MPLS Traffic Engineering: Shared Risk Link Groups

First Published: May 6, 2004
Last Updated: May 31, 2007

Shared Risk Link Groups (SRLGs) refer to situations where links in a network share a common fiber (or a common physical attribute). If one link fails, other links in the group may fail too. Links in the group have a shared risk.

The MPLS Traffic Engineering: Shared Risk Link Groups feature enhances backup tunnel path selection so that a backup tunnel avoids using links that are in the same SRLG as interfaces the backup tunnel is protecting.

History for the MPLS Traffic Engineering: Shared Risk Link Groups Feature

Release	Modification
12.0(28)S	This feature was introduced.
12.0(29)S	Support for Open Shortest Path First (OSPF) was added.
12.2(33)SRA	This feature was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This feature was integrated into Cisco IOS Release 12.2(33)SXH.

Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

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

Contents

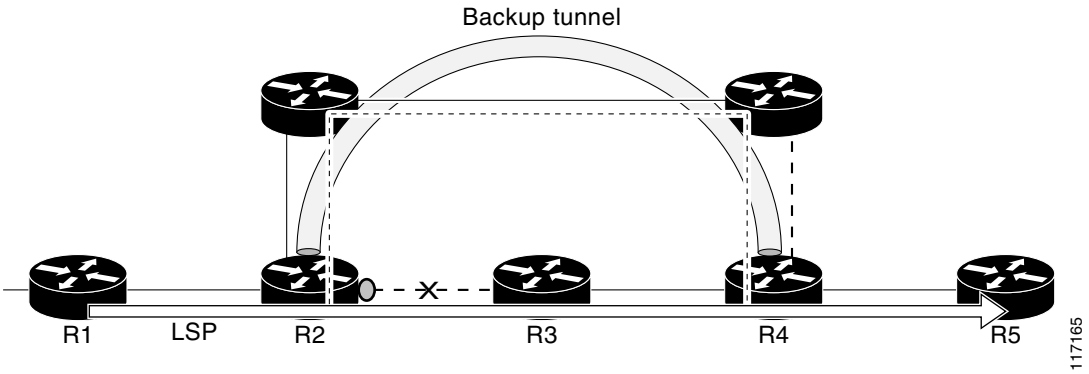
Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

MPLS Traffic Engineering: Shared Risk Link Groups

Backup tunnels should avoid using links in the same SRLG as interfaces they are protecting. Otherwise, when the protected link fails the backup tunnel fails too.

Figure 1 shows a primary label-switched path (LSP) from router R1 to router R5. The LSP protects against the failure of the R2-R3 link at R2 via a backup tunnel to R4. If the R2-R3 link fails, link protection reroutes the LSP along the backup tunnel. However, the R2-R3 link and one of the backup tunnel links are in the same SRLG. So if the R2-R3 link fails, the backup tunnel may fail too.

Figure 1 Backup Tunnel in the Same SRLG as the Interface It Is Protecting



The MPLS TE SRLG feature enhances backup tunnel path selection so a backup tunnel can avoid using links that are in the same SRLG as the interfaces it is protecting.

There are two ways for a backup tunnel to avoid the SRLGs of its protected interface:

- The router does not create the backup tunnel unless it avoids SRLGs of the protected interface.
- The router *tries* to avoid SRLGs of the protected interface, but if that is not possible the router creates the backup tunnel anyway. In this case there are two explicit paths. The first explicit path *tries* to avoid the SRLGs of the protected interface. If that does not work, the backup tunnel uses the second path (which ignores SRLGs).

Note Only backup tunnels that routers create automatically (called autotunnel backup) can avoid SRLGs of protected interfaces. For more information about these backup tunnels, see the "Autotunnel Backup" section on page 5.

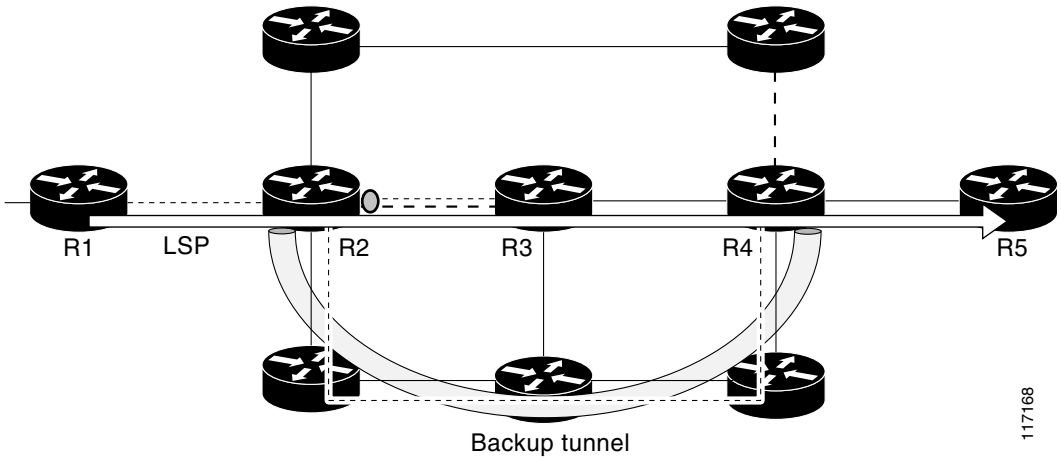
To activate the MPLS TE SRLG feature, you must do the following:

- Configure the SRLG membership of each link that has a shared risk with another link.
- Configure the routers to automatically create backup tunnels that avoid SRLGs of the protected interfaces.

For a detailed explanation of the configuration steps, see the "How to Configure MPLS Traffic Engineering: Shared Risk Link Groups" section on page 7.

OSPF and Intermediate System-to-Intermediate System (IS-IS) flood the SRLG membership information (including other TE link attributes such as bandwidth availability and affinity) so that all routers in the network have the SRLG information for each link. With this topology information, routers can compute backup tunnel paths that exclude links having SRLGs in common with their protected interfaces. As shown in Figure 2, the backup tunnel avoids the link between R2 and R3, which shares an SRLG with the protected interface.

Figure 2 Backup Tunnel that Avoids SRLG of Protected Interface



Prerequisites for MPLS Traffic Engineering: Shared Risk Link Groups

- You must configure Fast Reroutable tunnels.
- You must ensure to enable the Autotunnel backup.

Restrictions for MPLS Traffic Engineering: Shared Risk Link Groups

- The backup tunnel must be within a single area.
- Manually created backup tunnels do not automatically avoid SRLGs of protected interfaces.
- You cannot specify that a *primary* tunnel avoid links belonging to specified SRLGs.

Information About MPLS Traffic Engineering: Shared Risk Link Groups

To configure MPLS traffic engineering SRLGs, you need to understand the following concepts:

MPLS Traffic Engineering

MPLS is an Internet Engineering Task Force (IETF)-specified framework that provides for the efficient designation, routing, forwarding, and switching of traffic flows through the network.

Traffic engineering (TE) is the process of adjusting bandwidth allocations to ensure that enough is left for high-priority traffic.

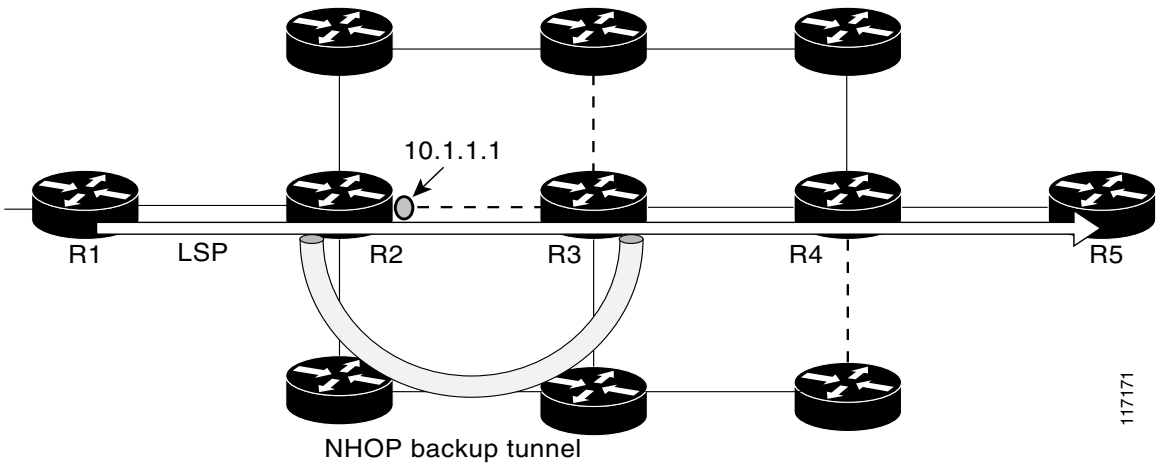
In MPLS TE, the upstream router creates a network tunnel for a particular traffic stream, then fixes the bandwidth available for that tunnel.

Fast Reroute

Fast Reroute (FRR) protects MPLS TE LSPs from link and node failures by locally repairing the LSPs at the point of failure. This protection allows data to continue to flow on LSPs while their headend routers attempt to establish new end-to-end LSPs to replace them. FRR locally repairs the protected LSPs by rerouting them over backup tunnels that bypass failed links or nodes.

Backup tunnels that bypass only a single link of the LSP's path provide link protection. They protect LSPs if a link along their path fails by rerouting the LSP's traffic to the next hop (bypassing the failed link). These are referred to as next-hop (NHOP) backup tunnels because they terminate at the LSP's next hop beyond the point of failure. Figure 3 illustrates an NHOP backup tunnel.

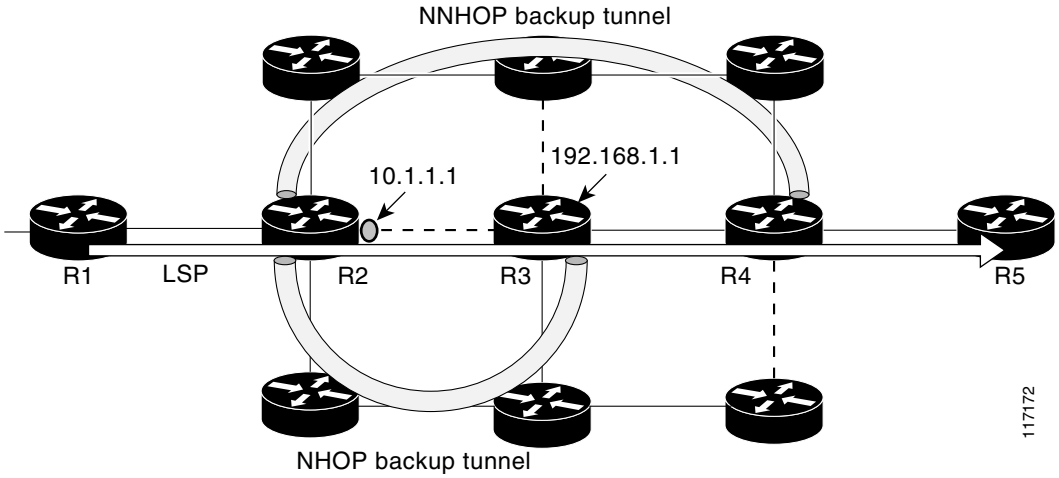
Figure 3 NHOP Backup Tunnel



FRR provides node protection for LSPs. Backup tunnels that bypass next-hop nodes along LSP paths are called next-next-hop (NNHOP) backup tunnels because they terminate at the node following the next-hop node of the LSP paths, thereby bypassing the next-hop node. They protect LSPs if a node along their path fails by enabling the node upstream of the failure to reroute the LSPs and their traffic around the failed node to the next-next hop. FRR supports the use of RSVP Hellos to accelerate the detection of node failures. NNHOP backup tunnels also provide protection from link failures, because they bypass the failed link and the node.

Figure 4 illustrates an NNHOP backup tunnel.

Figure 4 NNHOP Backup Tunnel



Autotunnel Backup

Autotunnel backup is the ability of routers to create backup tunnels automatically. Therefore, you do not need to preconfigure each backup tunnel and then assign the backup tunnel to the protected interface. In this release of SRLGs, only automatically created backup tunnels can avoid SRLGs or their protected interfaces.

For information about backup tunnels, see the "Fast Reroute" section on page 4.

For detailed information about autotunnel backup and how you can change the default command values, see *MPLS Traffic Engineering AutoTunnel Primary and Backup*, Release 12.0(27)S.

To globally activate the autotunnel backup feature, enter the **mpls traffic-eng auto-tunnel backup** command.

Figure 5 illustrates an NNHOP automatically generated backup tunnel that excludes the router 192.168.1.1 and terminates at router R4. The backup tunnel must avoid touching any links of 192.168.1.1.

Figure 5 Autotunnel Backup for NNHOP

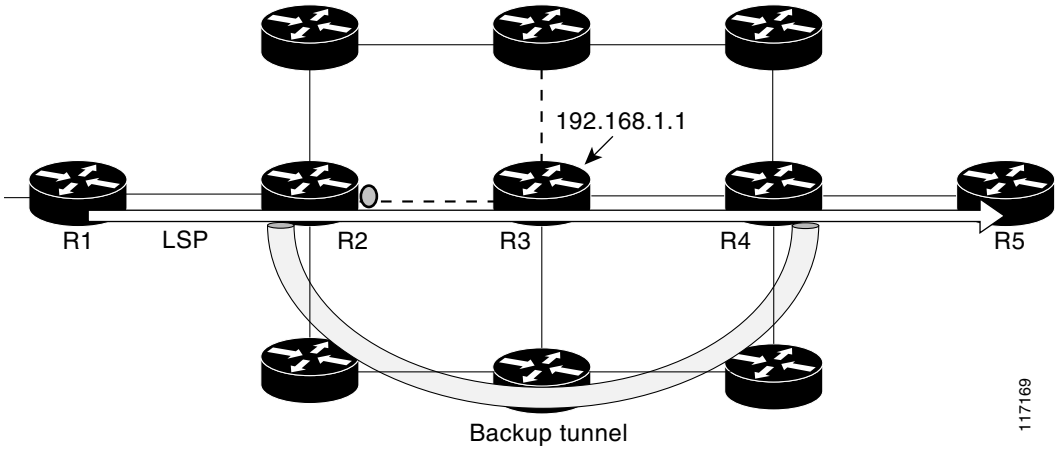
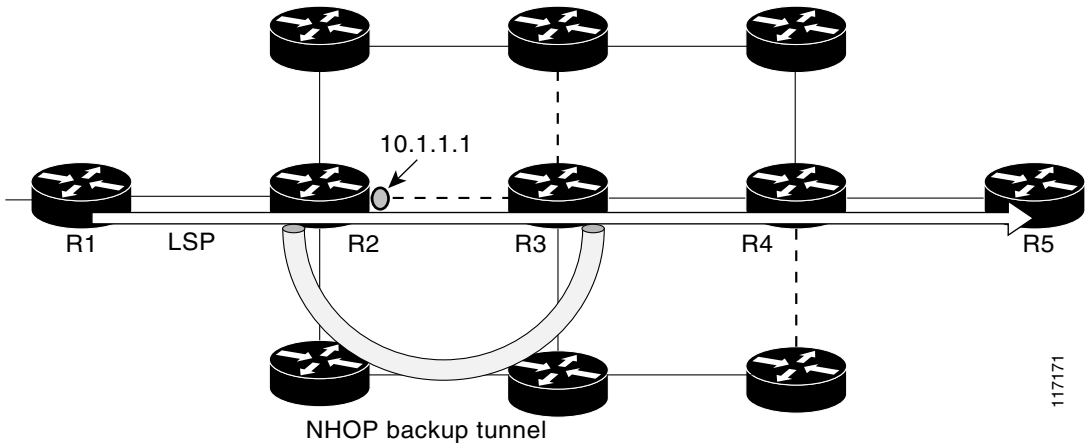


Figure 6 illustrates an NHOP automatically generated backup tunnel that terminates at router R3 and avoids the link 10.1.1.1, not the entire node.

Figure 6 Autotunnel Backup for NHOP



Note NNHOP excludes the router ID (the entire router must be excluded; that is, no link of the router can be included in the backup tunnel's path). NHOP excludes only the link when the backup tunnel's path is computed.

How to Configure MPLS Traffic Engineering: Shared Risk Link Groups

This section contains the following procedures:

- Configuring the SRLG Membership of Each Link That Has a Shared Risk with Another Link, page 7 (required)
- Configuring the Routers That Automatically Create Backup Tunnels to Avoid SRLGs of Their Protected Interfaces (required)

Configuring the SRLG Membership of Each Link That Has a Shared Risk with Another Link

Enter the commands on the physical interface.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *interface slot/port*
4. **mpls traffic-eng srlg** [*num*]
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *interface slot/port* **Example:** `Router(config)# interface pos 1/1`	Specifies an interface and enters interface configuration mode.

	Command or Action	Purpose
Step 4	**mpls traffic-eng srlg** [*num*] **Example:** `Router(config-if)# mpls traffic-eng srlg 5`	Configures the SRLG membership of a link (interface). **Note** To make the link a member of multiple SRLGs, enter the **mpls traffic-eng srlg** command multiple times.
Step 5	**exit** **Example:** `Router(config-if)# exit`	Returns to global configuration mode.

Configuring the Routers That Automatically Create Backup Tunnels to Avoid SRLGs of Their Protected Interfaces

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mpls traffic-eng auto-tunnel backup srlg exclude** [**force** | **preferred**]
4. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**mpls traffic-eng auto-tunnel backup srlg exclude** [**force** | **preferred**] **Example:** `Router(config)# mpls traffic-eng auto-tunnel backup srlg exclude force`	Specifies that auto-created backup tunnels should avoid SRLGs of its protected interface(s). If you specify the **force** keyword, SRLGs are *forced* to avoid the SRLGs. If you specify the **preferred** keyword, SRLGs *try* to avoid the SRLGs, but the backup tunnel can be created if SRLGs cannot be avoided.
Step 4	**exit** **Example:** `Router(config)# exit`	Returns to privileged EXEC mode.

Verifying the MPLS Traffic Engineering: Shared Risk Link Groups Configuration

To verify the MPLS traffic engineering SRLG configuration, perform the following steps.

SUMMARY STEPS

1. **show running-config**
2. **show mpls traffic-eng link-management interfaces** *interface slot/port*
3. **show mpls traffic-eng topology**
4. **show mpls traffic-eng topology srlg**
5. **show mpls traffic-eng topology brief**
6. **show mpls traffic-eng link-management advertisements**
7. **show ip rsvp fast-reroute**
8. **mpls traffic-eng auto-tunnel backup srlg exclude force**
9. **show ip explicit-paths**
10. **show mpls traffic-eng tunnels tunnel** *num*
11. **mpls traffic-eng auto-tunnel backup srlg exclude preferred**
12. **show ip explicit-paths**
13. **show ip rsvp fast-reroute**

DETAILED STEPS

Step 1 Use the following commands to configure the SRLG membership of interface pos3/1:

```
Router> enable
Router# configure terminal
Router(config)# interface pos 3/1
Router(config-if)# mpls traffic-eng srlg 1
Router(config-if)# mpls traffic-eng srlg 2
Router# show running-config

interface POS 3/1
 ip address 10.0.0.33 255.255.255.255
 no ip directed-broadcast
 ip router isis
 encapsulation ppp
 no ip mroute-cache
 mpls traffic-eng tunnels
 mpls traffic-eng backup-path Tunnel5000
 mpls traffic-eng srlg 1
 mpls traffic-eng srlg 2
 tag-switching ip
 crc 32
 clock source internal
 pos ais-shut
 pos report rdool
 pos report lais
 pos report lrdi
 pos report pais
 pos report prdi
```

```
 pos report sd-ber
 isis circuit-type level-2-only
 ip rsvp bandwidth 20000 20000 sub-pool 5000
```

Step 2 **show mpls traffic-eng link-management interfaces pos 3/1**

Use this command to show the SRLG membership configured on interface pos 3/1:

```
Router# show mpls traffic-eng link-management interfaces pos 3/1

System Information::
    Links Count:         11
Link ID:: PO3/1 (10.0.0.33)
    Link Status:
      SRLGs:               1 2
      Physical Bandwidth:  2488000 kbits/sec
      Max Res Global BW:   20000 kbits/sec (reserved:0% in, 0% out)
      Max Res Sub BW:      5000 kbits/sec (reserved:0% in, 0% out)
      MPLS TE Link State:  MPLS TE on, RSVP on, admin-up, flooded
      Inbound Admission:   allow-all
      Outbound Admission:  allow-if-room
      Admin. Weight:       10 (IGP)
      IGP Neighbor Count:  1
      IGP Neighbor:        ID 0000.0000.0004.00, IP 10.0.0.34 (Up)
    Flooding Status for each configured area [1]:
      IGP Area[1]: isis  level-2: flooded
```

Step 3 **show mpls traffic-eng topology**

Use this command to show the SRLG link membership flooded via the IGP:

```
Router# show mpls traffic-eng topology

My_System_id:0000.0000.0003.00 (isis  level-2)

Signalling error holddown:10 sec Global Link Generation 9

IGP Id:0000.0000.0003.00, MPLS TE Id:10.0.3.1 Router Node  (isis
level-2)
      link[0]:Point-to-Point, Nbr IGP Id:0000.0000.0004.00,
nbr_node_id:2, gen:9
          frag_id 0, Intf Address:10.0.0.33, Nbr Intf Address:10.0.0.34
          TE metric:10, IGP metric:10, attribute_flags:0x0
          SRLGs:1 2
          physical_bw:2488000 (kbps), max_reservable_bw_global:20000
(kbps)
          max_reservable_bw_sub:5000 (kbps)

                               Global Pool       Sub Pool
               Total Allocated Reservable        Reservable
               BW (kbps)       BW (kbps)         BW (kbps)
               ---------------  -----------       ----------
        bw[0]:           0            20000             5000
        bw[1]:           0            20000             5000
        bw[2]:           0            20000             5000
        bw[3]:           0            20000             5000
        bw[4]:           0            20000             5000
        bw[5]:           0            20000             5000
```

Step 4 **show mpls traffic-eng topology srlg**

Use this command to display all the links in the network that are members of a given SRLG:

```
Router# show mpls traffic-eng topology srlg
```

```
MPLS TE Id:0000.0000.0003.00 (isis  level-2)
  SRLG:1
     10.0.0.33
  SRLG:2
     10.0.0.33
```

The following command shows that there are two links in SRLG 1:

```
Router# show mpls traffic-eng topology srlg

MPLS TE Id:0000.0000.0003.00 (isis  level-2)
  SRLG:1
     10.0.0.33
     10.0.0.49
```

Step 5 show mpls traffic-eng topology brief

Use this command to display brief topology information:

```
Router# show mpls traffic-eng topology brief

My_System_id:0000.0000.0003.00 (isis  level-2)

Signalling error holddown:10 sec Global Link Generation 9

IGP Id:0000.0000.0003.00, MPLS TE Id:10.0.3.1 Router Node  (isis
level-2)
      link[0]:Point-to-Point, Nbr IGP Id:0000.0000.0004.00,
nbr_node_id:2, gen:9
          frag_id 0, Intf Address:10.0.0.33, Nbr Intf Address:10.0.0.34
          TE metric:10, IGP metric:10, attribute_flags:0x0
          SRLGs:1 2
```

Step 6 show mpls traffic-eng link-management advertisements

Use this command to show local link information that MPLS TE link management is currently flooding into the global TE topology:

```
Router# show mpls traffic-eng link-management advertisements

Flooding Status:      ready
Configured Areas:     1
IGP Area[1] ID::  isis  level-2
  System Information::
    Flooding Protocol:    ISIS
  Header Information::
    IGP System ID:        0000.0000.0003.00
    MPLS TE Router ID:    10.0.3.1
    Flooded Links:        2
  Link ID::  0
    Link Subnet Type:     Point-to-Point
    Link IP Address:      10.0.0.49
    IGP Neighbor:         ID 0000.0000.0007.00, IP 10.0.0.50
    TE metric:            80000
    IGP metric:           80000
    SRLGs:                None
    Physical Bandwidth:   622000 kbits/sec
    Res. Global BW:       20000 kbits/sec
    Res. Sub BW:          5000 kbits/sec
    Downstream::
                                Global Pool   Sub Pool
                                -----------   --------------
      Reservable Bandwidth[0]:  20000         5000 kbits/sec
      Reservable Bandwidth[1]:  20000         5000 kbits/sec
      Reservable Bandwidth[2]:  20000         5000 kbits/sec
```

```
    Reservable Bandwidth[3]:  20000         5000 kbits/sec
    Reservable Bandwidth[4]:  20000         5000 kbits/sec
    Reservable Bandwidth[5]:  20000         5000 kbits/sec
    Reservable Bandwidth[6]:  20000         5000 kbits/sec
    Reservable Bandwidth[7]:  20000         5000 kbits/sec
  Attribute Flags:      0x00000000
Link ID::  1
  Link Subnet Type:     Point-to-Point
  Link IP Address:      10.0.0.33
  IGP Neighbor:         ID 0000.0000.0004.00, IP 10.0.0.34
  TE metric:            10
  IGP metric:           10
  SRLGs:                1
  Physical Bandwidth:   2488000 kbits/sec
  Res. Global BW:       20000 kbits/sec
  Res. Sub BW:          5000 kbits/sec
  Downstream::
                            Global Pool   Sub Pool
                            -----------   --------------
    Reservable Bandwidth[0]:  20000         5000 kbits/sec
    Reservable Bandwidth[1]:  20000         5000 kbits/sec
    Reservable Bandwidth[2]:  20000         5000 kbits/sec
    Reservable Bandwidth[3]:  20000         5000 kbits/sec
    Reservable Bandwidth[4]:  20000         5000 kbits/sec
    Reservable Bandwidth[5]:  20000         5000 kbits/sec
    Reservable Bandwidth[6]:  20000         5000 kbits/sec
    Reservable Bandwidth[7]:  20000         5000 kbits/sec
  Attribute Flags:      0x00000000
```

Step 7 **show ip rsvp fast-reroute**

Use this command to show that the primary tunnel is going over Pos3/1 on R3, on which SLRG 1 is configured:

```
Router# show ip rsvp fast-reroute

Primary    Protect      BW      Backup
Tunnel     I/F        BPS:Type  Tunnel:Label  State   Level   Type
-------    -------    --------  ------------  -----   -----   ----
R3-PRP_t0  PO3/1 0:G  None      None          None    None    None
```

Step 8 **mpls traffic-eng auto-tunnel backup**

mpls traffic-eng auto-tunnel backup srlg exclude force

Use the following commands to configure autotunnel backup with **srlg force**:

```
Router(config)# mpls traffic-eng auto-tunnel backup
Router(config)# mpls traffic-eng auto-tunnel backup srlg exclude force
```

Step 9 **show ip explicit-paths**

Use the following command to verify that **srlg force** is configured with the **srlg exclude** pos3/1 link in the IP explicit path:

```
Router# show ip explicit-paths

PATH __dynamic_tunnel65436 (loose source route, path complete,
generation 24, status non-configured)
    1:exclude-address 10.0.0.33
    2:exclude-srlg    10.0.0.33
```

Step 10 **show mpls traffic-eng tunnels tunnel** *num*

Use the following command to show that autotunnel backup is configured but is down because the headend router does not have any other path to signal and it cannot use pos2/1 because it belongs in the same SRLG; that is, SRLG 1.

```
Router# show mpls traffic-eng tunnels tunnel 65436

Name:R3-PRP_t65436                        (Tunnel65436) Destination:
10.0.4.1
  Status:
    Admin:up         Oper:down   Path:not valid   Signalling:Down
    path option 1, type explicit __dynamic_tunnel65436

  Config Parameters:
    Bandwidth:0        kbps (Global)  Priority:7  7   Affinity:
0x0/0xFFFF
    Metric Type:TE (default)
    AutoRoute: disabled  LockDown:disabled  Loadshare:0
bw-based
    auto-bw:disabled

  Shortest Unconstrained Path Info:
    Path Weight:10 (TE)
    Explicit Route:10.0.0.34 10.0.4.1
  History:
    Tunnel:
      Time since created:5 minutes, 29 seconds
    Path Option 1:
      Last Error:PCALC::No path to destination, 0000.0000.0004.00
```

Step 11 **mpls traffic-eng auto-tunnel backup**

mpls traffic-eng auto-tunnel backup srlg exclude preferred

The following commands configure autotunnel backup with **srlg exclude preferred**:

```
Router(config)# mpls traffic-eng auto-tunnel backup
Router(config)# mpls traffic-eng auto-tunnel backup srlg exclude preferred
```

Step 12 **show ip explicit-paths**

The following command shows **srlg exclude preferred** with two explicit paths. The first path avoids the SRLGs of the protected interface. The second path does not avoid the SRLGs:

```
Router# show ip explicit-paths

PATH __dynamic_tunnel65436 (loose source route, path complete,
generation 30, status non-configured)
    1:exclude-address 10.0.0.33
    2:exclude-srlg    10.0.0.33
PATH __dynamic_tunnel65436_pathopt2 (loose source route, path complete,
generation 33, status non-configured)
    1:exclude-address 10.0.0.33
```

Step 13 **show ip rsvp fast-reroute**

The following command shows that the primary tunnel is protected with autotunnel backup using the second path option (see Step 10) that does not avoid the SRLGs.

```
Router# show ip rsvp fast-reroute

Primary    Protect      BW      Backup
Tunnel     I/F        BPS:Type  Tunnel:Label  State   Level   Type
-------    -------    --------  ------------  -----   -----   ----
R3-PRP_t0  PO3/1 0:G  0:G       Tu65436:0     Ready   any-unl nhop
```

```
Router# show mpls traffic-eng tunnels tunnel 65436

Name:R3-PRP_t65436                        (Tunnel65436) Destination:
10.0.4.1
  Status:
    Admin:up         Oper:up     Path:valid       Signalling:connected

    path option 2, type explicit __dynamic_tunnel65436_pathopt2 (Basis
for Setup, path weight 80020)
    path option 1, type explicit __dynamic_tunnel65436
  Config Parameters:
    Bandwidth:0        kbps (Global)  Priority:7  7   Affinity:
0x0/0xFFFF
    Metric Type:TE (default)
    AutoRoute: disabled  LockDown:disabled  Loadshare:0
bw-based
    auto-bw:disabled
  Active Path Option Parameters:
    State:explicit path option 2 is active
    BandwidthOverride:disabled  LockDown:disabled  Verbatim:disabled

InLabel  : -
  OutLabel :POS2/1, 23
  RSVP Signalling Info:
       Src 10.0.3.1, Dst 10.0.4.1, Tun_Id 65436, Tun_Instance 3
    RSVP Path Info:
      My Address:10.0.3.1
      Explicit Route:10.0.0.50 10.0.0.66 10.0.0.113 10.0.4.1
      Record   Route:  NONE
      Tspec:ave rate=0 kbits, burst=1000 bytes, peak rate=0 kbits
    RSVP Resv Info:
      Record   Route:  NONE
      Fspec:ave rate=0 kbits, burst=1000 bytes, peak rate=0 kbits
  Shortest Unconstrained Path Info:
    Path Weight:10 (TE)
    Explicit Route:10.0.0.34 10.0.4.1
```

Configuration Examples for MPLS Traffic Engineering: Shared Risk Link Groups

This section provides the following configuration examples:

- Configuring the SRLG Membership of Each Link That Has a Shared Risk with Another Link: Example, page 14
- Configuring the Routers that Automatically Create Backup Tunnels to Avoid SRLGs of Their Protected Interfaces: Example, page 16

Configuring the SRLG Membership of Each Link That Has a Shared Risk with Another Link: Example

The following example shows how to specify that the SRLG membership of each link has a shared risk with another link.

As shown in Figure 7 and in the following commands:

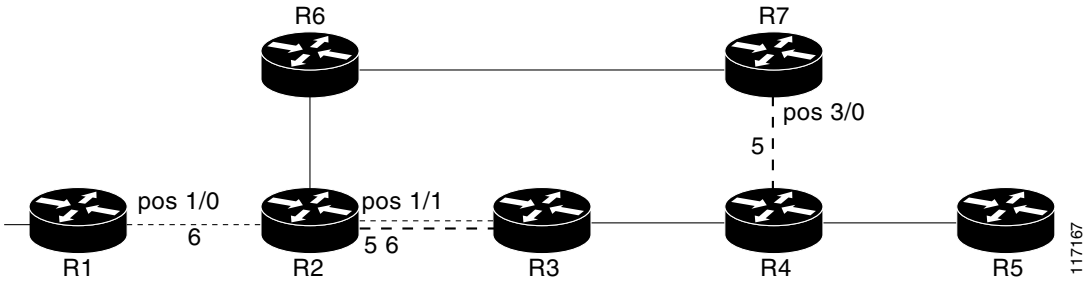
- link R2-R3 = SRLG5
- link R2-R3 = SRLG6
- link R7-R4 = SRLG5
- link R1-R2 = SRLG6

```
Router1# configure terminal
Router1# interface pos 1/0
Router1(config-if)# mpls traffic-eng srlg 6

Router2# configure terminal
Router2# interface pos 1/1
Router2(config-if)# mpls traffic-eng srlg 5
Router2(config-if)# mpls traffic-eng srlg 6

Router7# configure terminal
Router7# interface pos 3/0
Router7(config-if)# mpls traffic-eng srlg 5
```

Figure 7 SRLG Membership



Configuring the Routers that Automatically Create Backup Tunnels to Avoid SRLGs of Their Protected Interfaces: Example

The following example shows how to specify that automatically created backup tunnels are forced to avoid SRLGs of their protected interface(s):

```
Router# configure terminal
Router(config)# mpls traffic-eng auto-tunnel backup
Router(config)# mpls traffic-eng auto-tunnel backup srlg exclude force
```

Figure 8 illustrates the automatically created NNHOP backup tunnel that would be created to avoid SRLGs of the protected interface if the following conditions exist:

The exclude-address is 192.168.1.1.

The link at R2 has an IP address of 10.1.1.1.

The backup tunnel's explicit path avoids links that have a membership in the same SRLG as the link whose IP address is 10.1.1.1.

Figure 8 srlg exclude force—NNHOP Autobackup Tunnel

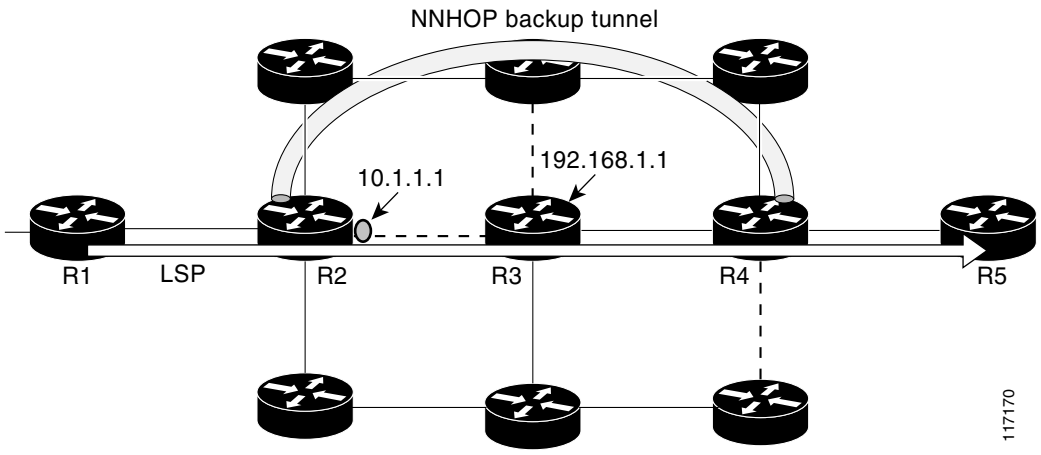
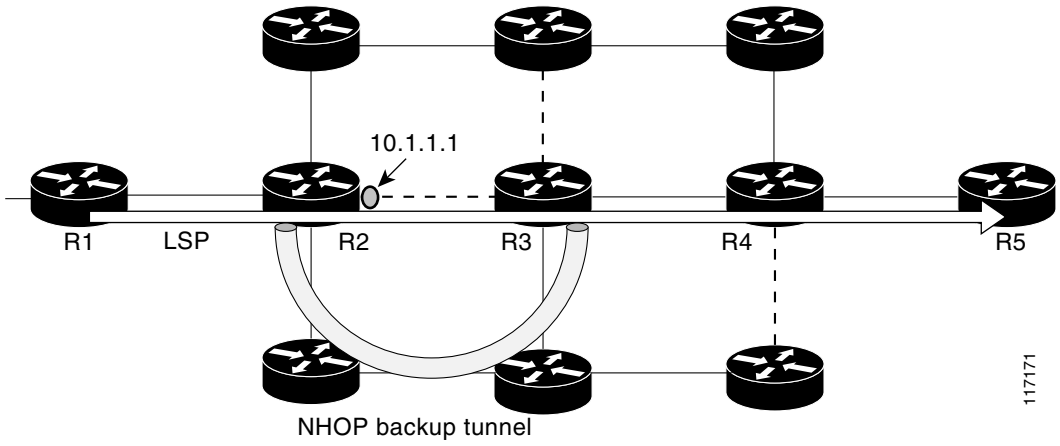


Figure 9 illustrates the automatically created NHOP backup tunnel that would be created.

Figure 9 srlg exclude force—NHOP Autobackup Tunnel



Additional References

The following sections provide references related to the MPLS Traffic Engineering: Shared Risk Link Groups feature.

Related Documents

Related Topic	Document Title
MPLS traffic engineering	• *Cisco IOS IP Switching Command Reference*, Release 12.4T • *Cisco IOS IP Switching Command Reference*, Release 12.2SR • *Cisco IOS IP Switching Command Reference*, Release 12.2SB • *Cisco IOS IP Switching Configuration Guide*, Release 12.4
Fast Reroute	• *MPLS Traffic Engineering—Fast ReRoute Link Protection*, Release 12.0(26)S
IS-IS	• *Cisco IOS IP Routing Protocols Command Reference*, Release 12.4T • *Cisco IOS IP Routing Protocols Command Reference*, Release 12.2SR • *Cisco IOS IP Routing Protocols Command Reference*, Release 12.2SB • *Cisco IOS IP Routing Protocols Configuration Guide*, Release 12.4
OSPF	• *Cisco IOS IP Routing Protocols Command Reference*, Release 12.4T • *Cisco IOS IP Routing Protocols Command Reference*, Release 12.2SR • *Cisco IOS IP Routing Protocols Command Reference*, Release 12.2SB • *Cisco IOS IP Routing Protocols Configuration Guide*, Release 12.4
Autotunnel backups	• *MPLS Traffic Engineering AutoTunnel Primary and Backup*, Release 12.0(27)S

Standards

Standard	Title
None	—

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
draft-ietf-isis-gmpls-extensions-16.txt	*IS-IS Extensions in Support of Generalized MPLS*

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register on Cisco.com.	http://www.cisco.com/techsupport

Command Reference

This feature uses no new or modified commands.

Glossary

Fast Reroute—A mechanism for protecting MPLS traffic engineering (TE) LSPs from link and node failure by locally repairing the LSPs at the point of failure. This protection allows data to continue to flow on them while their headend routers attempt to establish end-to-end LSPs to replace them. FRR locally repairs the protected LSPs by rerouting them over backup tunnels that bypass failed links or nodes.

hop—Passage of a data packet between two network nodes (for example, between two routers).

IGP—Interior Gateway Protocol. An Internet protocol used to exchange routing information within an autonomous system.

interface—A network connection.

IP address—A 32-bit address assigned to hosts using TCP/IP. An IP address belongs to one of five classes (A, B, C, D, or E) and is written as four octets separated by periods (dotted decimal format). Each address consists of a network number, an optional subnetwork number, and a host number. The network and subnetwork numbers together are used for routing, and the host number is used to address an individual host within the network or subnetwork. A subnet mask is used to extract network and subnetwork information from the IP address.

IP explicit path—A list of IP addresses, each representing a node or link in the explicit path.

IS-IS—Intermediate System-to-Intermediate System. OSI link-state hierarchal routing protocol based on DECnet Phase V routing, where intermediate system (IS) routers exchange routing information based on a single metric to determine the network topology.

LDP—Label Distribution Protocol. A standard protocol between MPLS-enabled routers to negotiate the labels (addresses) used to forward packets.

link—A point-to-point connection between adjacent nodes.

LSP—label-switched path. A path that is followed by a labeled packet over several hops, starting at an ingress LSR and ending at an egress LSR.

LSR—label switching router. A Layer 3 router that forwards a packet based on the value of a label encapsulated in the packet.

MPLS—Multiprotocol Label Switching. A method for forwarding packets (frames) through a network. It enables routers at the edge of a network to apply labels to packets. ATM switches or existing routers in the network core can switch packets according to the labels with minimal lookup overhead.

node—An endpoint of a network connection or a junction common to two or more lines in a network. Nodes can be interconnected by links, and serve as control points in the network.

OSPF—Open Shortest Path First. A link-state hierarchical Interior Gateway Protocol (IGP) routing algorithm, derived from the IS-IS protocol. OSPF features include least-cost routing, multipath routing, and load balancing.

router—A network-layer device that uses one or more metrics to determine the optimal path along which network traffic should be forwarded. Routers forward packets from one network to another based on network layer information.

router ID—Something by which a router originating a packet can be uniquely distinguished from all other routers; for example, an IP address from one of the router's interfaces.

traffic engineering—The techniques and processes used to cause routed traffic to travel through the network on a path other than the one that would have been chosen if standard routing methods had been used.

tunnel—A secure communication path between two peers, such as two routers. A traffic engineering tunnel is a label-switched tunnel that is used for traffic engineering. Such a tunnel is set up through means other than normal Layer 3 routing; it is used to direct traffic over a path different from the one that Layer 3 routing could cause the tunnel to take.

Note See *Internetworking Terms and Acronyms* for terms not included in this glossary.