changes. By performing a triggered RPF check, users can set the periodic RPF check to a relatively high value (for example, 10 seconds) and still fail over quickly.

The triggered RPF check enhancement reduces the time needed for service to be restored after disruption, such as for single service events (for example, in a situation with one source and one receiver) or as the service scales along any parameter (for example, many sources, many receivers, and many interfaces). This enhancement decreases in time-to-converge PIM (mroute), IGMP, and MSDP (SA cache) states.

Multicast Subsecond Convergence Benefits

- The scalability components improve on the efficiency of handling increases (or decreases) in service users (receivers) and service load (sources or content).
- New algorithms and processes (such as aggregated join messages, which deliver up to 1000 individual messages in a single packet) reduce the time to reach convergence by a factor of 10.
- Multicast subsecond convergence improves service availability for large multicast networks.
- Multicast users such as financial services firms and brokerages receive better quality of service, as multicast functionality is restored in a fraction of the time previously required.

Multicast Subsecond Convergence Application

The multicast subsecond convergence feature is used in financial, entertainment, and interactive gaming applications.

FINAL DRAFT - CISCO CONFIDENTIAL**MPLS Fast Reroute for Node Protection**

The MPLS fast reroute for node protection feature in Cisco Globally Resilient IP delivers intelligent path protection to the network core for MPLS-based Virtual Private Networks (VPNs). The feature allows users to configure a backup tunnel to the next next hop, which allows protection against link and node failure. MPLS fast reroute ensures that MPLS traffic reaches its destination despite link or node fault in the network core. When a router in the label-switching path is aware of data link or node problems at the next-hop destination, the router (known as the point of local repair [PLR]) stacks additional labels onto MPLS packets to reroute the traffic around the routing fault.

If the problem is in the data link, the PLR provides line protection by redirecting the traffic to the original next-hop destination through a different path. If there is a fault at the next hop, the PLR provides node protection by bypassing that hop altogether and routing the traffic to the next hop in the original path. In either case, when the MPLS traffic returns to the node on the original path, the fast reroute label is discarded and the original MPLS label is restored.

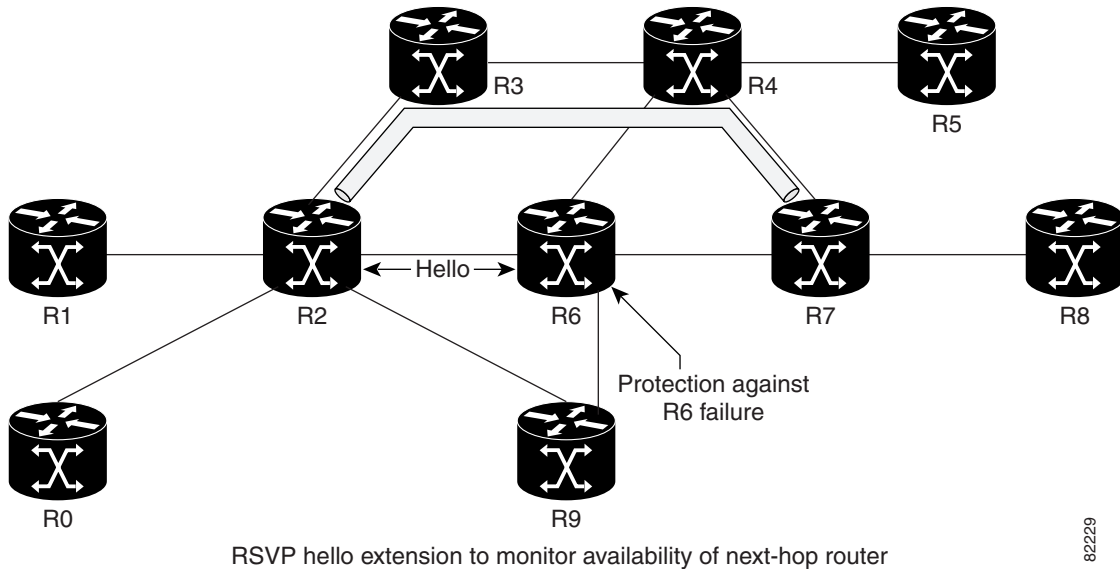
In addition to rerouting the traffic, the PLR router informs the head-end router of problems in the path, so that future traffic originating at the head-end router will use a different tunnel. The PLR also informs the headend router when an offending link or node is repaired, so the original MPLS tunnel can be assigned again to new traffic.

MPLS Fast Reroute for Node Protection Benefits

- Robust VPNs
- Decreased costs
- Increased end-user satisfaction
- Robust applications

MPLS Fast Reroute for Node Protection Application

Figure 9 shows how the MPLS fast reroute for node protection feature works.

FINAL DRAFT - CISCO CONFIDENTIAL**Figure 9 MPLS Fast Reroute for Node Protection**

The following is an example of MPLS fast reroute configuration:

Configuration Example 6: MPLS Fast Reroute

```

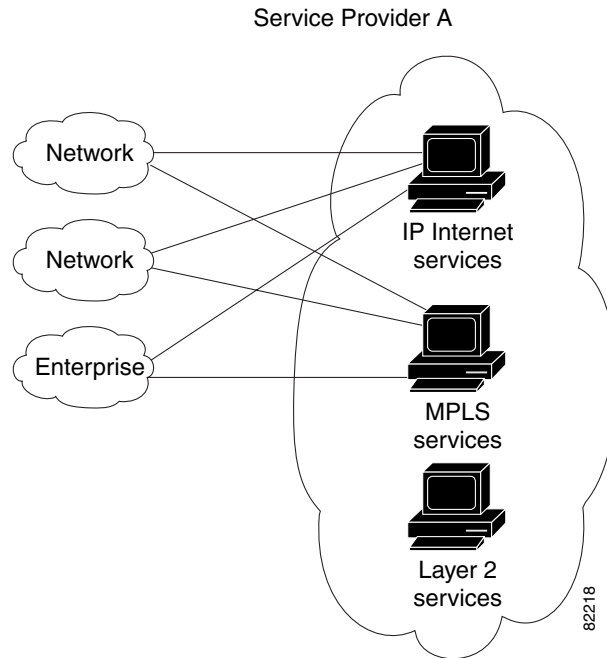
On R2
interface POS4/0
description Link to R4
ip address 10.1.13.2 255.255.255.252
no ip directed-broadcast
ip router isis
encapsulation ppp
mpls traffic-eng tunnels
mpls traffic-eng backup-path Tunnel10
mpls traffic-eng backup path Tunnel15
tag-switching ip
no peer neighbor-route
crc 32
clock source internal
pos ais-shut
pos report lrdi
ip rsvp bandwidth 155000 155000

```

Cisco Globally Resilient IP: Putting It All Together

This section provides examples of scenarios in which Cisco Globally Resilient IP features can be deployed. Users can select the Cisco Globally Resilient IP features that will work best in their network.

[Figure 10](#) provides an overall view of example SP and enterprise scenarios in which customers may use Globally Resilient IP features. In this illustration, Service Provider A has both an IP/Internet core and an MPLS core and provides service to various enterprise networks.

FINAL DRAFT - CISCO CONFIDENTIAL**Figure 10 Enterprise and Service Provider—Overall View**

Enterprise Scenario

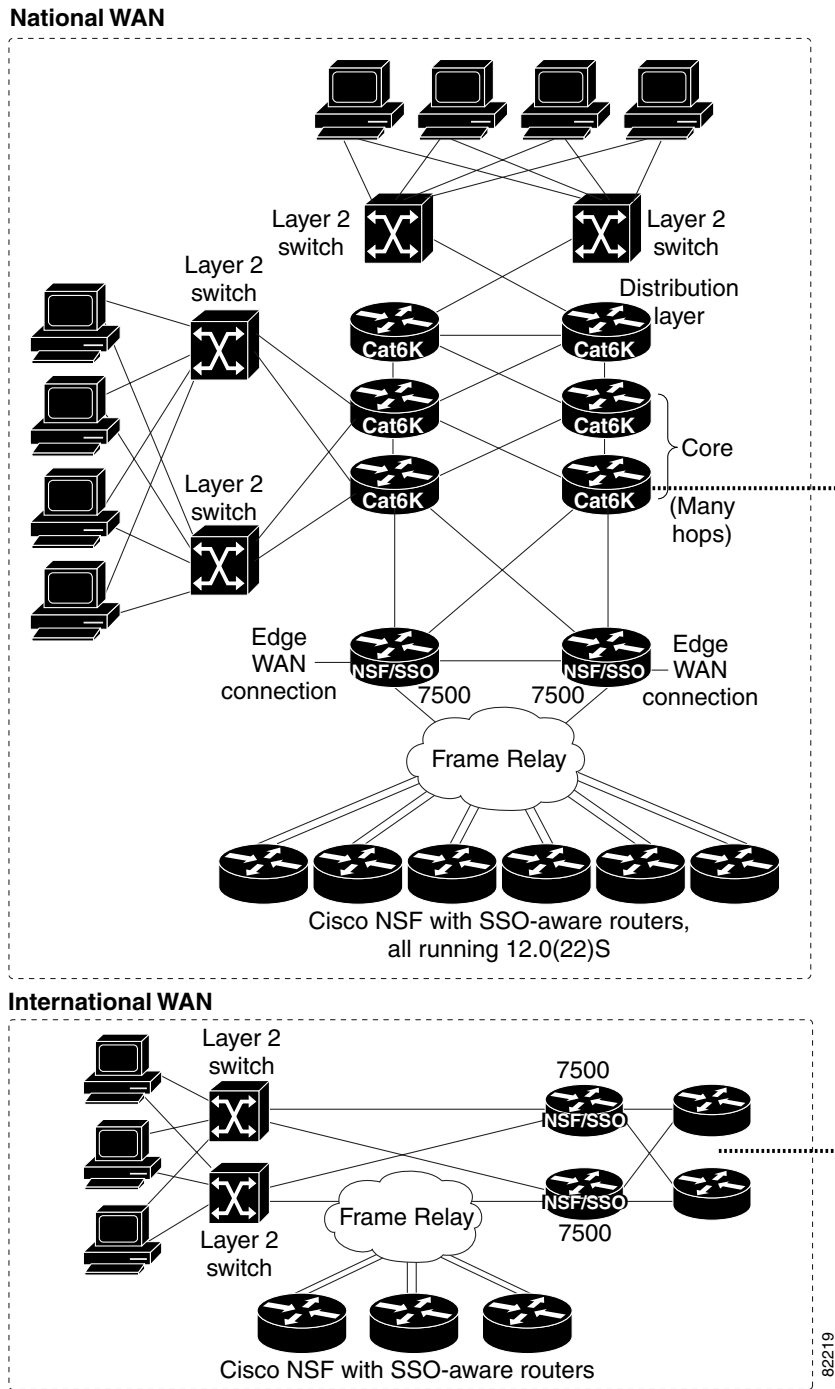
The enterprise deployment scenario describes customers that require the highest level of reliability and redundancy in the data network for applications such as real-time market data feeds. Even the shortest outage could cost millions of dollars. Their network must be designed for subsecond convergence and minimal latency. The applications they use typically have IP multicast requirements.

The lead customers in this market segment range from global finance companies and institutions such as NASDAQ and Merrill Lynch to global energy and commodity trading companies such as Shell.

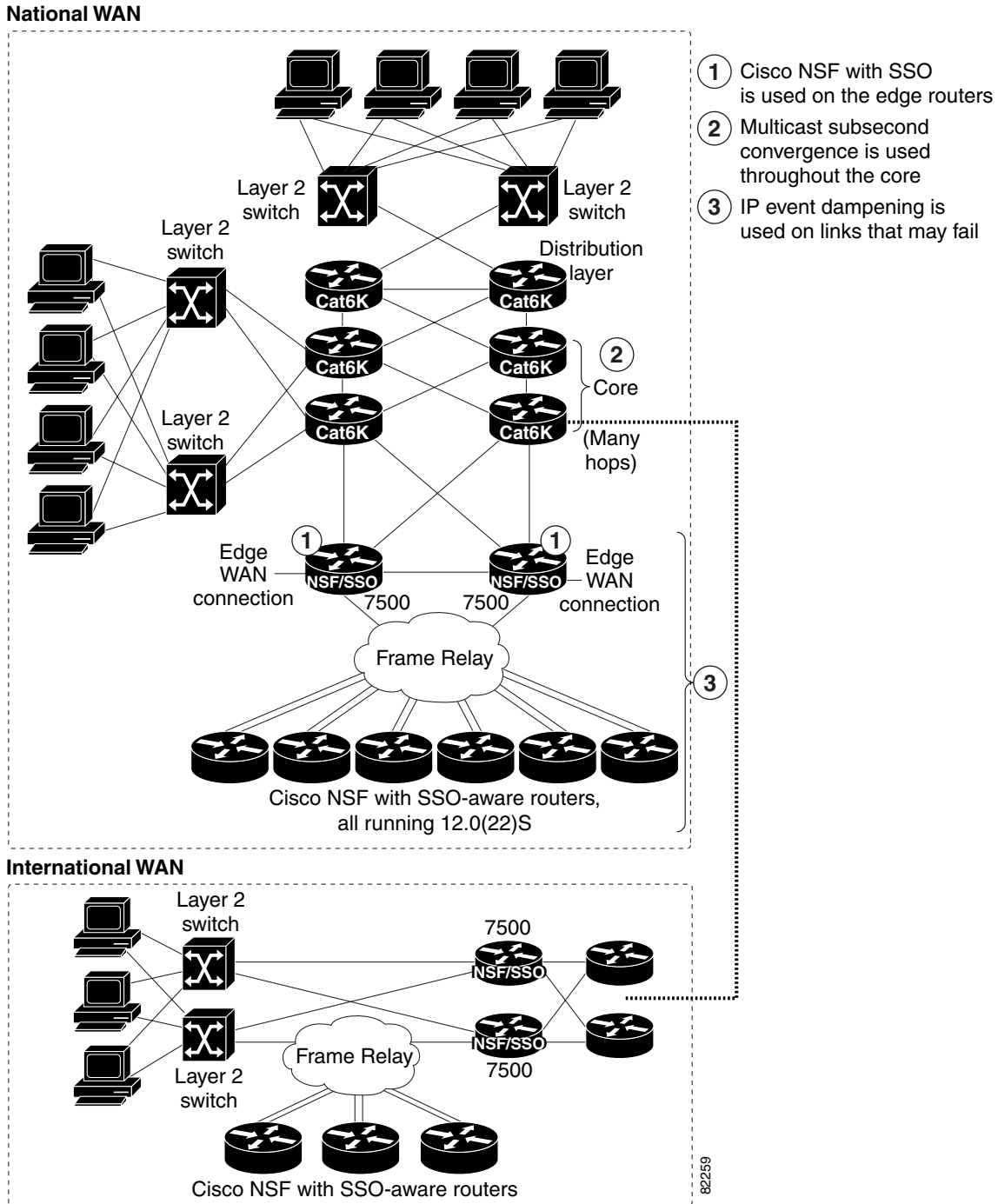
[Figure 11](#) shows an enterprise deployment scenario.

FINAL DRAFT - CISCO CONFIDENTIAL

Figure 11 Enterprise Scenario



The enterprise scenario shown in [Figure 11](#) uses the Globally Resilient IP features Cisco NSF with SSO, IP event dampening, and multicast subsecond convergence. [Figure 12](#) shows the enterprise scenario with these features, and the following subsections describe these features as they are used in this scenario.

FINAL DRAFT - CISCO CONFIDENTIAL**Figure 12 Enterprise Scenario with Globally Resilient IP Features****Cisco NSF with SSO**

Cisco NSF with SSO is configured on the edge routers that provide a Frame Relay WAN data traffic infrastructure between the enterprise core and Cisco NSF with SSO-aware routers. These edge routers, running on the Cisco IOS 7500 and Cisco 7200 platforms, are located both in the national and the

FINAL DRAFT - CISCO CONFIDENTIAL

international WANs. Cisco NSF with SSO-aware routers are located one layer away from the Cisco NSF with SSO-capable routers at the edge. In the release of the Globally Resilient IP features, the Cisco NSF with SSO-aware routers must all be running Cisco IOS Release 12.0(22)S software. Enabling Cisco NSF with SSO on edge routers is important for providing redundancy throughout the enterprise network.

IP Event Dampening

IP event dampening is provided on the edge routers running Cisco NSF with SSO, through the Frame Relay connection, and on the Cisco NSF with SSO-aware routers. This feature is provided throughout the WAN data traffic infrastructure because these links are more likely to fail than are the links within the core. All WAN links to the Cisco NSF with SSO aware routers are dual-connected for redundancy.

Multicast Subsecond Convergence

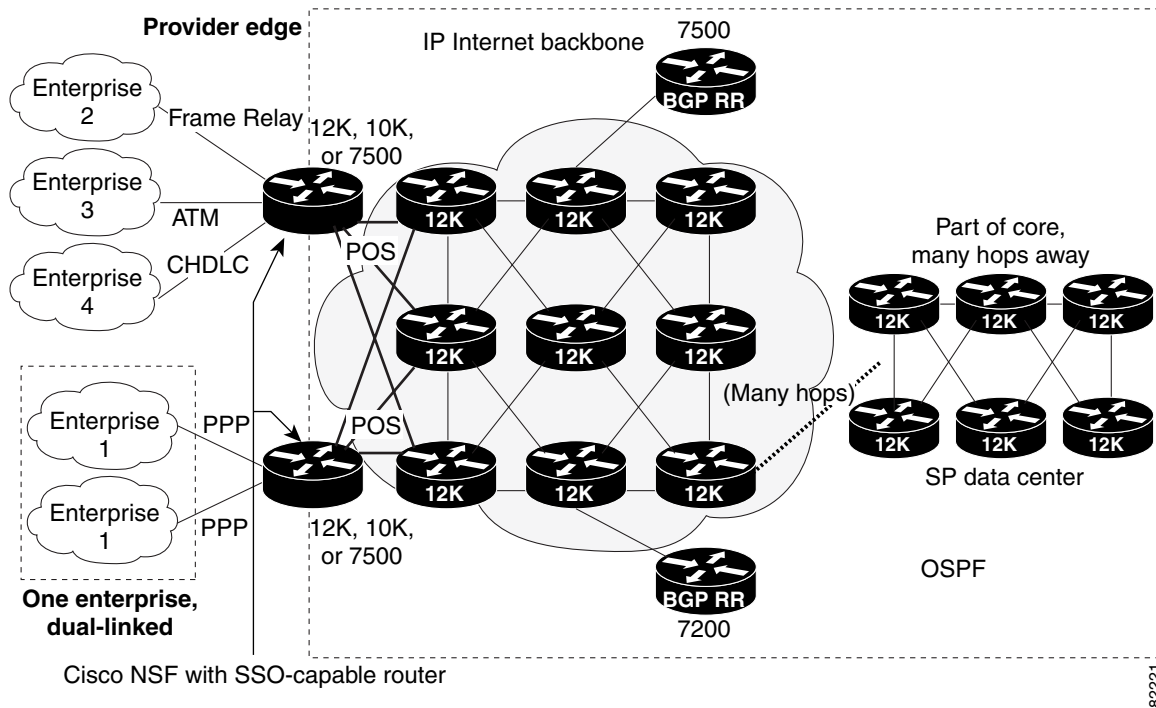
Multicast subsecond convergence is used throughout the entire core and distribution layer in order to disseminate information to all clients. For example, an enterprise network such as a large bank in which clients want to access the latest information on interest rates. Multicast subsecond convergence enabled on the enterprise core allows all clients to receive the latest information as soon as it is available.

Service Provider—IP Internet Scenario

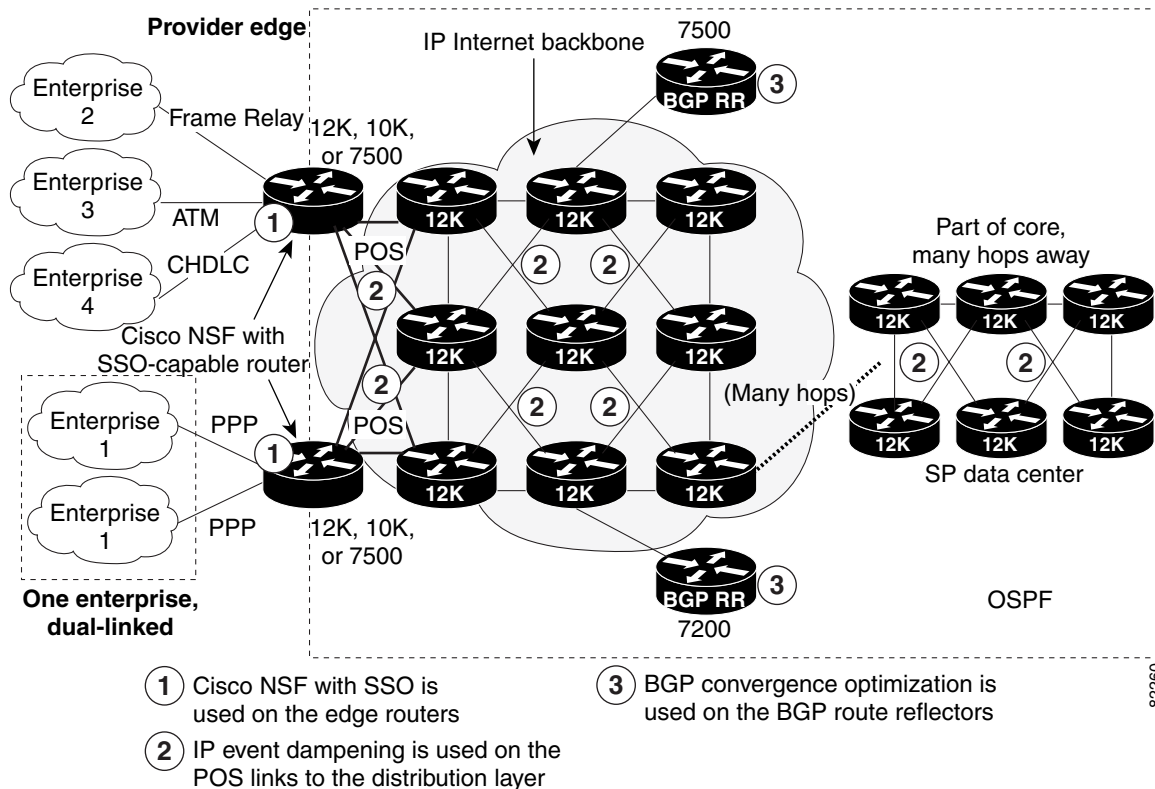
The SP IP Internet deployment scenario describes Tier 1 ISPs that offer a variety of services such as multiple Quality of Service (QoS) classes based on applications and customers and highly available and scalable VPN solutions. They have specific requirements for QoS and IP multicast.

Customers deploying these kinds of services include Sprint, France Telecom, AT&T, UUNet, and Telecom Italia.

[Figure 13](#) shows a possible SP IP Internet deployment scenario.

FINAL DRAFT - CISCO CONFIDENTIAL**Figure 13 SP IP Internet Scenario**

The SP IP Internet scenario shown in [Figure 13](#) uses the Globally Resilient IP features Cisco NSF with SSO, IP event dampening, and BGP convergence optimization. [Figure 14](#) shows the SP IP Internet scenario with these features, and the following subsections describe these features as they are used in this scenario.

FINAL DRAFT - CISCO CONFIDENTIAL**Figure 14 SP IP Internet Scenario with Globally Resilient IP Features**

Cisco NSF with SSO

Cisco NSF with SSO is configured on the edge routers that provide connections to various enterprise networks. These edge routers can be running the Cisco 7500, Cisco 10000, or Cisco 12000 platform. The connections are made using protocols including Frame Relay, ATM, HDLC, and PPP, and the enterprises all use Cisco NSF with SSO-aware routers. In the release of the Globally Resilient IP features, the Cisco NSF with SSO-aware routers must all be running Cisco IOS Release 12.0(22)S software. Enabling Cisco NSF with SSO on edge routers is important for providing redundancy throughout the SP IP Internet network.

IP Event Dampening

The IP event dampening feature is enabled on the links throughout the core and on the Packet over SONET (POS) links from the core to the distribution layer. This feature is provided throughout the WAN data traffic infrastructure.

BGP Convergence Optimization

BGP convergence optimization is enabled on the two BGP route reflector (RR) routers connected to the core using a single connection. One BGP RR is running on the Cisco 7500 platform and the other is running on the Cisco 7200 platform. Each of these two routers has many BGP peers in the autonomous system. The BGP convergence optimization feature allows BGP information to be provided to all of the peers of these routers in an efficient manner.

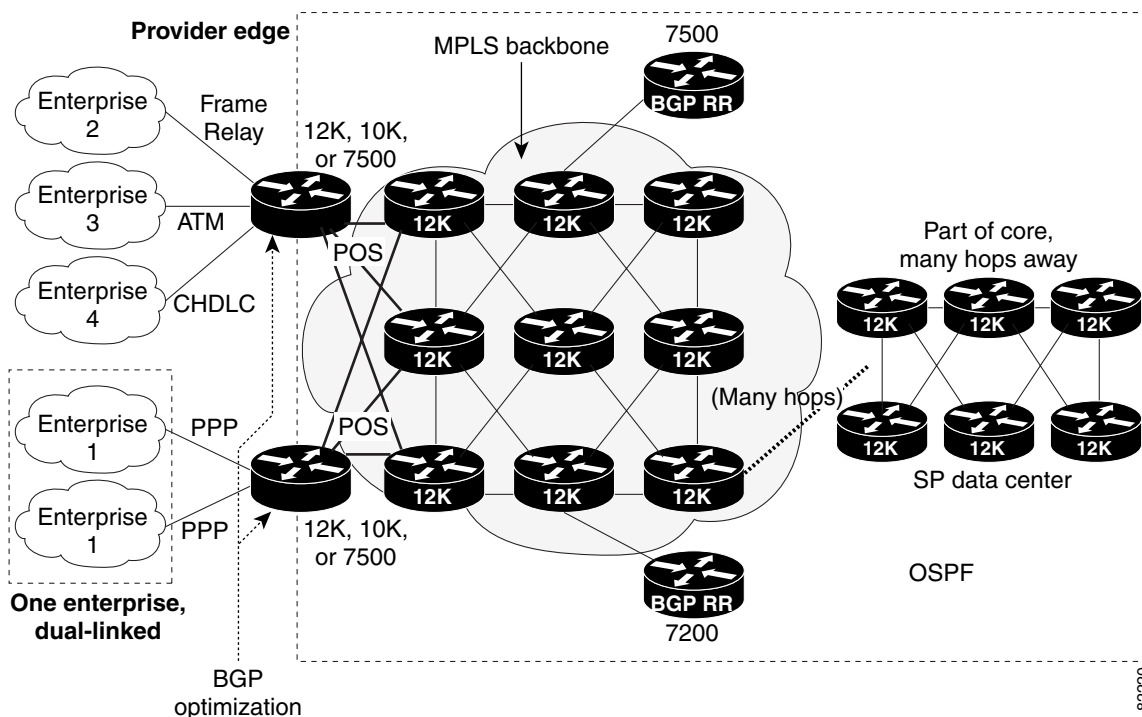
FINAL DRAFT - CISCO CONFIDENTIAL**Service Provider—MPLS Scenario**

The SP MPLS scenario describes Tier 1 ISPs offering advanced services that rely on MPLS technology. MPLS VPNs are the most widely deployed MPLS technology, and several customers use traffic engineering (TE) to optimize network utilization. Integration of QoS features with MPLS VPNs and MPLS TE allows for service offerings such as virtual leased line and toll bypass for voice. These customers have specific requirements for advanced MPLS features and QoS.

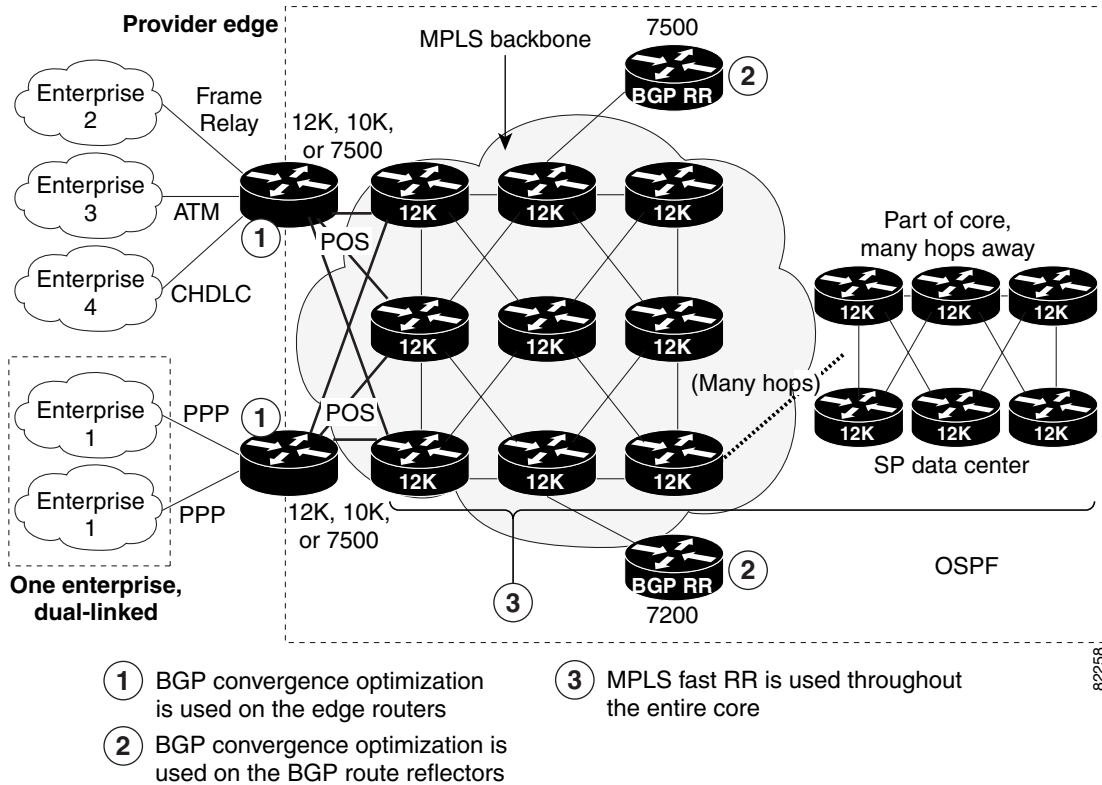
Customers that deploy the SP MPLS scenario include AT&T, Bell Canada, Deutsche Telecom, Global One, NTT, and SITA.

Figure 15 shows an SP MPLS deployment scenario.

Figure 15 SP MPLS Scenario



The SP MPLS scenario shown in Figure 15 uses BGP convergence optimization and MPLS fast reroute for node protection. Figure 16 shows the SP MPLS scenario with these features, and the following subsections describe these features as they are used in this scenario.

FINAL DRAFT - CISCO CONFIDENTIAL**Figure 16 SP MPLS Scenario with Globally Resilient IP Features**

BGP Convergence Optimization

In this scenario, BGP convergence optimization is provided on the edge routers, which may be running on the Cisco 7500, Cisco 10000, or Cisco 12000 platform. It is also used on the two BGP RR routers connected to the core, one running on the Cisco 7500 platform and the other running on the Cisco 7200 platform. Each of these two routers has many BGP peers in the autonomous system. The BGP convergence optimization feature allows BGP information to be provided to all of the peers of these routers in an efficient manner.

MPLS Fast Reroute for Node Protection

The MPLS fast reroute for node protection feature is implemented on every router in the SP MPLS core (except for the two BGP RR routers, which only perform route redistribution and are not in the MPLS forwarding path). This feature defines an alternate path in case of a single point of failure (SPOF). The feature sets up a tunnel that bypasses the SPOF and goes on to the next hop.

Related Documents

- *Cisco Nonstop Forwarding*, Cisco IOS Release 12.0(22)S feature module
- *Stateful Switchover*, Cisco IOS Release 12.0(22)S feature module
- *Multicast Subsecond Convergence*, Cisco IOS Release 12.0(22)S feature module

FINAL DRAFT - CISCO CONFIDENTIAL

- *Globally Resilient IP Data Sheet*, white paper
- *Cisco Globally Resilient IP Feature Overview*, white paper
- *Globally Resilient IP Executive Summary*, white paper

Terminology

Term	Definition
ATM	Asynchronous Transfer Mode
BGP	Border Gateway Protocol
CEF	Cisco Express Forwarding
ESR	edge services router (the Cisco 10000 series Internet router)
FR2	Frame Relay Fast Restart
FSU	Fast Software Upgrade
GLBP	Gateway Load Balancing Protocol
HA	high availability
IOS	Cisco Internetworking Operating System
IS-IS	Intermediate System-to-Intermediate System
MPLS	Multiprotocol Label Switching
MTBF	mean time between failures
MTTR	mean time to repair/reload
NAT	Network Address Translation
NSF	nonstop forwarding
Omega	Another name for 10000 ESR series routers
OSPF	Open Shortest Path First protocol
RP	Route Processor
RPM	Route Processor Module
RPR	Route Processor Redundancy
RPR+	Enhancement to RPR in which the standby RP is fully initialized
SLCR	Single Line Card Reload
SSO	stateful switchover