BGP Support for Nonstop Routing (NSR) with Stateful Switchover (SSO) Using L2VPN VPLS

The BGP Support for Nonstop Routing (NSR) with Stateful Switchover (SSO) feature enables using L2VPN VPLS provider edge (PE) routers to maintain Border Gateway Protocol (BGP) state with customer edge (CE) routers and ensure continuous packet forwarding during a Route Processor (RP) switchover or during a planned In-Service Software Upgrade (ISSU) for a PE router. CE routers do not need to be Nonstop Forwarding (NSF)-capable or NSF-aware to benefit from BGP NSR capabilities on PE routers. Only PE routers need to be upgraded to support BGP NSR--no CE router upgrades are required. BGP NSR with SSO, thus, enables service providers to provide the benefits NSF with the additional benefits of NSR without requiring CE routers to be upgraded to support BGP graceful restart.

Prerequisites for BGP Support for NSR with SSO

- Your network must be configured to run BGP.
- Multiprotocol Layer Switching (MPLS) Layer 3 VPNs must be configured.
- You must be familiar with NSF and SSO concepts and tasks.

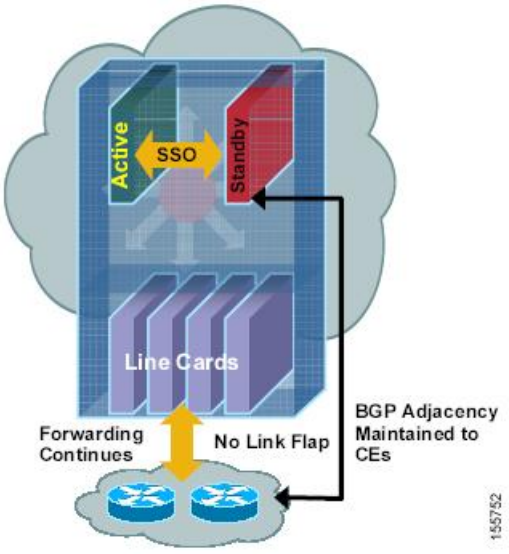
Information About BGP Support for Nonstop Routing (NSR) with Stateful Switchover (SSO)

Overview of BGP NSR with SSO

Prior to the introduction of BGP NSR with SSO in Cisco IOS Release 12.2(28)SB, BGP required that all neighboring devices participating in BGP NSF be configured to be either NSF-capable or NSF-aware (by configuring the devices to support the BGP graceful restart mechanism). BGP NSF, thus, required that all neighboring devices be upgraded to a version of Cisco IOS software that supports BGP graceful restart. However, in many MPLS VPN deployments, there are situations where PE routers engage in exterior BGP (eBGP) peering sessions with CE routers that do not support BGP graceful restart and cannot be upgraded to a software version that supports BGP graceful restart in the same time frame as the provider (P) routers.

BGP NSR with SSO provides a high availability (HA) solution to service providers whose PE routers engage in eBGP peering relationships with CE routers that do not support BGP graceful restart. BGP NSR works with SSO to synchronize BGP state information between the active and standby RP. SSO minimizes the amount of time a network is unavailable to its users following a switchover. When the BGP NSR with SSO feature is configured, in the event of an RP switchover, the PE router uses BGP NSR with SSO to maintain BGP state for eBGP peering sessions with CEs that are not NSF-aware (see the figure below). Additionally, the BGP NSR with SSO feature dynamically detects NSF-aware peers and runs graceful restart with those CE routers. For eBGP peering sessions with NSF-aware peers and for internal BGP (iBGP) sessions with BGP Route Reflectors (RRs) in the service provider core, the PE uses NSF to maintain BGP state. BGP NSR with SSO, thus, enables service providers to provide the benefits of NSF with the additional benefits of NSR without requiring CE routers to be upgraded to support BGP graceful restart.

Figure 1: BGP NSR with SSO Operations During an RP Switchover



BGP NSR with SSO is supported in BGP peer, BGP peer group, and BGP session template configurations. To configure support for BGP NSR with SSO in BGP peer and BGP peer group configurations, use the **neighbor ha-mode sso** command in address family configuration mode for IPv4 VRF address family BGP

peer sessions. To include support for Cisco BGP NSR with SSO in a peer session template, use the **ha-mode sso** command in session-template configuration mode.

Benefits of BGP NSR with SSO

- Minimizes services disruptions--Border Gateway Protocol (BGP) Nonstop Routing (NSR) with Stateful Switchover (SSO) reduces impact on customer traffic during route processor (RP) switchovers (scheduled or unscheduled events), extending high availability (HA) deployments and benefits at the edge.
- Enhances high-availability Nonstop Forwarding (NSF) and SSO deployment at the edge--BGP NSR with SSO allows incremental deployment by upgrading the provider edge device with the NSR capability so that customer-facing edge devices are synchronized automatically and no coordination or NSF awareness is needed with the customer side Cisco or third-party customer edge devices. The BGP NSR feature dynamically detects NSF-aware peers and runs graceful restart with those CE devices.
- Provides transparent route convergence--BGP NSR with SSO eliminates route flaps by keeping BGP state on both active and standby RPs and ensures continuous packet forwarding with minimal packet loss during RP failovers.

How to Configure BGP Support for Nonstop Routing (NSR) with Stateful Switchover (SSO)

Configuring a PE Device to Support BGP NSR with SSO

Perform this task to enable a provider edge (PE) device to maintain BGP state with customer edge (CE) devices and ensure continuous packet forwarding during a route processor (RP) switchover or during a planned ISSU. Border Gateway Protocol (BGP) Nonstop Routing (NSR) with Stateful Switchover (SSO) enables service providers to provide the benefits Nonstop Forwarding (NSF) with the additional benefits of NSR without requiring CE devices to be upgraded to support BGP graceful restart.

BGP NSR with SSO is supported in BGP peer, BGP peer group, and BGP session template configurations. Perform one of the following tasks in this section on a PE device, depending on whether you want to configure support for BGP NSR with SSO in a peer, a peer group, or a session template configuration:

Note The combination of BGP Nonstop Routing (NSR) and Stateful Switchover (SSO) is not supported. You cannot simultaneously configure the **bgp ha-mode sso** and **bgp additional-paths** [**send** | **receive**] under any address-family.

Prerequisites

- These tasks assume that you are familiar with BGP peer, BGP peer group, and BGP session template concepts. For more information, see the “Configuring a Basic BGP Network” module.
- The active and standby RP must be in SSO mode. For information about configuring SSO mode, see the “Configuring Stateful Switchover” module in the *High Availability Configuration Guide*.

- Graceful restart should be enabled on the PE device. We recommend that you enable graceful restart on all BGP peers in the provider core that participate in BGP NSF. For more information about configuring graceful restart, see the "Configuring Advanced BGP Features" module.
- CE devices must support the route refresh capability. For more information, see the "Configuring a Basic BGP Network" module.

Configuring a Peer to Support BGP NSR with SSO

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **bgp graceful-restart [restart-time** *seconds*] [**stalepath-time** *seconds*]
5. **address-family ipv4 vrf** *vrf-name*
6. **neighbor** *ip-address* **remote-as** *autonomous-system-number*
7. **neighbor** *ip-address* **ha-mode sso**
8. **neighbor** *ip-address* **activate**
9. **end**
10. **show ip bgp vpnv4 all sso summary**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**router bgp** *autonomous-system-number* **Example:** `Device(config)# router bgp 40000`	Enters router configuration mode for the specified routing process.
Step 4	**bgp graceful-restart [restart-time** *seconds*] [**stalepath-time** *seconds*] **Example:**	Enables the Border Gateway Protocol (BGP) graceful restart capability and BGP Nonstop Forwarding (NSF) awareness.

	Command or Action	Purpose
	`Device(config-router)# bgp graceful-restart`	• If you enter this command after the BGP session has been established, you must restart the session for the capability to be exchanged with the BGP neighbor. • Use this command on the restarting device and all of its peers (NSF-capable and NSF-aware).
Step 5	**address-family ipv4 vrf** *vrf-name* **Example:** `Device(config-router)# address-family ipv4 vrf test`	Enters address family configuration mode for IPv4 VRF address family sessions. • The **vrf**keyword and *vrf-name* argument specify that *IPv4 VRF instance information will be exchanged.* **Note** Only the syntax necessary for this task is displayed. For more details, see the *Cisco IOS IP Routing: BGP Command Reference*.
Step 6	**neighbor** *ip-address* **remote-as** *autonomous-system-number* **Example:** `Device(config-router-af)# neighbor 192.168.1.1 remote-as 45000`	Adds the IP address of the neighbor in the specified autonomous system to the IPv4 multiprotocol BGP neighbor table of the local router.
Step 7	**neighbor** *ip-address* **ha-mode sso** **Example:** `Device(config-router-af)# neighbor 192.168.1.1 ha-mode sso`	Configures the neighbor to support BGP Nonstop Routing (NSR) with Stateful Switchover (SSO).
Step 8	**neighbor** *ip-address* **activate** **Example:** `Device(config-router-af)# neighbor testgroup activate`	Enables the neighbor to exchange prefixes for the IPv4 address family with the local router. **Note** By default, neighbors that are defined using the **neighbor remote-as** command in router configuration mode exchange only unicast address prefixes.
Step 9	**end** **Example:** `Device(config-router-af)# end`	Exits address family configuration mode and enters privileged EXEC mode.
Step 10	**show ip bgp vpnv4 all sso summary** **Example:** `Device# show ip bgp vpnv4 all sso summary`	(Optional) Displays the number of BGP neighbors that are in SSO mode.

Configuring a Peer Group to Support BGP NSR with SSO

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **bgp graceful-restart [restart-time** *seconds*] [**stalepath-time** *seconds*]
5. **neighbor** *peer-group-name* **peer-group**
6. **neighbor** *ip-address* **remote-as** *autonomous-system-number*
7. **neighbor** *ip-address* **peer-group** *peer-group-name*
8. **neighbor** *peer-group-name* **ha-mode sso**
9. **address-family l2vpn vpls**
10. **neighbor** *peer-group-name* **activate**
11. **end**
12. **show ip bgp l2vpn vpls all sso summary**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**router bgp** *autonomous-system-number* **Example:** `Device(config)# router bgp 40000`	Enters router configuration mode for the specified routing process.
Step 4	**bgp graceful-restart [restart-time** *seconds*] [**stalepath-time** *seconds*] **Example:** `Device(config-router)# bgp graceful-restart`	Enables the Border Gateway Protocol (BGP) graceful restart capability and BGP Nonstop Forwarding (NSF) awareness. • If you enter this command after the BGP session has been established, you must restart the session for the capability to be exchanged with the BGP neighbor. • Use this command on the restarting device and all of its peers (NSF-capable and NSF-aware).

	Command or Action	Purpose
Step 5	**neighbor** *peer-group-name* **peer-group** **Example:** `Device(config-router-af)# neighbor testgroup peer-group`	Creates a BGP peer group.
Step 6	**neighbor** *ip-address* **remote-as** *autonomous-system-number* **Example:** `Device(config-router-af)# neighbor 192.168.1.1 remote-as 45000`	Adds the IP address of the neighbor in the specified autonomous system to the IPv4 multiprotocol BGP neighbor table of the local device.
Step 7	**neighbor** *ip-address* **peer-group** *peer-group-name* **Example:** `Device(config-router-af)# neighbor 192.168.1.1 peer-group testgroup`	Assigns the IP address of a BGP neighbor to a BGP peer group.
Step 8	**neighbor** *peer-group-name* **ha-mode sso** **Example:** `Device(config-router-af)# neighbor 192.168.1.1 ha-mode sso`	Configures the BGP peer group to support BGP Nonstop Routing (NSR) with Stateful Switchover (SSO).
Step 9	**address-family l2vpn vpls** **Example:** `Device(config-router)# address-family l2vpn vpls`	Specifies activation of L2VPN VPLS peering.
Step 10	**neighbor** *peer-group-name* **activate** **Example:** `Device(config-router-af)# neighbor testgroup activate`	Enables the neighbor to exchange prefixes for the IPv4 address family with the local device.
Step 11	**end** **Example:** `Device(config-router-af)# end`	Exits address family configuration mode and returns to global configuration mode.
Step 12	**show ip bgp l2vpn vpls all sso summary** **Example:** `Device# show ip bgp l2vpn vpls all sso summary`	(Optional) Displays the number of BGP neighbors that are in SSO mode.

Configuring Support for BGP NSR with SSO in a Peer Session Template

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **template peer-session** *session-template-name*
5. **ha-mode sso**
6. **exit-peer-session**
7. **end**
8. **show ip bgp template peer-session** [*session-template-name*]

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**router bgp** *autonomous-system-number* **Example:** `Device(config)# router bgp 101`	Enters router configuration mode and creates a Border Gateway Protocol (BGP) routing process.
Step 4	**template peer-session** *session-template-name* **Example:** `Device(config-router)# template peer-session CORE1`	Enters session-template configuration mode and creates a peer session template.
Step 5	**ha-mode sso** **Example:** `Device(config-router-stmp)# ha-mode sso`	Configures the neighbor to support BGP Nonstop Routing (NSR) with Stateful Switchover (SSO).
Step 6	**exit-peer-session** **Example:** `Device(config-router-stmp)# exit-peer-session`	Exits session-template configuration mode and returns to router configuration mode.

	Command or Action	Purpose
Step 7	**end** **Example:** `Device(config-router)# end`	Exits router configuration mode and returns to privileged EXEC mode.
Step 8	**show ip bgp template peer-session** [*session-template-name*] **Example:** `Device# show ip bgp template peer-session`	(Optional) Displays locally configured peer session templates. • The output can be filtered to display a single peer policy template with the *session-template-name* argument. This command also supports all standard output modifiers.

What to Do Next

After the peer session template is created, the configuration of the peer session template can be inherited by or applied to another peer session template with the **inherit peer-session** or **neighbor inherit peer-session** command.

For more information about configuring peer session templates, see the "Configuring a Basic BGP Network" chapter in the *Cisco IOS IP Routing: BGP Configuration Guide*.

Verifying BGP Support for NSR with SSO

SUMMARY STEPS

1. **enable**
2. **show ip bgpl2vpnvpls all sso summary**
3. **show ip bgpl2vpnvpls all neighbors**

DETAILED STEPS

Procedure

Step 1 **enable**

Enables privileged EXEC mode.

Example:

```
Device> enable
```

Step 2 **show ip bgpl2vpnvpls all sso summary**

This command is used to display the number of Border Gateway Protocol (BGP) neighbors that are in Stateful Switchover (SSO) mode.

The following is sample output from the **show ip bgp l2vpnvpls all sso summary** command:

Example:

```
Device# show ip bgp l2vpn vpls all sso summary
   Stateful switchover support enabled for 40 neighbors
```

Step 3 **show ip bgpl2vpnvpls all neighbors**

This command displays VPN address information from the BGP table.

The following is sample output from the **show ip bgp l2vpnvpls all neighbors** command. The "Stateful switchover support" field indicates whether SSO is enabled or disabled. The "SSO Last Disable Reason" field displays information about the last BGP session that lost SSO capability.

Example:

```
Device# show ip bgp l2vpn vpls all neighbors 10.3.3.3
BGP neighbor is 10.3.3.3,  vrf vrf1,  remote AS 3, external link
  Inherits from template 10vrf-session for session parameters
   BGP version 4, remote router ID 10.1.105.12
   BGP state = Established, up for 04:21:39
   Last read 00:00:05, last write 00:00:09, hold time is 30, keepalive interval is 10 seconds
   Configured hold time is 30, keepalive interval is 10 seconds
   Minimum holdtime from neighbor is 0 seconds
   Neighbor capabilities:
     Route refresh: advertised and received(new)
     Address family IPv4 Unicast: advertised and received
     Stateful switchover support enabled
   Message statistics:
     InQ depth is 0
     OutQ depth is 0
                         Sent       Rcvd
     Opens:                 1          1
     Notifications:         0          0
     Updates:               1          4
     Keepalives:         1534       1532
     Route Refresh:         0          0
     Total:              1536       1537
   Default minimum time between advertisement runs is 30 seconds
  For address family: L2VPN VPLS
   BGP table version 25161, neighbor version 25161/0
   Output queue size : 0
   Index 7, Offset 0, Mask 0x80
   7 update-group member
   Inherits from template 10vrf-policy
   Overrides the neighbor AS with my AS before sending updates
   Outbound path policy configured
   Route map for outgoing advertisements is Deny-CE-prefixes
                               Sent       Rcvd
   Prefix activity:            ----       ----
     Prefixes Current:           10         50 (Consumes 3400 bytes)
     Prefixes Total:             10         50
     Implicit Withdraw:           0          0
     Explicit Withdraw:           0          0
     Used as bestpath:          n/a          0
     Used as multipath:         n/a          0
                                 Outbound    Inbound
   Local Policy Denied Prefixes:    --------    -------
     route-map:                          150          0
     AS_PATH loop:                       n/a        760
     Total:                              150        760
   Number of NLRIs in the update sent: max 10, min 10
   Address tracking is enabled, the RIB does have a route to 10.3.3.3
   Address tracking requires at least a /24 route to the peer
```

```
   Connections established 1; dropped 0
   Last reset never
   Transport(tcp) path-mtu-discovery is enabled
   TCP session must be opened passively
Connection state is ESTAB, I/O status: 1, unread input bytes: 0 Connection is ECN Disabled Local
host: 10.0.21.1, Local port: 179 Foreign host: 10.0.21.3, Foreign port: 51205 Connection tableid
(VRF): 1
Enqueued packets for retransmit: 0, input: 0  mis-ordered: 0 (0 bytes)
Event Timers (current time is 0x1625488):
Timer          Starts    Wakeups            Next
Retrans          1746        210             0x0
TimeWait            0          0             0x0
AckHold          1535       1525             0x0
SendWnd             0          0             0x0
KeepAlive           0          0             0x0
GiveUp              0          0             0x0
PmtuAger            0          0             0x0
DeadWait            0          0             0x0
Linger              0          0             0x0
iss: 2241977291  snduna: 2242006573  sndnxt: 2242006573     sndwnd:  13097
irs:  821359845  rcvnxt:  821391670  rcvwnd:      14883  delrcvwnd:   1501
SRTT: 300 ms, RTTO: 303 ms, RTV: 3 ms, KRTT: 0 ms
minRTT: 0 ms, maxRTT: 300 ms, ACK hold: 200 ms Status Flags: passive open, retransmission timeout,
gen tcbs
   0x1000
Option Flags: VRF id set, always push, md5
Datagrams (max data segment is 4330 bytes):
Rcvd: 3165 (out of order: 0), with data: 1535, total data bytes: 31824
Sent: 3162 (retransmit: 210 fastretransmit: 0),with data: 1537, total data
bytes: 29300
SSO Last Disable Reason: Application Disable (Active)
```

Troubleshooting Tips

To troubleshoot BGP NSR with SSO, use the following commands in privileged EXEC mode, as needed:

- **debug ip bgp sso** --Displays BGP-related SSO events or debugging information for BGP-related interactions between the active RP and the standby RP. This command is useful for monitoring or troubleshooting BGP sessions on a PE router during an RP switchover or during a planned ISSU.
- **debug ip tcp ha** --Displays TCP HA events or debugging information for TCP stack interactions between the active RP and the standby RP. This is command is useful for troubleshooting SSO-aware TCP connections.
- **show tcp** --Displays the status of TCP connections. The display output will display the SSO capability flag and will indicate the reason that the SSO property failed on a TCP connection.
- **show tcp ha connections** --Displays connection-ID-to-TCP mapping data.

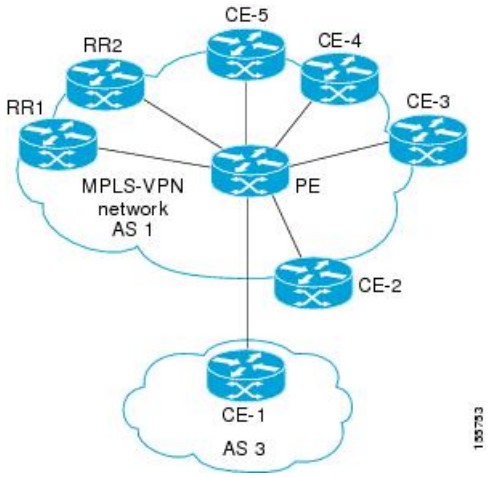
Configuration Examples for BGP Support for Nonstop Routing (NSR) with Stateful Switchover (SSO) using L2VPN VPLS

Example: Configuring BGP NSR with SSO Using L2VPN VPLS

The illustration below illustrates a sample Border Gateway Protocol (BGP) Nonstop Routing (NSR) with Stateful Switchful (SSO) network topology using L2VPN VPLS technology, and the configuration examples that follow show configurations from two devices in the topology: the RR1 device and the provider edge (PE) device.

Note The configuration examples omit some of the configuration required for Multiprotocol Label Switching (MPLS) VPNs because the purpose of these examples is to illustrate the configuration of BGP NSR with SSO.

Figure 2: BGP NSR with SSO Example Topology



RR1 Configuration

The following example shows the BGP configuration for RR1 in the illustration above. RR1 is configured as a Nonstop Forwarding (NSF)-aware route reflector (RR). In the event of an route processor (RP) switchover, the PE device uses NSF to maintain the BGP state of the internal peering session with RR1.

```
!
router bgp 1
 no synchronization
 bgp log-neighbor-changes
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
 neighbor 10.2.2.2 remote-as 1
 neighbor 10.2.2.2 update-source Loopback0
 no auto-summary
 !
```

```
 address-family l2vpn vpls
 neighbor 10.2.2.2 activate
 neighbor 10.2.2.2 send-community both
 neighbor 10.2.2.2 route-reflector-client
 exit-address-family
 !
```

PE Configuration

The following example shows the BGP NSR with SSO configuration for the PE device in the illustration above. The PE device is configured to support both NSF-awareness and the BGP NSR with SSO capability. In the event of an RP switchover, the PE device uses BGP NSR with SSO to maintain BGP state for the external BGP (eBGP) peering session and uses NSF to maintain BGP state for the internal BGP (iBGP) session with RR1.

```
!
router bgp 2
 no synchronization
 bgp log-neighbor-changes
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
 neighbor 10.1.1.1 remote-as 1
 neighbor 10.1.1.1 update-source Loopback0
 neighbor 10.3.3.3 remote-as 3
 neighbor 10.3.3.3 ha-mode sso
 neighbor 10.3.3.3 activate
 neighbor 10.3.3.3 as-override
 no auto-summary
 !
 address-family l2vpn vpls
 neighbor 10.1.1.1 activate
 neighbor 10.1.1.1 send-community both
 exit-address-family
 !
 no auto-summary
 no synchronization
 exit-address-family
!
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
BGP commands	Cisco IOS BGP Command Reference
MTR commands	Cisco IOS Multitopology Routing Command Reference

Related Topic	Document Title
Configuring Multitopology Routing	Multitopology Routing Configuration Guide
BGP NSR Support for iBGP Peers	BGP Configuration Guide
BGP NSR Support for MPLS VPNv4 and VPNv6 Inter-AS Option B	BGP Configuration Guide
BGP-IPV6 NSR	BGP Configuration Guide

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for BGP Support for Nonstop Routing (NSR) with Stateful Switchover (SSO) Using L2VPN VPLS

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1: Feature Information for BGP Support for Nonstop Routing (NSR) with Stateful Switchover (SSO)

Feature Name	Releases	Feature Information
BGP Support for Nonstop Routing (NSR) with Stateful Switchover (SSO) Using L2VPN VPLS	Cisco IOS XE Fuji 16.7.1	The BGP Support for Nonstop Routing (NSR) with Stateful Switchover (SSO) using L2VPN VPLS feature enables provider edge (PE) routers to maintain Border Gateway Protocol (BGP) state with customer edge (CE) routers and ensure continuous packet forwarding during a Route Processor (RP) switchover or during a planned In-Service Software Upgrade (ISSU) for a PE router. CE routers do not need to be Nonstop Forwarding (NSF)-capable or NSF-aware to benefit from BGP NSR capabilities on PE routers. Only PE routers need to be upgraded to support BGP NSR--no CE router upgrades are required. BGP NSR with SSO, thus, enables service providers to provide the benefits NSF with the additional benefits of NSR without requiring CE routers to be upgraded to support BGP graceful restart. The following commands were modified: • **debug ip bgp sso** • **show ip bgp l2vpn**