

MINT 709 Capstone Project Report

Protection and Restoration in MPLS based Networks

SARTAJ SINGH
sartaj@ualberta.ca

Supervisor
Juned Noonari

Submitted To
Mike MacGregor
Professor
Department of Computing Science
University of Alberta

April 18, 2015

ABSTRACT

Multi-Protocol Label Switching (MPLS) is growing in popularity as a set of protocols for provisioning and managing core networks.[6]

Multi-protocol label switching integrates label-swapping framework with network layer routing that allows flexibility in the delivery of new routing services, since it allows new services to be added without changing the basic forwarding mechanism ,this enables more sophisticated features such as traffic engineering to be implemented. Although the current routing algorithms are very robust and survivable, the amount of time they take to recover from a failure is significant, causing serious disruption of network services. This is unacceptable to many organizations that aim to provide a highly reliable service, and thus require recovery times on the order of tens of milliseconds.[10]

Since MPLS binds packets to a route (or path) via the labels, and is likely to be the technology of choice in the future IP-based network, it is important that MPLS be able to provide protection and restoration of traffic.[10]

The Internet has transformed into a multiservice medium converging voice, video, and data communications.

In ISP network there is need to deploy service differentiation ,so that ISPs can provide various classes of service for different customers. In order to provide such capabilities in the network, the basic traffic forwarding mechanism used in Internet must be enhanced to support traffic engineering. [4]

Some services such as VoIP and media streaming do not tolerate data loss or/and delays[19], but due to the dynamic nature of networks ,network failure is common therefore the traffic on the MPLS network needs to be protected against network failure.[19]

CONTENTS

List Of Network Diagrams	II
Abbreviations.....	III
1. Introduction.....	01
2. Multiprotocol Label Switching.....	02
3. Virtual Private Networks.....	04
4. Signaling Protocols In MPLS.....	07
5. LDP(Label Distribution Protocol).....	09
6. MP-BGP (Multiprotocol Border Gateway Protocol)	12
7. RSVP-TE (Resource Reservation Protocol-Traffic Engineering)	13
8. MPLS Traffic Engineering	16
9. Traffic Protection In MPLS Networks.....	23
a. Path Protection.....	24
b. Local Protection	28
i. Link Protection	30
1. Link Facility Protection.....	30
2. Link 1:1 Protection	44
ii. Node Protection	51
1. Node Facility Protection	51
2. Node 1:1 Protection.....	55
10. Loop Free Alternate Fast Re-Route	61
11. CE-PE Protection	73
12. Recent Work in MPLS Traffic Engineering.....	75
Conclusion.....	78
Future Work	79
References	80
Appendix	

List Of Network Diagrams

NETWORK DIAGRAM 01.....	05
NETWORK DIAGRAM 02.....	05
NETWORK DIAGRAM 03.....	06
NETWORK DIAGRAM 04.....	08
NETWORK DIAGRAM 05.....	11
NETWORK DIAGRAM 06.....	12
NETWORK DIAGRAM 07.....	14
NETWORK DIAGRAM 08.....	14
NETWORK DIAGRAM 09.....	16
NETWORK DIAGRAM 10.....	17
NETWORK DIAGRAM 11.....	18
NETWORK DIAGRAM 12.....	21
NETWORK DIAGRAM 13.....	24
NETWORK DIAGRAM 14.....	29
NETWORK DIAGRAM 15.....	30
NETWORK DIAGRAM 16.....	31
NETWORK DIAGRAM 17.....	37
NETWORK DIAGRAM 18.....	44
NETWORK DIAGRAM 19.....	44
NETWORK DIAGRAM 20.....	45
NETWORK DIAGRAM 21.....	51
NETWORK DIAGRAM 22.....	52
NETWORK DIAGRAM 23.....	56
NETWORK DIAGRAM 24.....	56
NETWORK DIAGRAM 25.....	57
NETWORK DIAGRAM 26.....	61
NETWORK DIAGRAM 27.....	62
NETWORK DIAGRAM 28.....	68
NETWORK DIAGRAM 29.....	68
NETWORK DIAGRAM 30.....	68
NETWORK DIAGRAM 31.....	68
NETWORK DIAGRAM 32.....	69
NETWORK DIAGRAM 33.....	70
NETWORK DIAGRAM 34.....	73

ABBREVIATIONS

MPLS: Multiprotocol Label Switching
VPN: Virtual Private Networks
PHP: Penultimate Hop Popping
OSFP: Open Shortest Path First
IS-IS: Intermediate System to Intermediate System
ISP: Internet Service Provider
BGP: Border Gateway Protocol
LSP: Label Switched Path
IGP: Interior Gateway Protocol
CE: Customer Edge router
PE: Provider Edge router
P: Provider router
LDP: Label Distribution Protocol
IP: Internet Protocol
MP-BGP: Multiprotocol Border Gateway Protocol
RSVP-TE: Resource Reservation Protocol-Traffic Engineering
CSPF: Constrained-Based Shortest Path First
FIB: Forwarding Information Base
LFIB: Label Forwarding Information Base
FRR: Fast Re-route
QoS: Quality of service
BFD: Bidirectional Forwarding Detection
ERO: Explicit Route Object
FEC: Forwarding Equivalent Class
PLR: Point of Local Repair
MP: Merge Point
NHop: Next-hop
NNHop: Next-next-hop
PHP: Penultimate Hop Popping
VoIP: Voice over Internet Protocol
VRF: Virtual Routing and Forwarding

INTRODUCTION

The Internet Service Provider (ISP) provides connectivity to end users and enterprise companies, and the internetworking between different ISPs forms the Internet. IP-Protocol is the principal protocol for information exchange, it uses network packets in the delivery of data between the source and the destination, a router which uses IP network analyses the destination address of data packets to determine the shortest path and without considering other factors that may affect the connection such as latency and congestion. It is very difficult to source route the packet from source to destination in IP networks.[19][2]

As voice, video and data networks merge they inherit service level requirements of their composite functions and therefore the network should display very high levels of reliability and availability. Downtime must consequently be kept to a minimum, and backup resources must be provided to take over when any component fails. It is not only the availability that the individual customers expect but they also need reasonable levels of bandwidth, similarly corporate customers may have data streams that are sensitive to delays and disruption.[6]

Therefore MPLS is required which not only provides traffic engineering but also provides protection and restoration for network failures.

As the path which the packet will take is not known in advance hence it is difficult to implement network protection techniques in routers which use IP networks. The Multiprotocol Label Switching (MPLS) overcomes drawbacks of IP networks, as MPLS establishes a connection oriented communication over the connectionless IP network.[19] MPLS overlays an IP network to allow resources to be reserved and paths pre-determined. It provides tunnels through the network to connect devices that lie at the edge of the network and therefore traffic engineering can be implemented for the packet moving from one network to the other network. [8][1]

MPLS is growing in popularity for provisioning and managing core networks like those of ISPs, voice-centric like those of traditional telecommunications companies, or one of the modern networks that combine voice, video and data. [6]

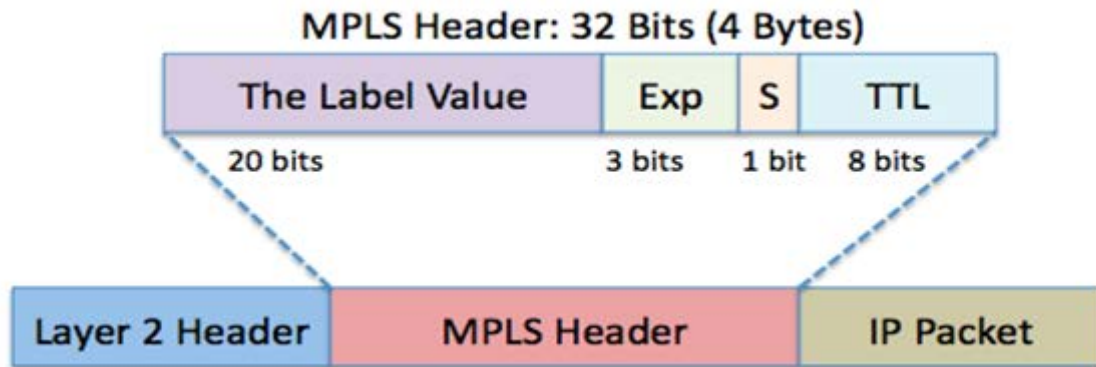
MULTIPROTOCOL LABEL SWITCHING

MPLS allows data to be transported using the Layer 2 (switching) rather than the Layer 3 (routing) level, MPLS sets up a path for a given sequence of a packet by placing a label on each data packet and therefore reducing time for look up for the next hop in the IP tables.[19]

This makes moving data packet traffic faster, and allows network management easier.[19]

The MPLS uses labels to identify virtual links (paths) between distant nodes rather than endpoints[19], MPLS prepend a label to a data packet that informs the network about the destination of data packet.

MPLS works by adding an MPLS header containing one or more MPLS labels to the data packet it is also called as label stack. The MPLS header is placed between the Layer 2 header and Layer 3 header and thus it is called Layer 2.5 header. Network diagram illustrates an example of a MPLS header. [19]



(network diagram source wikipedia)

FIGURE 1 MPLS HEADER

Each label stack entry is made up of 32 bits and is divided into following four fields:[19][25]

- Label = 20 bits
- TC (Traffic Class) also known as EXP (Experimental) = 3 bits
- S (Bottom of stack) = 1 bit
- TTL (Time To Live) =8 bits

Label bits are used for forwarding the labeled packet through the network.[19][25]

TC bits are reserved for experimental use, these bits are also used for QoS and ECN (Explicit Congestion Notification).[19][25]

S bit is the bottom of a stack flag. It tells if the current label is the last label or it is followed by other MPLS labels.[19][25]

TTL bits are propagated from the IP TTL at the ingress PE and is propagated back to the IP packet at the egress PE. TTL is used to prevent loops in network.[19][25]

Terminology Used in MPLS Networks:

Label Switched Path (LSP): LSP is the route MPLS data packets use from the ingress PE to the egress PE on the network. LSPs are unidirectional and need to be configured on every node.[19][24]

Customer Edge router (CE): This is the router at the customer network that connects to the service provider network(PE).[19][24]

Provider Edge router (PE): This is the last router between the service provider's network and the customer network(CE). It can be a router between two internetworked service providers(ISP's).[19][24]

Provider network: This is the network at the service provider end, it can be used to connect customer sites or it can also be used for internetworking between ISP's. [19][24]

Customer network: This is the network at the customer's premises. It is configured and managed locally by the customer.[19][24]

Provider router (P): This is a transit router inside the service provider's network. It connects one or more PE/P routers. [19][24]

For maintaining MPLS forwarding information IP/MPLS capable routers maintain Label Forwarding Information Base (LFIB) which store the port and the corresponding MPLS router label.

In the MPLS network classification is done only by the ingress PE and forwarding is done hop-by-hop inside the Service Provider Network.[19][24]

For carrying IP packet over MPLS network, packet is prepended by MPLS headers. On the basis of MPLS header, ingress PE router identifies the egress PE to which the traffic is destined and the corresponding LSP for that traffic flow. [19][24]

IP packet coming from customer side (CE Router) enters the network, the ingress PE router checks the FIB and identifies the route to the egress PE router. It then checks the corresponding destination label in its LFIB and adds an MPLS label to the packet. [19][26]

The process of adding an MPLS label to IP Packet at ingress PE is called push. [19][26]

As a MPLS packet enters the P router, the router checks its LFIB to determine the next hop. The incoming label is then removed and replaced with the outgoing label and the packet is forwarded. [19][26]

The process of removing incoming label and replacing it with an outgoing label on the provider network is called swap. [19][26]

When packet comes at egress PE router, a normal IP lookup is done to determine which link to forward the data. The MPLS label is then removed and the packet is forwarded as an IP packet.

The removing of the label is referred to as a pop. [19][26]

The popping of the MPLS label by the PE egress router can slow the network since the process needs more processing power(As it is running MPLS and routing protocol together). To reduce the processing needed by the PE egress router, a process called **Penultimate Hop Popping (PHP)** is used in which the P router before the egress PE router pops the MPLS label and forwards IP packet to the egress PE router. The P router that performs PHP is informed by the neighboring PE egress router by sending implicit-null as its local label which is then used by the P router as the outgoing label. [19][26]

Virtual Private Networks

A Virtual Private Network is a private communication network that makes use of the public ISP for secure access to different sites of the organization's(Customer) network. [1]

MPLS allows the tunneling of packets from the ingress PE router to the egress PE Router[1] and therefore VPN networks can be configured using MPLS in the service provider network.

MPLS VPN's are network based which provides for traffic separation by uniquely identifying each VPN flow. A VPN consists of CE routers attached with the VPN aware PE router of the service Provider network. The customer sites use the CE routers to communicate with other customer site network(CE). Only the PE routers are aware of the VPN process. [1][24]

The CE router provides the PE router with the routing information of the corresponding customer site by using separate routing and forwarding table called the Virtual Routing and Forwarding table (VRF) .[1]

PE router maintains a separate VRF table for connection between each PE-CE ,so that VPN routes can be separated from the Global routing table, and also from other customer VPN's. Each PE router allocate a unique route distinguisher(RD) which allows VPN forwarding in the backbone of the network, also if two customers are attached to same PE router than PE router allocates a unique label to each route in each VRF(VPN LABEL). The PE routers exchange information about the VPN customers and routes among themselves by using Multiprotocol Border Gateway Protocol.[1][24]

LAYER 3 VPN

In Layer 3 VPN each customer can use RFC1918 addresses(In lab setup both companies ABC and XYZ use same 192.168.1.0/24 and 192.168.2.0/24 networks) so, as to make VRF addresses unique provider routers use 64 bit prefix called route distinguisher (RD) to separate the routes of two companies in Service Provider network, similarly to distinguish traffic between different VPN's it uses VPN Label which helps the PE router to forward the traffic to correct VPN site, this label stacking for each of the IP packets is done by the ingress PE router.

Therefore In Layer 3 VPN , at least two MPLS headers are used (the outer label is known as transport label and the inner label is called VPN label).

These two MPLS headers are called an MPLS header stack. Network diagram shows an example of a MPLS header stack. [19]



FIGURE 2 MPLS header stack

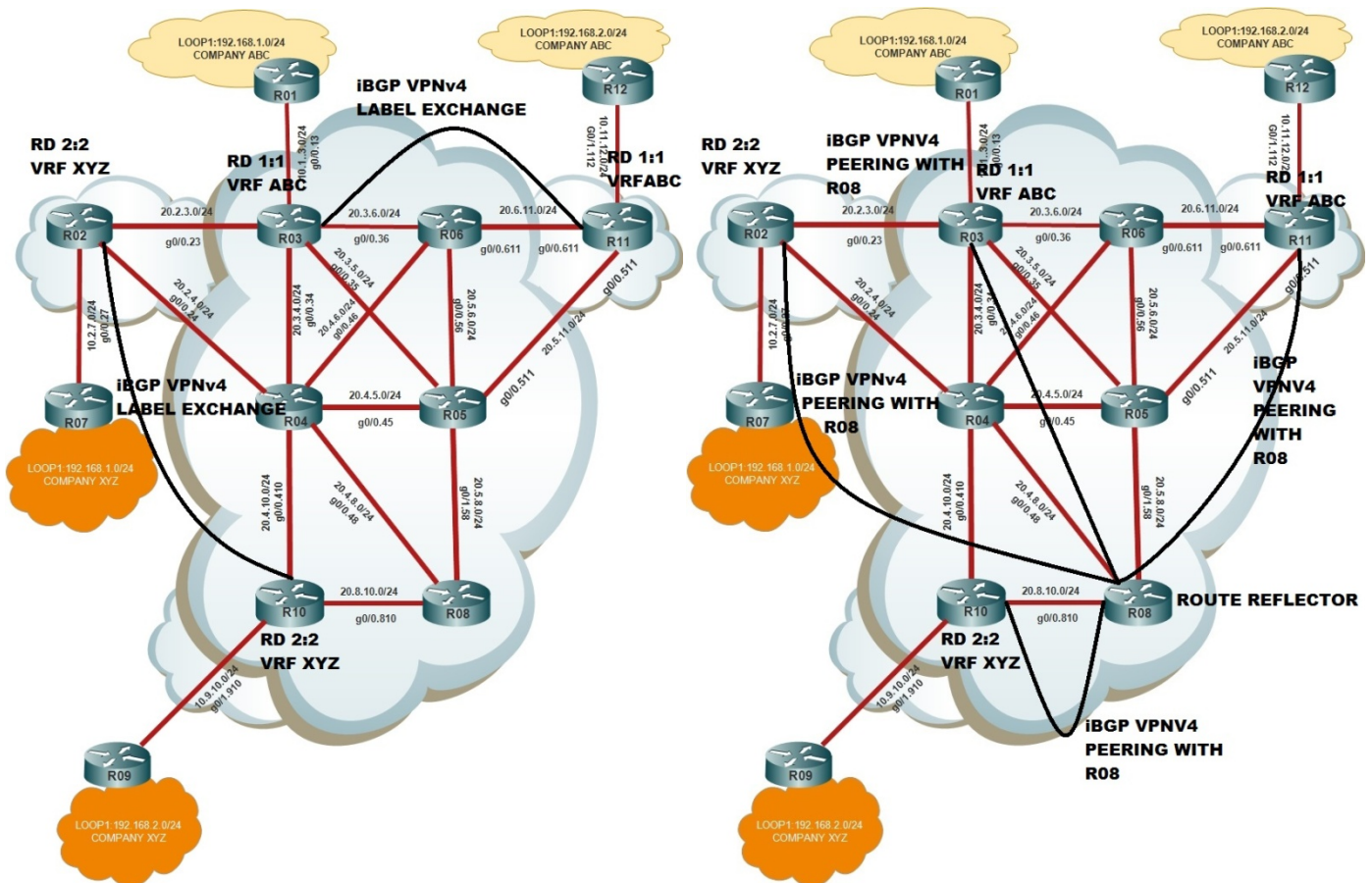
The outer header (transport header) is used for transporting the packet from the ingress router to the egress router(transport label is obtained from the global forwarding table).[19] The inner header(VPN label) differentiate different VPN's connected on the PE router.

The ingress router learns the outer label through either RSVP(in case explicit path are defined) or LDP protocols. [19]

Layer 3 VPN's inner label is learnt through MP-BGP.

Both labels are combined into an MPLS label stack, are attached in front of the IP packet, and are sent toward the egress PE-router. All the P-routers in the network switch the VPN packet based only on the top label in the stack(Transport Label), which is pointing toward the egress PE router. [1][24]

The egress PE-router on receiving this labeled packet, drops the first label, and performs a lookup on the second label, which uniquely identify the target VRF . A lookup is performed in the target VRF, and the packet is sent toward the proper CE router.[1][24]



NETWORK DIAGRAM 1: SHOWS iBGP VPNv4 PEERING BETWEEN PE ROUTERS

NETWORK DIAGRAM 2: SHOWS iBGP VPNv4 PEERING BETWEEN PE'S AND ROUTE REFLECTOR

PE routers exchange information about the VPN customers using Multiprotocol Border Gateway Protocol. In lab setup instead of peering between different sites PE routers ,peering is done between each PE and route reflector which is R08 in this case.

```

File Edit View Options Transfer Script Tools Window Help
Enter host <Alt+R>
MINT R1 MINT R2 MINT R3 MINT R4 MINT R5 MINT R6 MINT R7 MINT R8 x
R8#show ip bgp vpnv4 all
BGP table version is 27, local router ID is 8.8.8.8
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, s stale, m multipath, b backup-path, f RT-Filter,
               x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

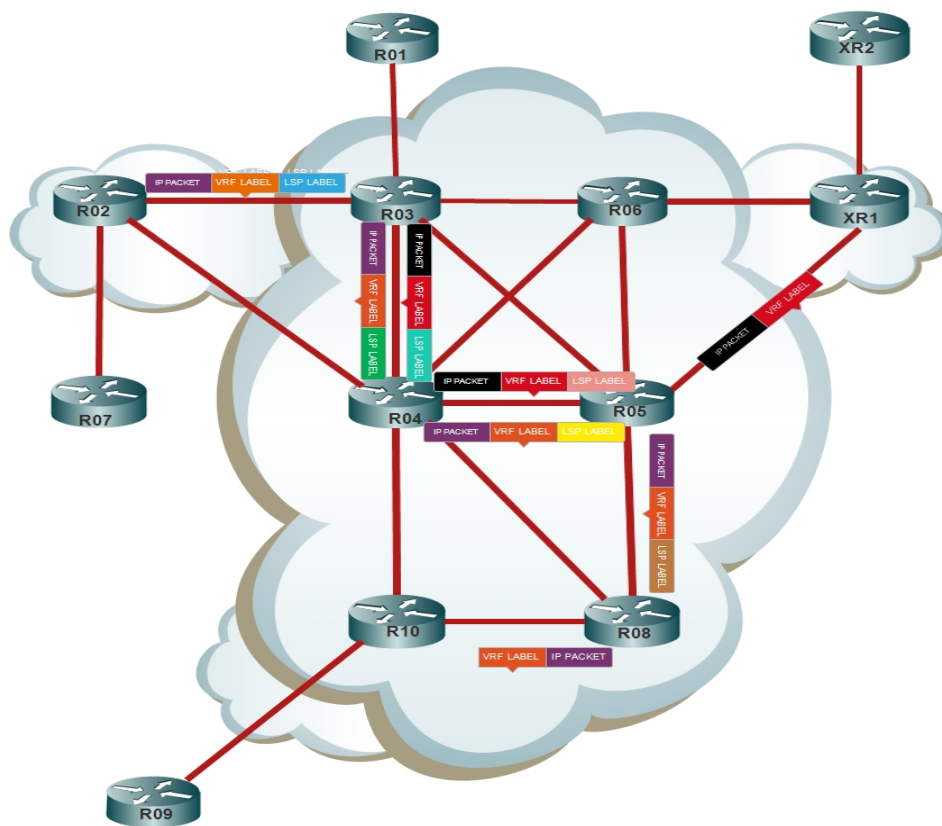
   Network          Next Hop        Metric LocPrf Weight Path
Route Distinguisher: 1:1
*>i 1.1.1.1/32       3.3.3.3         2      100    0 ?
*>i 10.1.3.0/24      3.3.3.3         0      100    0 i
*>i 10.11.12.0/24    11.11.11.11     0      100    0 i
*>i 12.12.12.12/32  11.11.11.11     2      100    0 ?
*>i 192.168.1.0      3.3.3.3         2      100    0 ?
*>i 192.168.2.0     11.11.11.11     2      100    0 ?
Route Distinguisher: 2:2
*>i 7.7.7.7/32       2.2.2.2         2      100    0 ?
*>i 9.9.9.9/32       10.10.10.10     2      100    0 ?
*>i 10.2.7.0/24      2.2.2.2         0      100    0 i
*>i 10.9.10.0/24     10.10.10.10     0      100    0 i
*>i 192.168.1.0      2.2.2.2         2      100    0 ?
*>i 192.168.2.0     10.10.10.10     2      100    0 ?
R8#

```

VPNv4 ROUTES FOR EACH SITE EXCHANGED WITH ROUTE REFLECTOR

Network diagram 3 below illustrates an MPLS network with an MPLS header stack. In this example, there are two companies that use core network. Customer ABC VPN site network and Customer XYZ VPN site. In order to connect company ABC site on R03 to company ABC other site on router R11, we have to use Layer 3 MPLS VPN, similar connection is required for company XYZ connected to PE R02 to other VPN site connected on PE R10.

Customer on R01 sends data to customer on R12 for company ABC, when packet comes at R03 it performs MPLS stacking in this case two labels are required (inner label is VPN label and outer label is transport label). When packet moves from R03 to R04 only the outer transport label is swapped and there is no change to inner VPN label. When packet moves from R04 to R05 then also only the outer transport label is swapped. When packet moves from R05 to R11 then outer label is removed and packet is passed to router R11 (Assuming PHP is activated), after packet is received on router R11 it checks the inner VPN label and according to VPN label it forwards the packet to the customer on R12 network belonging to company ABC. Similar procedure is followed when customer on R07 for company XYZ sends data on customer on R09 for company XYZ.



NETWORK DIAGRAM 3: IP Packet with two MPLS headers

```

R7#
R7#
R7#
R7#traceroute 9.9.9.9
Type escape sequence to abort.
Tracing the route to 9.9.9.9
VRF info: (vrf in name/id, vrf out name/id)
 0 10.2.7.2 0 msec 0 msec 0 msec
 1 20.2.3.3 [MPLS: Labels 322/10022 Exp 0] 0 msec 0 msec 4 msec
 2 20.3.4.4 [MPLS: Labels 419/10022 Exp 0] 0 msec 0 msec 4 msec
 3 20.4.5.5 [MPLS: Labels 519/10022 Exp 0] 0 msec 0 msec 0 msec
 4 20.5.8.8 [MPLS: Labels 822/10022 Exp 0] 0 msec 0 msec 4 msec
 5 20.9.10.10 [MPLS: Labels 10022 Exp 0] 0 msec 0 msec 0 msec
 6 10.9.10.9 4 msec 0 msec *
 7 10.9.10.9 4 msec 0 msec *
R7#
R7#
R7#
R7#

R1#
R1#traceroute 12.12.12.12
Type escape sequence to abort.
Tracing the route to 12.12.12.12
VRF info: (vrf in name/id, vrf out name/id)
 0 10.1.3.3 0 msec 0 msec 0 msec
 1 20.3.4.4 [MPLS: Labels 423/11021 Exp 0] 0 msec 4 msec 0 msec
 2 20.4.5.5 [MPLS: Labels 523/11021 Exp 0] 4 msec 0 msec 0 msec
 3 20.4.5.5 [MPLS: Labels 523/11021 Exp 0] 4 msec 0 msec 0 msec
 4 10.11.12.11 [MPLS: Labels 11021 Exp 0] 4 msec 0 msec 0 msec
 5 10.11.12.12 4 msec * 0 msec
R1#
R1#
R1#
R1#
    
```

TRACEROUTE SHOWS MPLS PACKETS DUAL STACKED FOR BOTH COMPANIES VPN TRAFFIC

SIGNALING PROTOCOLS IN MPLS

There are three signaling protocols in MPLS that are used to distribute the MPLS labels:[26]

LDP : Label Distribution Protocol

MP-BGP : Multiprotocol Border Gateway Protocol

RSVP-TE : Resource Reservation Protocol-Traffic Engineering

LDP and RSVP-TE are incapable of routing, hence IGP (Interior Gateway Protocol) is required for performing calculation of topology information to all the routers in the network. [19]

There are different IGP protocols like OSPF,IS-IS,RIP,EIGRP

RIP and EIGRP can't be used as routing as they can't forward the Traffic Engineering information.

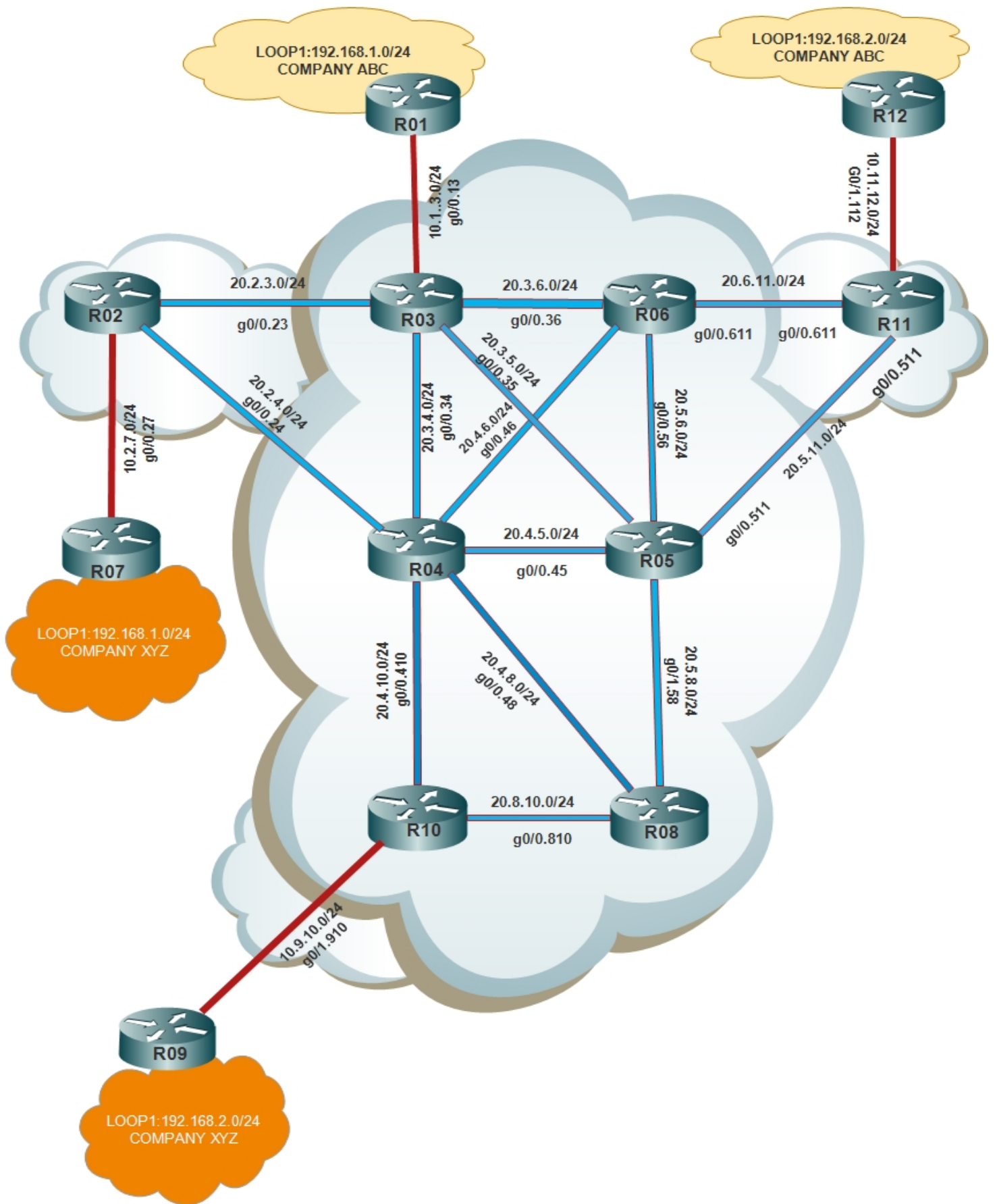
The Link State Protocol are used as they have extensions for traffic engineering.

There are two link protocols for traffic engineering:

1. Intermediate System to Intermediate System Extensions for TE(IS-IS TE)
2. Open Shortest Path First Extensions for TE(OSPF TE)

IS-IS TE is an extension of IS-IS which also performs IP routing on networks. It is a control plane protocol used by network operators to manage MPLS packets(LDP requires link state protocol for the distribution of labels). It advertises traffic engineering information to all the routers that are part of the same network, changes to the network resources, such as bandwidth, links and nodes disruption and/or failure, are instantly shared to all the routers in order to manage the network with failure information. IS-IS TE supports both LDP and RSVP-TE.[19]

In lab setup in provider network IS-IS TE is used. Blue lines connecting routers show on which router interfaces IS-IS TE is enabled.



NETWORK DIAGRAM 4: BLUE LINES IN NETWORK DIAGRAM SHOWS THE INTERFACES OF THE ROUTERS ON WHICH IS-IS TE IS ENABLED

Label Distribution Protocol

LDP can be used for label distribution in MPLS enabled network. Using LDP, routers in Service Provider network can map network layer routing information to data layer switching paths which helps in establishment of LSPs end to end between routers.[3] [27]

LSPs can be established between both neighboring routers and routers that are not directly connected, making label switching possible end to end in Service Provider network.[3][27]

There are four types of LDP messages:[3][27]

1. **Discovery message:** Used to declare and maintain the presence of routers on service provider network.[3][27]
2. **Session message:** Used to establish, maintain, and terminate sessions between LDP peers.[3][27]
3. **Advertisement message:** Used to create, modify, or remove label to FEC bindings.[3][27]
4. **Notification message:** Used to provide advisory information and information related to signal errors.[3][27]

TCP is used for following messages in LDP[27]

- a. Session messages
- b. Advertisement messages
- c. Notification messages

UDP is used for following messages in LDP[27]

- a) Discovery messages

Fundamental Operation of LDP[3][27]

LDP goes through four phases in operation

1. Discovery
2. Session establishment and maintenance
3. LSP establishment and maintenance
4. Session termination

Discovery

In discovery phase the router which wants to establish a session sends Hello messages to its neighboring routers periodically.[3]

LDP provides two discovery mechanisms:

Basic discovery mechanism

The basic discovery mechanism is used to discover local LDP routers(routers directly connected at link layer) and to establish local LDP sessions. Router periodically sends LDP link Hellos as UDP packets out an interface to its local router.[3]

Extended discovery mechanism

The extended discovery mechanism is used to discover remote LDP peers (routers not directly connected at link layer) and to establish remote LDP sessions. Router periodically sends LDP targeted Hellos as UDP packets to a given IP address of the interface or to loopback address of the remote router.[3]

2) Session establishment and maintenance[3]

In this phase, router perform following steps to establish sessions between routers:

1. Establishing transport layer connections (TCP connections) between routers.[3]
2. Initializing sessions and negotiating session parameters (LDP version, label distribution mode, label spaces, timers)[3]

To maintain sessions LSRs send Hello messages and Keepalive messages to each other.[3]

3) LSP establishment and maintenance

For establishing LSP's routers bind FECs with labels and notify adjacent routers of these bindings.

When there is a change in network topology, ingress PE router checks its routing table and if ingress PE router finds in its routing table a new destination address for which no entry exist in FEC, then PE assigns new FEC for the destination address and determine the route for the FEC that are to be used. For this the ingress PE creates label request message that contains the FEC requiring a label and sends the message to its downstream routers (DoD mode)[3][27]

Upon receiving the label request message, the downstream routers records this request message, they then find in their routing table the next hop for the FEC, and sends the label request message to their downstream routers.[3][27]

This process of recording and sending the label request message to downstream routers keeps on occurring until the destination router is reached. When the label request message reaches the destination router, destination router checks if it has spare label, it validates the label request message and assigns label to the FEC.

Then, the router creates a label mapping message containing the assigned label and sends the message to its upstream routers.[3][27]

Upon receiving the label mapping message, an upstream routers checks the status of the corresponding label request message that is locally maintained. If it has information about the request message, the router assigns a label to the FEC, and adds an entry in its LFIB for the binding, and sends the label mapping message on to its own upstream routers.[3][27]

When the ingress PE router receives the label mapping message, it adds an entry in its LFIB, resulting in establishment of LSP, and now the packets of the FEC is label switched along the LSP.[3][27]

4) Session termination

LDP checks Hello messages to determine adjacency and checks Keepalive messages to determine the integrity of sessions[3], if Hello and Keepalive messages are being dropped then the session is terminated.

For advertisement of Labels in LDP two type of modes are common :

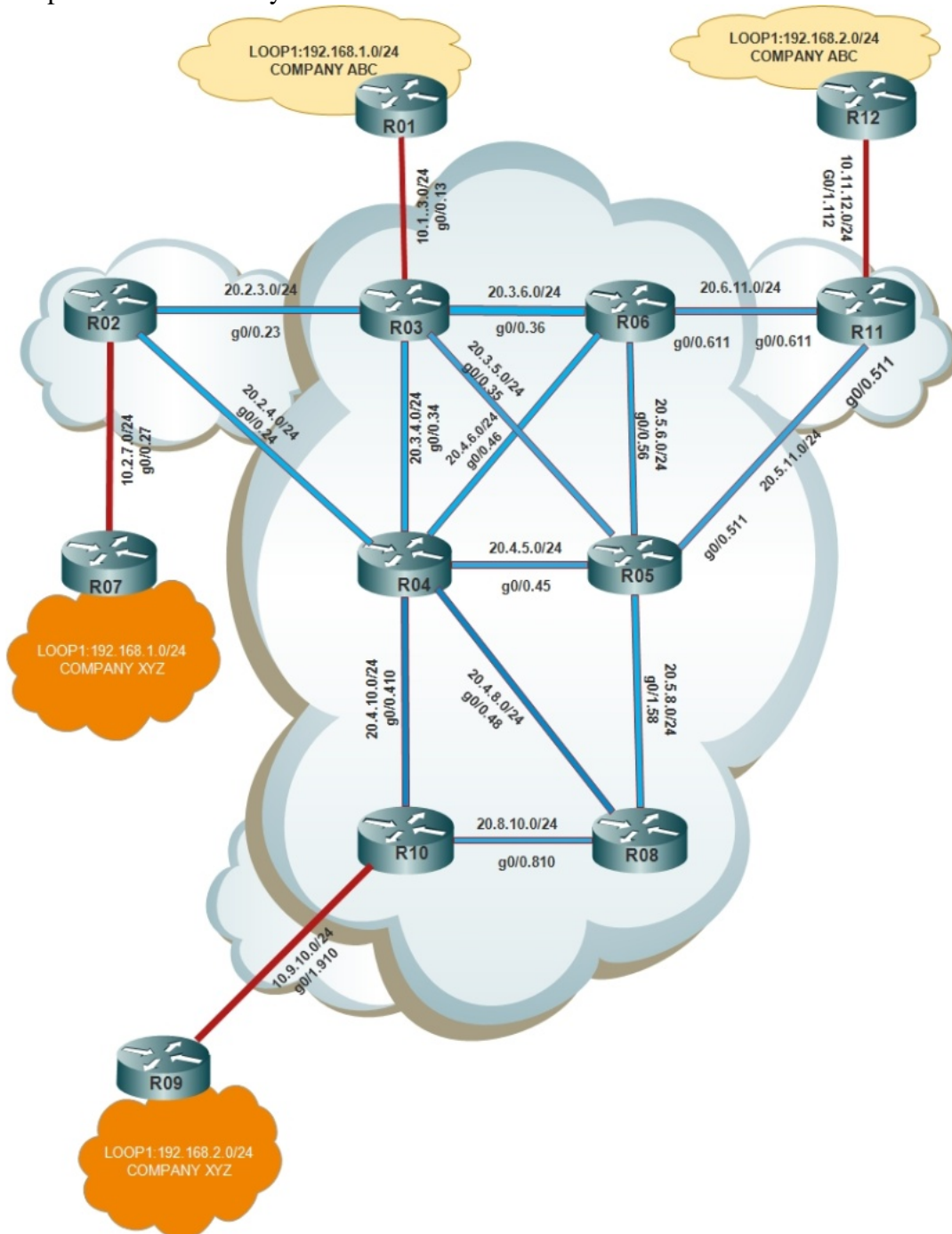
DoD mode

In DoD mode, an upstream router sends a label request message containing the description of a FEC to its downstream router, which assigns a label to the FEC, encapsulates the binding information in a label mapping message and sends the message back to it.[3]

DU mode

In DU mode downstream router advertises label binding information to its upstream routers unsolicited after the LDP session is established.[3]

For avoiding black holes LDP protocol should be enabled only on those interfaces of the router on which routing protocol is enabled(IS-IS TE or OSPF-TE), as routing protocols have their own loop prevention techniques, so loops in LSP created by LDP can be avoided.

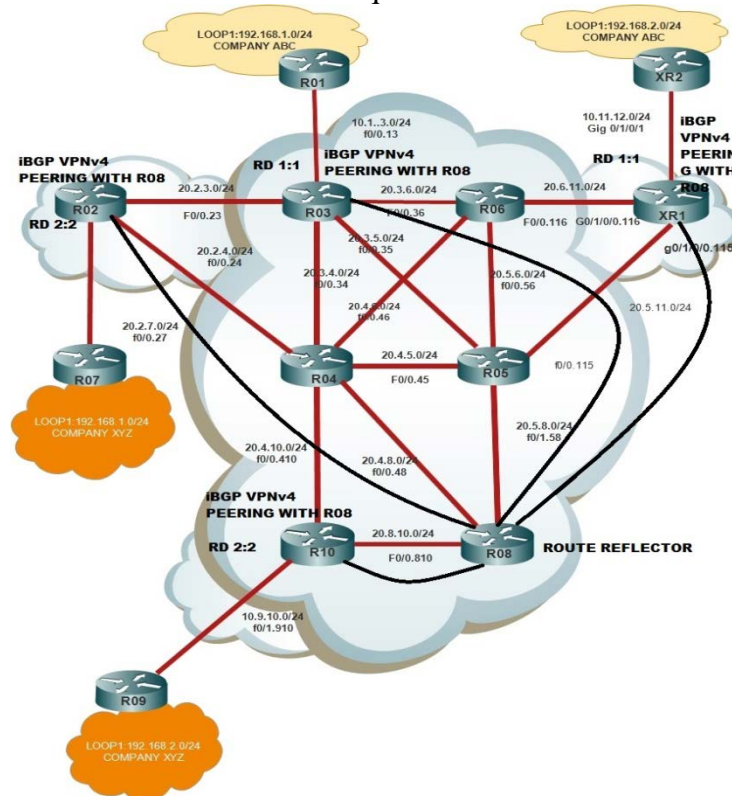


Network diagram 5: shows the links in BLUE color on which LDP protocol and routing protocol (IS-IS TE) is enabled

Multiprotocol Border Gateway Protocol

Multiprotocol Border Gateway Protocol (MP-BGP) also known as Multiprotocol BGP is an extension of Border Gateway Protocol (BGP) that allows different types of addresses (address families) to be distributed. Unlike BGP which supports only IPv4 unicast addresses, MP-BGP supports both IPv4 and IPv6 addresses and both unicast and multicast variants of each address category. It is used in MPLS and IP VPNs (Layer 3 VPNs).[19]

In lab setup MP-BGP is used for connecting different PE routers and for scalability Route Reflector is established for sending VPNv4 information between required PE routers.



NETWORK DIAGRAM 6: MP-BGP BETWEEN ROUTE REFLECTOR AND PE ROUTERS CONTAINING VPNv4 INFORMATION

```

R8#show ip bgp vpnv4 all
BGP table version is 27, local router ID is 8.8.8.8
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
               x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

   Network          Next Hop        Metric LocPrf Weight Path
Route Distinguisher: 1:1
*>i 1.1.1.1/32       3.3.3.3         2      100      0 ?
*>i 10.1.3.0/24     3.3.3.3         0      100      0 i
*>i 10.11.12.0/24   11.11.11.11    0      100      0 i
*>i 12.12.12.12/32  11.11.11.11    2      100      0 ?
*>i 192.168.1.0     3.3.3.3         2      100      0 ?
*>i 192.168.2.0    11.11.11.11    2      100      0 ?
Route Distinguisher: 2:2
*>i 7.7.7.7/32      2.2.2.2         2      100      0 ?
*>i 9.9.9.9/32      10.10.10.10    2      100      0 ?
*>i 10.2.7.0/24     2.2.2.2         0      100      0 i
*>i 10.9.10.0/24    10.10.10.10    0      100      0 i
*>i 192.168.1.0     2.2.2.2         2      100      0 ?
*>i 192.168.2.0    10.10.10.10    2      100      0 ?
R8#
    
```

MP-BGP USED BETWEEN ROUTE REFLECTOR AND PE ROUTERS TO GET VPNv4 INFORMATION

Resource Reservation Protocol-Traffic Engineering

Resource Reservation Protocol (RSVP) reserves resources on each router along a path on which reservation is desired. RSVP operates at the transport layer and it don't participate in data transmission. RSVP works Unidirectional (resources are reserved only in one direction), the router that initiates resource reservation requests is responsible for maintaining reservation information by sending Path and Resv messages.[28]

Extended RSVP(RSVP-TE) can support MPLS label distribution and allow resource reservation information to be transmitted with label bindings. RSVP-TE operates as a signaling protocol for LSP tunnel setup in MPLS TE. [3]

Each LSP set up using RSVP-TE is assigned a resource reservation style. During an RSVP session, the receiver decides which reservation style can be used for this session and thus which LSPs can be used.[3]

There are two common resource reservation style used by RSVP-TE:[3][28]

1. **Fixed-filter style (FF)** :In this resources are reserved for individual senders and cannot be shared among senders on the same session.[3][28]
2. **Shared-explicit style (SE)**:In this resources are reserved for senders on the same session and shared among them.[3][28]

RSVP-TE messages[3][28]

RSVP-TE uses RSVP messages with extensions. The following are RSVP messages that are used:

1. **Hello messages**: Hello messages are sent between two directly connected RSVP neighboring routers to set up and maintain the neighbor relationship that has local significance on the link.[3][28]
2. **Path messages**: Path messages are transmitted along the path of data transmission downstream by each RSVP sender to save path state information on each router along the path. [3][28]
3. **Resv messages**: Resv messages are sent by each receiver upstream towards senders to request resource reservation .Resv messages are also used to create and maintain reservation state on each router along the opposite direction of data transmission path.[3][28]
4. **PathTear messages**: PathTear messages are sent downstream immediately after the failure to remove the path state and related reservation state on each router along the path.[3][28]
5. **ResvTear messages**: ResvTear messages are sent upstream immediately after the detection of failure to remove the reservation state on each router along the path.[3]
6. **PathErr messages**: PathErr messages are sent upstream to report Path message errors to senders.[3]
7. **ResvErr messages**: ResvErr messages are sent downstream to notify the downstream nodes that error occurs during Resv message processing.[3]
8. **ResvConf messages**: ResvConf messages are acknowledgement messages for Resv messages.[3]

The TE extension to RSVP adds new objects to the Path message and the Resv message. These objects carry not only label bindings but also routing constraints(to support FRR protection)[3]

New objects added to the Path message include [28]

1. LABEL_REQUEST
2. EXPLICIT_ROUTE, RECORD_ROUTE
3. SESSION_ATTRIBUTE

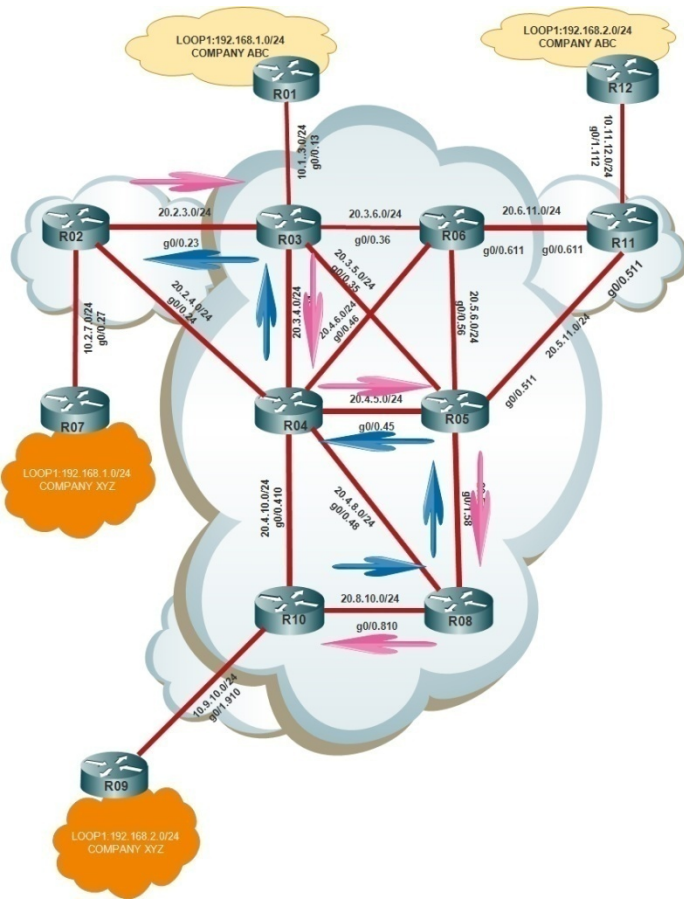
New objects added to the Resv message include [28]

1. LABEL

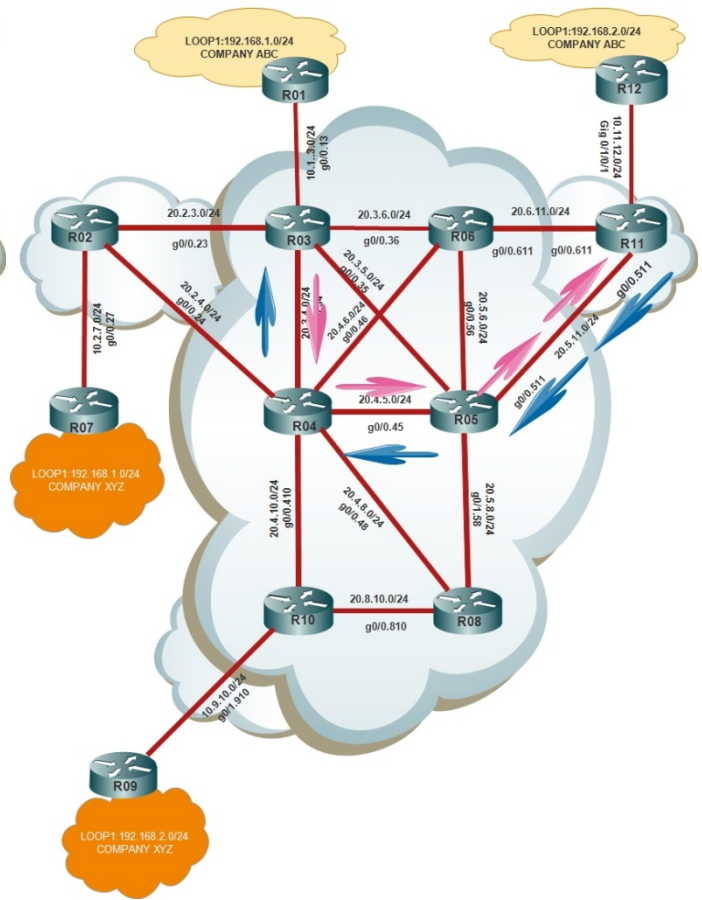
2. RECORD_ROUTE[3]

Setting up an LSP tunnel

Network diagram 7 shows PATH (pink) and RESV messages (blue) when tunnels for explicit path from R02 to R10 for company XYZ is created, for communication originating from R07 to R09.



Network diagram 7: shows PATH (pink) and RESV messages (blue) when tunnels for explicit path from R02 to R10 for company XYZ is created, for communication originating from R07 to R09



Network diagram 8: shows PATH (pink) and RESV messages (blue) when tunnels for explicit path from R03 to R11 for company ABC is created, for communication originating from R01 to R12

Similar in Network Diagram 8, tunnel is created for company ABC between R03 and R11 for defining explicit path from customer on R01 to customer on router R12.

Procedure for setting up an LSP tunnel with RSVP:

- 1) The ingress PE router sends a Path message towards the egress PE router.[3]
- 2) After receiving the Path message, the egress PE router sends back a Resv message towards the ingress PE router. The routers that the Resv message traverses along the path reserve resources as required. [3]
- 3) When the ingress PE router receives the Resv message, LSP is established.[3]

As resources are reserved on the routers along the path for the LSP establishment using RSVP-TE, services on the LSP are guaranteed. [3]

RSVP maintains path and reservation state by periodically retransmitting two types of messages: Path and Resv. These periodically retransmitted Path and Resv messages are called refresh messages. They are sent

along the path that the last Path or Resv message travels to synchronize state between RSVP neighbors and recover lost RSVP messages.(Also known as Soft State)[3]

LSP Selection Mechanism

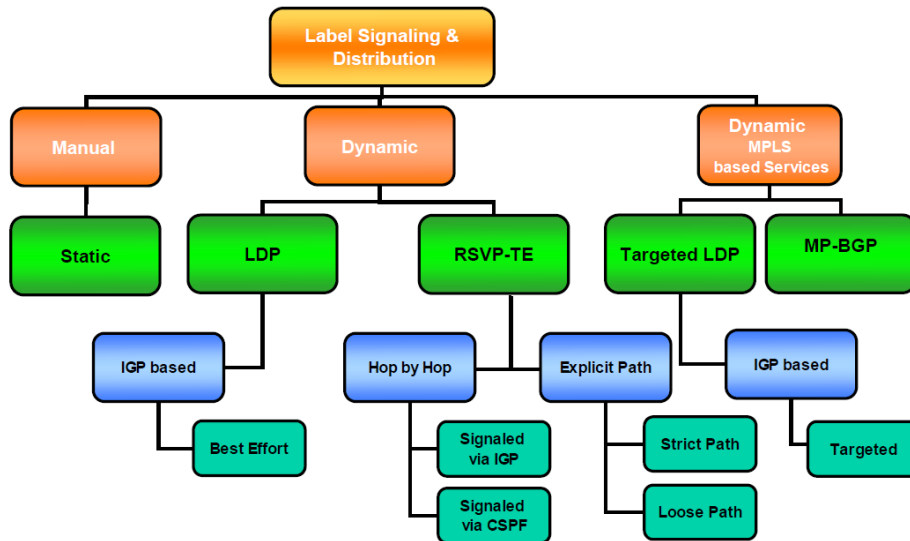
Two methods are defined for LSP selection in MPLS network:

HOP-BY-HOP

EXPLICIT ROUTING

Hop-by-Hop Routing the routers send requests, and distribute and release label binding information. The routers discover neighboring routers and establish a session with them.[19]

Explicit routing In explicit routing the entire list of nodes in which the data packet will pass is specified in advance. [19]



LDP SIGNALLING AND DISTRIBUTION (SOURCE wikipedia)

MPLS Traffic Engineering

The Internet has transformed into multiservice medium converging voice, video, and data communication networks. In ISP network there is need to deploy service differentiation for different packets ,so that ISPs can provide various classes of service for different customers. In order to provide such capabilities in the network, the basic traffic forwarding mechanism used in Internet must be enhanced to support traffic engineering. Traffic engineering helps in enhancing performance of network through guaranteed quality of service (QoS), improving utilization of network resources by distributing traffic evenly across network links, and providing for quick recovery when a node or link fails.[4]

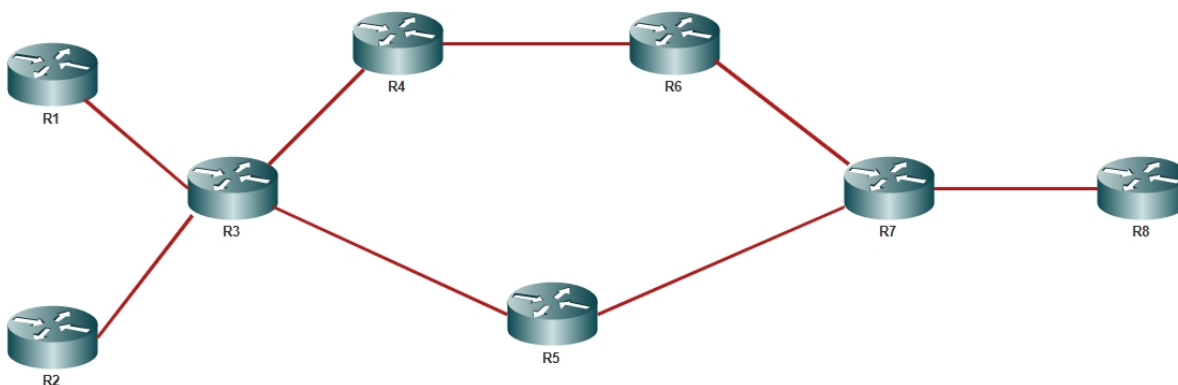
In an MPLS traffic-engineered network, any Label-Switched Path (LSP) can be dynamically shifted from a congested path to an alternative path. This represents an efficiency improvement over the traditional operational methods for IP networks.[4]

The following are the advantages of using MPLS traffic engineering in core networks:

1. With MPLS, traffic engineering capabilities are integrated into Layer 2, which makes switching of packets much faster.[4]
2. With the help of MPLS-TE routers can route IP traffic flows across a network based on the resources the traffic flow requires and the resources available in the network.[4]
3. With the help of MPLS-TE routers can perform constraint-based routing, which helps in finding the shortest path for the traffic that meets the resource requirements and constraints(bandwidth, QoS etc)[4]
4. MPLS-TE enabled networks can dynamically recovers from link or node failures by adapting to a new set of constraints after the failure.[4]
5. MPLS-TE enables unequal-cost load sharing and permits the use of paths other than IGP learned paths.[4]

1)PROBLEM SOLVED BY TRAFFIC ENGINEERING

In IP routing networks, IP Packets between two points is sent over the shortest path available even though multiple paths may exist. During traffic congestion, this may lead to some routes being over utilized and some routes being underutilized, this results in inefficient utilization of network resources. MPLS-TE manages network resources more efficient by specifying explicit routes and by setting certain bandwidth guarantees. MPLS-TE computes a path at the source taking into account all the constraints imposed while calculation of the paths.[1][2]



NETWORK DIAGRAM 9

In Network Diagram 9 ,if dynamic protocols are implemented for connection between R1 to R8 (assuming each path has same cost and bandwidth),R1 will take path R1-R3-R5-R7-R8 which will result in overutilization of the link from R3-R5-R7 whereas link between R3-R4-R6-R7 will be underutilized.

To solve this problem MPLS-TE can be employed so, that router R3 use both the path to reach router R8,for traffic flowing from R3 to R7 upper path(R3-R4-R6-R7) can be explicitly defined and for traffic flowing in reverse from R7 to R3 lower path(R8-R7-R5-R3) can be explicitly defined.

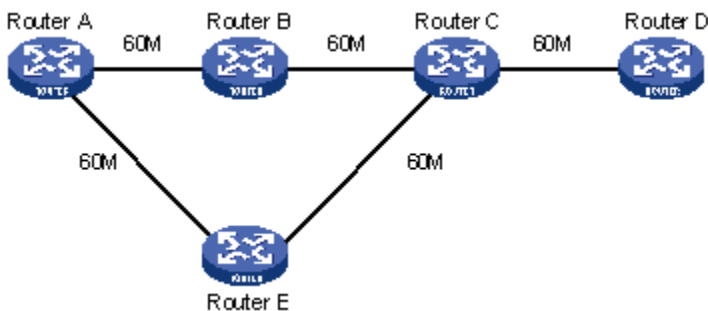
2)PROBLEM SOLVED BY TRAFFIC ENGINEERING

In addition to supporting explicit routing MPLS also has the ability to distribute information about network resources and topology, reserve network resources and modify link attributes. MPLS Traffic Engineering (MPLS TE) increases the availability and the value of the network to users. [1]

RSVP-TE is commonly used for MPLS Traffic Engineering.

MAKE-BEFORE-BREAK[2]

Make-before-break is a mechanism to change MPLS TE tunnel attributes with minimum data loss and without extra bandwidth.



Network Diagram 10:For Make-Before-Break

Network diagram 10 presents a scenario where a path Router A → Router B → Router C → Router D is established with 30 Mbps reserved bandwidth between Router A and Router D. The remaining bandwidth is then 30 Mbps. [2]

If 40 Mbps path bandwidth is requested, the remaining bandwidth of the Router A → Router B → Router C → Router D path will be inadequate. The problem cannot be addressed by selecting another path, Router A → Router E → Router C → Router D, because the bandwidth of the Router C → Router D link is inadequate.[19]

To address the problem, you may use the make-before-break mechanism. It allows the new path to share the bandwidth of the original path at the Router C → Router D link. Upon creation of the new path, traffic is switched to the new path and the previous path is torn down.[2]

For company XYZ

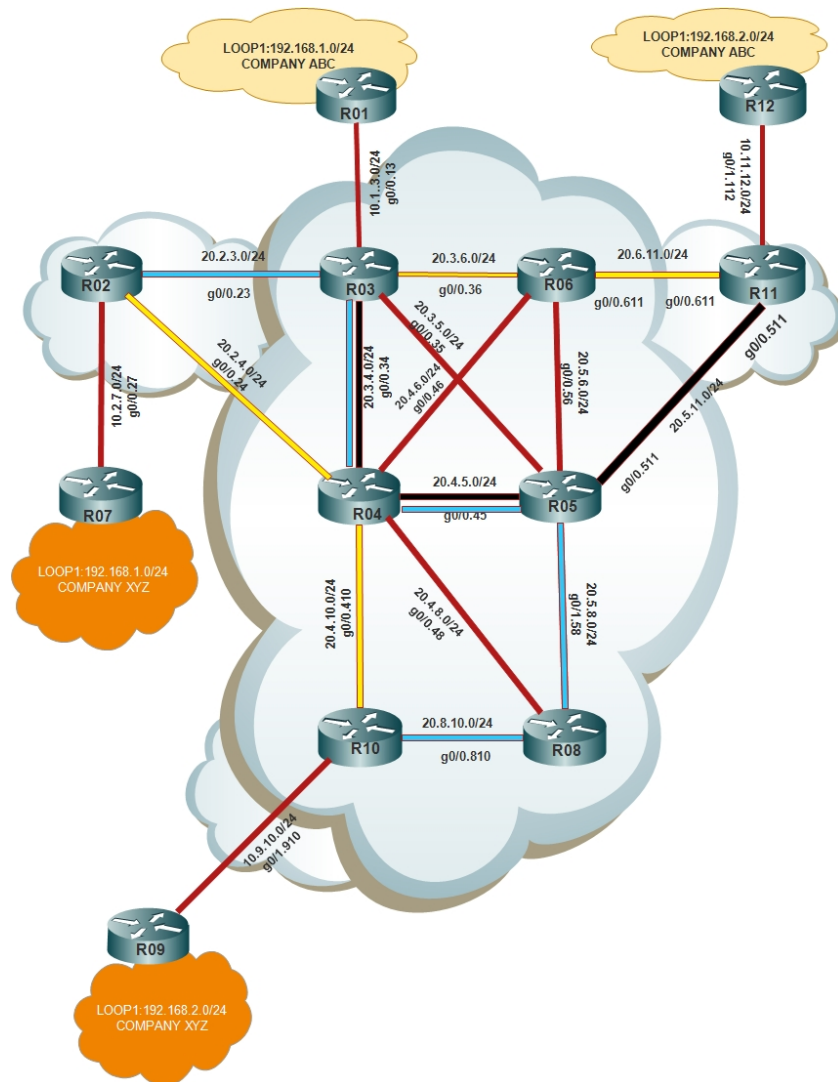
The network that is used in lab demonstration for communication initiated from customer on R07 to customer on R09 path followed is R07-R02-R03-R04-R05-R08-R10-R09.

Similarly for company ABC

For communication initiated for customer on R01 to R12 path followed is R01-R03-R04-R05-R11-R12

Below network diagram show the path that will be followed if no traffic engineering is used(path yellow for communication originating from customer R07 and R1 for company XYZ and ABC to R09 and R12 respectively)

and path shown by blue are explicit path defined for customer on R07 for company XYZ to R09(traffic flowing from R07 towards R09) ,similarly explicit path (in black) for customer on R1 for company ABC going to R12.



Network diagram 11:shows traffic flowing from R07 and R01 towards R09 AND R12 for companies XYZ(BLUE PATH) AND ABC(BLACK PATH) Respectively

```

File Edit View Options Transfer Script Tools Window Help
Enter host <Alt+R>
MINT R1 MINT R2 x MINT R3 MINT R4 MINT R5 MINT R6 MINT R7 MINT R9 MI
R2#show mpls traffic-eng tunnels tunnel 0
Name: R2_t0 (Tunnel0) Destination: 10.10.10.10
Status:
Admin: up Oper: up Path: valid Signalling: connected
path option 10, type explicit TO_R9 (Basis for Setup, path weight 50)

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 10 is active
BandwidthOverride: disabled LockDown: disabled verbatim: disabled

InLabel : -
OutLabel : GigabitEthernet0/0.23, 322
RSVP Signalling Info:
Src 2.2.2.2, Dst 10.10.10.10, Tun_Id 0, Tun_Instance 49
RSVP Path Info:
My Address: 20.2.3.2
Explicit Route: 20.2.3.3 20.3.4.3 20.3.4.4 20.4.5.4
20.4.5.5 20.5.8.5 20.5.8.8 20.8.10.8
20.8.10.10 10.10.10.10
Record Route: NONE
Tspec: ave rate=0 kbits, burst=1000 bytes, peak rate=0 kbits
RSVP Resv Info:
Record Route: 3.3.3.3(322) 4.4.4.4(419)
5.5.5.5(519) 8.8.8.8(822)
10.10.10.10(0)
Fspec: ave rate=0 kbits, burst=1000 bytes, peak rate=0 kbits
Shortest Unconstrained Path Info:
Path Weight: 30 (TE)
Explicit Route: 20.2.4.2 20.2.4.4 20.4.8.4 20.4.8.8
20.8.10.8 20.8.10.10 10.10.10.10

History:
Tunnel:
Time since created: 27 minutes, 30 seconds
Time since path change: 10 minutes, 22 seconds
Number of LSP IDs (Tun_Instances) used: 49
Current LSP:
Uptime: 10 minutes, 22 seconds
Prior LSP:
ID: path option 10 [7]
Removal Trigger: configuration changed
R2#

```

SHOWS EXPLICITLY DEFINED PATH FOR TRAFFIC FROM R07 FLOWING TOWARDS R09 AND ESTABLISHMENT OF TUNNEL0 AT R02 FOR COMPANY XYZ

```

File Edit View Options Transfer Script Tools Window Help
Enter host <Alt+R>
MINT R1 MINT R2 MINT R3 x MINT R4 MINT R5 MINT R6 MINT R7 MINT R9 MINT
R3#show mpls traffic-eng tunnels tunnel 0
Name: R3_t0 (Tunnel0) Destination: 11.11.11.11
Status:
Admin: up Oper: up Path: valid Signalling: connected
path option 10, type explicit TO_R11 (Basis for Setup, path weight 30)

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 10 is active
BandwidthOverride: disabled LockDown: disabled verbatim: disabled

InLabel : -
OutLabel : GigabitEthernet0/0.34, 423
RSVP Signalling Info:
Src 3.3.3.3, Dst 11.11.11.11, Tun_Id 0, Tun_Instance 7
RSVP Path Info:
My Address: 20.3.4.3
Explicit Route: 20.3.4.4 20.4.5.4 20.4.5.5 20.5.11.5
20.5.11.11 11.11.11.11
Record Route: NONE
Tspec: ave rate=0 kbits, burst=1000 bytes, peak rate=0 kbits
RSVP Resv Info:
Record Route: 4.4.4.4(423) 5.5.5.5(523)
11.11.11.11(0)
Fspec: ave rate=0 kbits, burst=1000 bytes, peak rate=0 kbits
Shortest Unconstrained Path Info:
Path Weight: 20 (TE)
Explicit Route: 20.3.5.3 20.3.5.5 20.5.11.5 20.5.11.11
11.11.11.11

History:
Tunnel:
Time since created: 6 minutes, 26 seconds
Time since path change: 6 minutes, 25 seconds
Number of LSP IDs (Tun_Instances) used: 7
Current LSP:
Uptime: 6 minutes, 25 seconds
Prior LSP:
ID: path option 10 [6]
Removal Trigger: configuration changed
R3#
R3#
R3#

```

SHOWS EXPLICITLY DEFINED PATH FOR TRAFFIC FROM R01 FLOWING TOWARDS R12 AND ESTABLISHMENT OF TUNNEL0 AT R03 FOR COMPANY ABC

```

R7#
R7#
R7#
R7#traceroute 9.9.9.9
Type escape sequence to abort.
Tracing the route to 9.9.9.9
VRF info: (vrf in name/id, vrf out name/id)
 0 10.2.7.2 0 msec 0 msec 0 msec
 1 20.2.3.3 [MPLS: Labels 322/10022 Exp 0] 0 msec 0 msec 4 msec
 2 20.3.4.4 [MPLS: Labels 419/10022 Exp 0] 0 msec 0 msec 4 msec
 3 20.4.5.5 [MPLS: Labels 519/10022 Exp 0] 0 msec 0 msec 0 msec
 4 20.5.8.8 [MPLS: Labels 822/10022 Exp 0] 0 msec 0 msec 4 msec
 5 10.9.10.10 [MPLS: Label 10022 Exp 0] 0 msec 0 msec 0 msec
 6 10.9.10.9 4 msec 0 msec *
R7#
R7#
R7#
R7#

```

**TRACEROUTE FOR COMPANY XYZ TRAFFIC
ORIGINATING AT R07**

```

R1#traceroute 12.12.12.12
Type escape sequence to abort.
Tracing the route to 12.12.12.12
VRF info: (vrf in name/id, vrf out name/id)
 0 10.1.3.3 0 msec 0 msec 0 msec
 1 20.3.4.4 [MPLS: Labels 423/11021 Exp 0] 0 msec 4 msec 0 msec
 2 20.4.5.5 [MPLS: Labels 523/11021 Exp 0] 4 msec 0 msec 0 msec
 3 10.11.12.11 [MPLS: Label 11021 Exp 0] 4 msec 0 msec 0 msec
 4 10.11.12.12 4 msec * 0 msec
R1#
R1#
R1#
R1#

```

**TRACEROUTE FOR COMPANY ABC TRAFFIC
ORIGINATING AT R01**

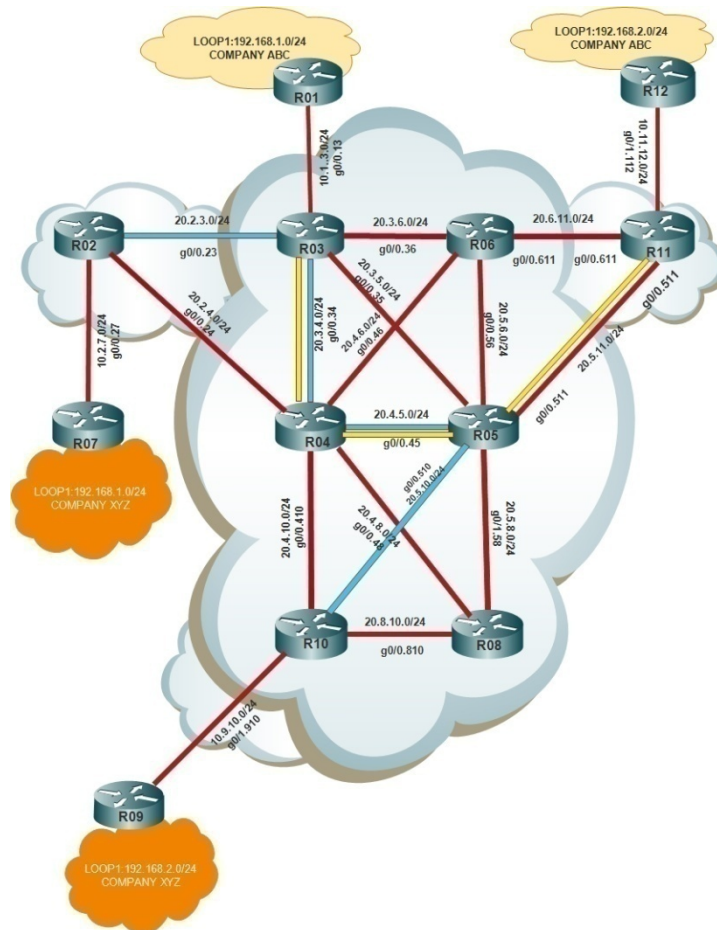
For communication initiated on R09 to customer on R07 path followed is R09-R10-R05-R04-R03-R02-R07.

For communication initiated for customer on R12 TO R01 path followed is R12-R11-R05-R06-R04-R03-R01

TRAFFIC ENGINEERING FOR REVERSE PATH FOR BOTH COMAPNIES ABC AND XYZ TRAFFIC

Traffic Engineering for traffic originating from R09 To R07 for Company XYZ FOLLOWS PATH R09-R10-R05-R04-R03-R02-R07(Path shown in blue)

Traffic Engineering for traffic originating From R12 To R01 for Company ABC follows path R12-R11-R05-R04-R03-R01(Path shown in yellow)



Network diagram 12:shows traffic flowing from R09 and R12 towards R07 AND R01 for companies XYZ(BLUE PATH) AND ABC(YELLOW PATH) Respectively

```

R10#show mpls traffic-eng tunnels tunnel 0
Name: R10_t0 (Tunnel0) Destination: 2.2.2.2
Status:
  Admin: up Oper: up Path: valid Signalling: connected
  path option 10, type explicit TO_R7 (basis for Setup, path weight 40)
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 10 is active
  BandwidthOverride: disabled LockDown: disabled verbatim: disabled

InLabel : -
OutLabel : GigabitEthernet0/0.510, 522
RSVP Signalling Info:
  Src 10.10.10.10, Dst 2.2.2.2, Tun_Id 0, Tun_Instance 7
RSVP Path Info:
  My Address: 20.5.10.10
  Explicit Route: 20.5.10.5 20.4.5.5 20.4.5.4 20.3.4.4
  Record Route: 20.3.4.3 20.2.3.3 20.2.3.2 2.2.2.2
  Record Route: NONE
  TSpec: ave rate=0 kbits, burst=1000 bytes, peak rate=0 kbits
RSVP Resv Info:
  Record Route: 5.5.5.5(522) 4.4.4.4(421)
  3.3.3.3(323) 2.2.2.2(0)
  FSpec: ave rate=0 kbits, burst=1000 bytes, peak rate=0 kbits
Shortest Unconstrained Path Info:
  Path weight: 30 (TE)
  Explicit Route: 20.8.10.10 20.8.10.8 20.4.8.8 20.4.8.4
  20.2.4.4 20.2.4.2 2.2.2.2
History:
Tunnel:
  Time since created: 1 minutes, 28 seconds
  Time since path change: 1 minutes, 28 seconds
  Number of LSP IDs (Tun_Instances) used: 7
Current LSP:
  Uptime: 1 minutes, 28 seconds
Prior LSP:
  ID: path option 10 [6]
  Removal Trigger: configuration changed
R10#

```

SHOWS EXPLICITLY DEFINED PATH FOR TRAFFIC FROM R09 FLOWING TOWARDS R07 AND ESTABLISHMENT OF TUNNEL0 AT R10 FOR COMPANY XYZ

```

R11#show mpls traffic-eng tunnels tunnel 0
Name: R11_t0 (Tunnel0) Destination: 3.3.3.3
Status:
Admin: up Oper: up Path: valid Signalling: connected
path option 10, type explicit TO_R3 (Basis for Setup, path weight 30)

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 10 is active
BandwidthOverride: disabled LockDown: disabled verbatim: disabled

InLabel : -
OutLabel : GigabitEthernet0/0.511, 524
RSVP Signalling Info:
Src 11.11.11.11, Dst 3.3.3.3, Tun_Id 0, Tun_Instance 8
RSVP Path Info:
My Address: 20.5.11.11
Explicit Route: 20.5.11.5 20.4.5.5 20.4.5.4 20.3.4.4
                20.3.4.3 3.3.3.3
Record Route: NONE
Tspec: ave rate=0 kbits, burst=1000 bytes, peak rate=0 kbits
RSVP Resv Info:
Record Route: 5.5.5.5(524) 4.4.4.4(420)
                3.3.3.3(0)
Fspec: ave rate=0 kbits, burst=1000 bytes, peak rate=0 kbits
Shortest Unconstrained Path Info:
Path Weight: 20 (TE)
Explicit Route: 20.5.11.11 20.5.11.5 20.3.5.5 20.3.5.3
                3.3.3.3

History:
Tunnel:
Time since created: 33 seconds
Time since path change: 32 seconds
Number of LSP IDs (Tun_Instances) used: 8
Current LSP:
Uptime: 32 seconds
Prior LSP:
ID: path option 10 [7]
Removal Trigger: configuration changed
R11#
R11#

```

SHOWS EXPLICITEDLY DEFINED PATH FOR TRAFFIC FROM R12 FLOWING TOWARDS R01 AND ESTABLISHMENT OF TUNNEL0 AT R11 FOR COMPANY ABC

```

R12#traceroute 1.1.1.1
Type escape sequence to abort.
Tracing the route to 1.1.1.1
VRF info: (vrf in name/id, vrf out name/id)
 1 10.11.12.11 4 msec 0 msec 0 msec
 2 20.5.11.5 [MPLS: Labels 524/316 Exp 0] 0 msec 4 msec 0 msec
 3 20.4.5.4 [MPLS: Labels 420/316 Exp 0] 0 msec 4 msec 0 msec
 4 10.1.3.3 [MPLS: Label 316 Exp 0] 4 msec 0 msec 0 msec
 5 10.1.3.1 4 msec * 0 msec
R12#
R12#
R12#
R12#
R12#

```

TRACEROUTE FOR COMPANY ABC TRAFFIC ORIGINATING AT R12

```

R9#traceroute 7.7.7.7
Type escape sequence to abort.
Tracing the route to 7.7.7.7
 1 10.9.10.10 0 msec 0 msec 0 msec
 2 20.5.10.5 [MPLS: Labels 515/223 Exp 0] 0 msec 0 msec 0 msec
 3 20.4.5.4 [MPLS: Labels 415/223 Exp 0] 4 msec 0 msec 0 msec
 4 10.2.7.2 [MPLS: Label 223 Exp 0] 4 msec 0 msec 0 msec
 5 10.2.7.7 4 msec 0 msec *
R9#
R9#
R9#

```

TRACEROUTE FOR COMPANY XYZ TRAFFIC ORIGINATING AT R09

Traffic Protection In MPLS Networks

Some services such as VoIP and video streaming do not tolerate data loss or/and delays, but due to the dynamic nature of networks ,network failure is common therefore the traffic on the MPLS enabled networks needs to be protected against network failure. Traffic protection is the fast restoration of the network resources to ensure minimum data loss. Resources can be either logical (LSP) or physical (the nodes or the links). Network failures can occur due to different reasons such as a loosely connected cable, router crashes, power loss, cable or fiber cuts. A network failure can be classified as either a link failure or a node failure.[19]

Before MPLS, a network failure existed but the IGP was the main protocol that the network administrators used to forward packet around the failure to the working part of the network. [19]

Below are some drawbacks of using IGP for Traffic Protection: [29][19]

1. Delay between network resource failure and network re-routing to avoid the failed resources.
2. Network congestion or network blackhole until the new route is created.
3. Data lost during the detection of network failure(This depends on Hello packets timers of IGP Protocols).

In an MPLS network fast restoration of the network resources is used to protect the network from data loss. [19]

To provide a proper high availability network the network provider must predict and plan for network failures in advance.[6]

The key objective of traffic protection are:

1. Failure survival of MPLS network so that disruption to packet flow can be minimized that means established LSPs (which may be carrying data) should not be teared down while the failure is recovered. [6]
2. In voice world 60ms is maximum disruption to VOIP traffic that is undetected by human brain before the network resources failure becomes noticeable, so for voice traffic network failure should be less than 60 ms.
3. The process of repair in one part of the network should cause as little disruption to other parts of the network. Broadcasting failure information as done in IGP Protocols around the network should be avoided as it disrupt flow of data traffic.[6]

All of the solutions to these requirements involve forms of redundancy whether within links, nodes of the networking devices. The cost of these solutions imposes an additional requirement that redundant resources should be kept to a minimum and preferably shared in the network.[6]

Protection can be implemented on RSVP-TE enabled MPLS networks and can be divided into:[19][3]

1. Path Protection (End-to-End protection)
2. Local Protection
 - I. Link protection
 - a) Link protection in facility protection
 - b) Link protection in 1:1 protection
 - II. Node protection
 - a) Node protection in facility protection
 - b) Node protection in 1:1 protection

Path Protection

With MPLS support for Traffic Engineering, it is possible to pre-compute backup LSP(standby path) for the primary LSP. [19]

Path protection provides an end to end failure recovery mechanism , one or more LSPs can be established in advance, which provides failure protection for the protected LSP. [19]

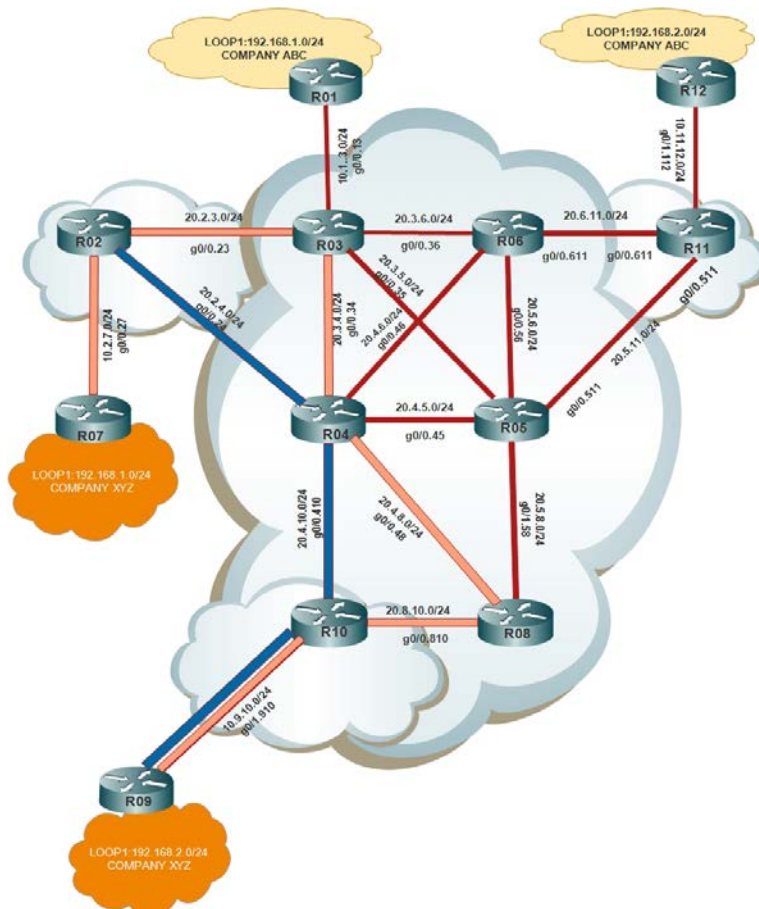
Links should not be shared between the primary and backup LSP since failure to the shared link or node would affect both the LSPs(Shared Risk Link Groups).[19]

Network Diagram 13 below shows an example of a network with a primary and a backup path from R02 to R10.

Path protection is the establishment of an additional LSP in parallel with an existing LSP, where the additional LSP is used only in case of failure. [15]

Both the primary and backup LSPs are configured at the headend. Both are signaled ahead of time in the control plane. When any of the resources in the path of primary LSP breaks ,headend is signaled and pre-computed backup path is used for flow of data.[2]

In the below network diagram 13 for company XYZ path protection is implemented between routers R02 and R10.Path from router R02 to R10 uses PINK path(R02-R03-R04-R08-R10) and in case of failure(standby path) BLUE path is used(R02-R04-R10).All the configuration related to path protection are done at headend R02



NETWORK DIAGRAM 13:PATH PROTECTION

```

File Edit View Options Transfer Script Tools Window Help
Enter host <Alt+R>
MINT R1 MINT R2 x MINT R3 MINT R4 MINT R5 MINT R6 MINT R7
R2#show ip explicit-paths
PATH PATH1_TO_R9 (strict source route, path complete, generation 58)
  1: next-address 2.2.2.2
  2: next-address 20.2.3.3
  3: next-address 3.3.3.3
  4: next-address 20.3.4.4
  5: next-address 4.4.4.4
  6: next-address 20.4.8.8
  7: next-address 8.8.8.8
  8: next-address 20.8.10.10
  9: next-address 10.10.10.10
PATH PATH2_TO_R9 (strict source route, path complete, generation 65)
  1: next-address 2.2.2.2
  2: next-address 20.2.4.4
  3: next-address 4.4.4.4
  4: next-address 20.4.10.10
  5: next-address 10.10.10.10
R2#

```

Explicitly defined path for primary LSP(PATH_TO_R09) and backup LSP(PATH2_TO_R9)

```

File Edit View Options Transfer Script Tools Window Help
Enter host <Alt+R>
MINT R1 MINT R2 x MINT R3 MINT R4 MINT R5 MINT R6 MINT R7 MINT R9 MINT R10 MINT R11
R2#show mpls traffic-eng tunnels tunnel 0
Name: R2_t0 (Tunnel0) Destination: 10.10.10.10
Status:
  Admin: up Oper: up Path: valid Signalling: connected
  path option 10, type explicit PATH1_TO_R9 (Basis for Setup, path weight 40)
  Path Protection: 0 Common Link(s), 1 Common Node(s)
  path protect option 10, type explicit PATH2_TO_R9 (Basis for Protect, path weight 20)
Config Parameters:
  Bandwidth: 0 kbps (Global) Priority: 7 7 Affinity: 0x0/0xFFFF
  Metric Type: TE (default)
  AutoRoute: enabled LockDown: disabled Loadshare: 0 bw-based
  auto-bw: disabled
Active Path Option Parameters:
  State: explicit path option 10 is active
  Bandwidthoverride: disabled Lockdown: disabled verbatim: disabled

InLabel : -
OutLabel : GigabitEthernet0/0.23, 322
RSVP Signalling Info:
  Src 2.2.2.2, Dst 10.10.10.10, Tun_Id 0, Tun_Instance 42
RSVP Path Info:
  My Address: 20.2.3.2
  Explicit Route: 20.2.3.3 20.3.4.3 20.3.4.4 20.4.8.4
                  20.4.8.8 20.8.10.8 20.8.10.10 10.10.10.10
  Record Route: NONE
  Tspec: ave rate=0 kbits, burst=1000 bytes, peak rate=0 kbits
RSVP Resv Info:
  Record Route: 3.3.3.3(322) 4.4.4.4(430)
                  8.8.8.8(822) 10.10.10.10(0)
  Fspec: ave rate=0 kbits, burst=1000 bytes, peak rate=0 kbits
Shortest Unconstrained Path Info:
  Path weight: 20 (TE)
  Explicit Route: 20.2.4.2 20.2.4.4 20.4.10.4 20.4.10.10
                  10.10.10.10
History:
  Tunnel:
    Time since created: 13 minutes, 7 seconds
    Time since path change: 33 seconds
    Number of LSP IDs (Tun_Instances) used: 42
  Current LSP:
    Uptime: 33 seconds
  Prior LSP:
    ID: path option 10 [40]
    Removal Trigger: tunnel shutdown
R2#

```

Before Failure Path1_To_R9 Is Used And Backup Path Is Precomputed(Path2_To_R9)

```

R2#show mpls traffic-eng tunnels tunnel 0
Name: R2_t0 (Tunnel0) Destination: 10.10.10.10
Status:
  Admin: up Oper: up Path: valid Signalling: connected
  path protect option 10, type explicit PATH2_TO_R9 (Basis for Protect, path weight 20)
  path option 10, type explicit PATH1_TO_R9

Config Parameters:
  Bandwidth: 0 kbps (Global) Priority: 7 7 Affinity: 0x0/0xFFFF
  Metric Type: TE (default)
  AutoRoute: enabled LockDown: disabled Loadshare: 0 bw-based
  auto-bw: disabled
Active Path Option Parameters:
  State: explicit path option 10 is active
  BandwidthOverride: disabled LockDown: disabled verbatim: disabled

InLabel : -
OutLabel : GigabitEthernet0/0.24, 429
RSVP Signalling Info:
  Src 2.2.2.2, Dst 10.10.10.10, Tun_Id 0, Tun_Instance 43
RSVP Path Info:
  My Address: 20.2.4.2
  Explicit Route: 20.2.4.4 20.4.10.4 20.4.10.10 10.10.10.10
  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: 20 (TE)
  Explicit Route: 20.2.4.2 20.2.4.4 20.4.10.4 20.4.10.10
                  10.10.10.10

History:
Tunnel:
  Time since created: 18 minutes, 3 seconds
  Time since path change: 4 seconds
  Number of LSP IDs (Tun_Instances) used: 43
Current LSP:
  Uptime: 5 minutes, 29 seconds
  Selection:
Prior LSP:
  ID: path option 10 [42]
  Removal Trigger: path error
R2#

```

WHEN RESOURCES FAIL IN PRIMARY PATH(PATH1_TO_R9) ,TUNNEL USES PRECOMPUTED BACKUP PATH(PATH2_TO_R9)

```

R7#traceroute 9.9.9.9
Type escape sequence to abort.
Tracing the route to 9.9.9.9
VRF info: (vrf in name/id, vrf out name/id)
 1 10.2.7.2 0 msec 0 msec 0 msec
 2 20.2.3.3 [MPLS: Labels 322/10022 Exp 0] 0 msec 0 msec 0 msec
 3 20.3.4.4 [MPLS: Labels 430/10022 Exp 0] 4 msec 0 msec 0 msec
 4 20.4.8.8 [MPLS: Labels 822/10022 Exp 0] 4 msec 0 msec 0 msec
 5 10.9.10.10 [MPLS: Label 10022 Exp 0] 4 msec 0 msec 0 msec
 6 10.9.10.9 4 msec 0 msec *
R7#traceroute 9.9.9.9
Type escape sequence to abort.
Tracing the route to 9.9.9.9
VRF info: (vrf in name/id, vrf out name/id)
 1 10.2.7.2 0 msec 0 msec 0 msec
 2 20.2.4.4 [MPLS: Labels 429/10022 Exp 0] 0 msec 0 msec 0 msec
 3 10.9.10.10 [MPLS: Label 10022 Exp 0] 0 msec 0 msec 0 msec
 4 10.9.10.9 0 msec 0 msec *
R7#

```

TRACEROUTE BEFORE FAILURE OF PRIMARY LSP AND AFTER FAILURE OF PRIMARY LSP

ADVANTAGE OF PATH PROTECTION

1. End to End LSP protection is performed.
2. The backup LSP has the same features such as bandwidth ,QoS as the primary LSP, therefore the network characteristics remain the same, no matter which LSP is in use(primary or backup).[19]

DISADVANTAGE OF PATH PROTECTION

1. Path protection scheme is less scalable as resources are pre-occupied by both primary LSP and backup LSP. In ISP network thousands of LSP's are used for traffic flow, therefore using path protection for each LSP is not feasible.[2]
2. Speed of failure recovery is limited by propagation of error to repair point(In this case router R02),until failure information is being propagated to headend traffic is blackholed.[6]
3. Backup LSP can be configured only at ingress router.
4. Two LSPs are signaled end to end and hence resources are reserved. The backup LSP can't be used to carry traffic(low priority traffic) except during a failure condition so there is wastage of resources.

Local Protection

In local protection only segment of the primary LSP is protected, in case of failure backup LSP is routed around the failed node or link and the primary LSP that could have gone through the failed link or node is encapsulated in the backup LSP. As only a segment of the primary LSP is protected, it is important to protect the most important nodes/links.[3][19]

Advantages of Local protection over Path protection

1. Faster failure recovery ,failure is locally repaired.
2. Scalability
3. The operator can pick which resources and which LSPs to protect ,hence optimal resource utilization.

Disadvantage of Local protection over Path protection:

1. END TO END protection is not available
2. In complex network it is difficult to compute which nodes and links need protection and which don't.

NOTE

FOR FACILITY PROTECTION

TO DEMONSTRATE FACILITY PROTECTION ONLY TRAFFIC FLOWING FROM R02 TO R10 FOR COMPANY XYZ IS **FACILITY** PROTECTED IN ONE DIRECTION.

SIMILARLY, TO DEMONSTRATE FACILITY PROTECTION ONLY TRAFFIC FLOWING FROM R03 TO R11 FOR COMPANY ABC IS **FACILITY** PROTECTED IN ONE DIRECTION.

FOR 1:1 PROTECTION

TO DEMONSTRATE **1:1** PROTECTION ONLY TRAFFIC FLOWING FROM R10 TO R02 FOR COMPANY XYZ IS **1:1** PROTECTED IN ONE DIRECTION.

SIMILARLY, TO DEMONSTRATE **1:1** PROTECTION ONLY TRAFFIC FLOWING FROM R11 TO R01 FOR COMPANY ABC IS **1:1** PROTECTED IN ONE DIRECTION.

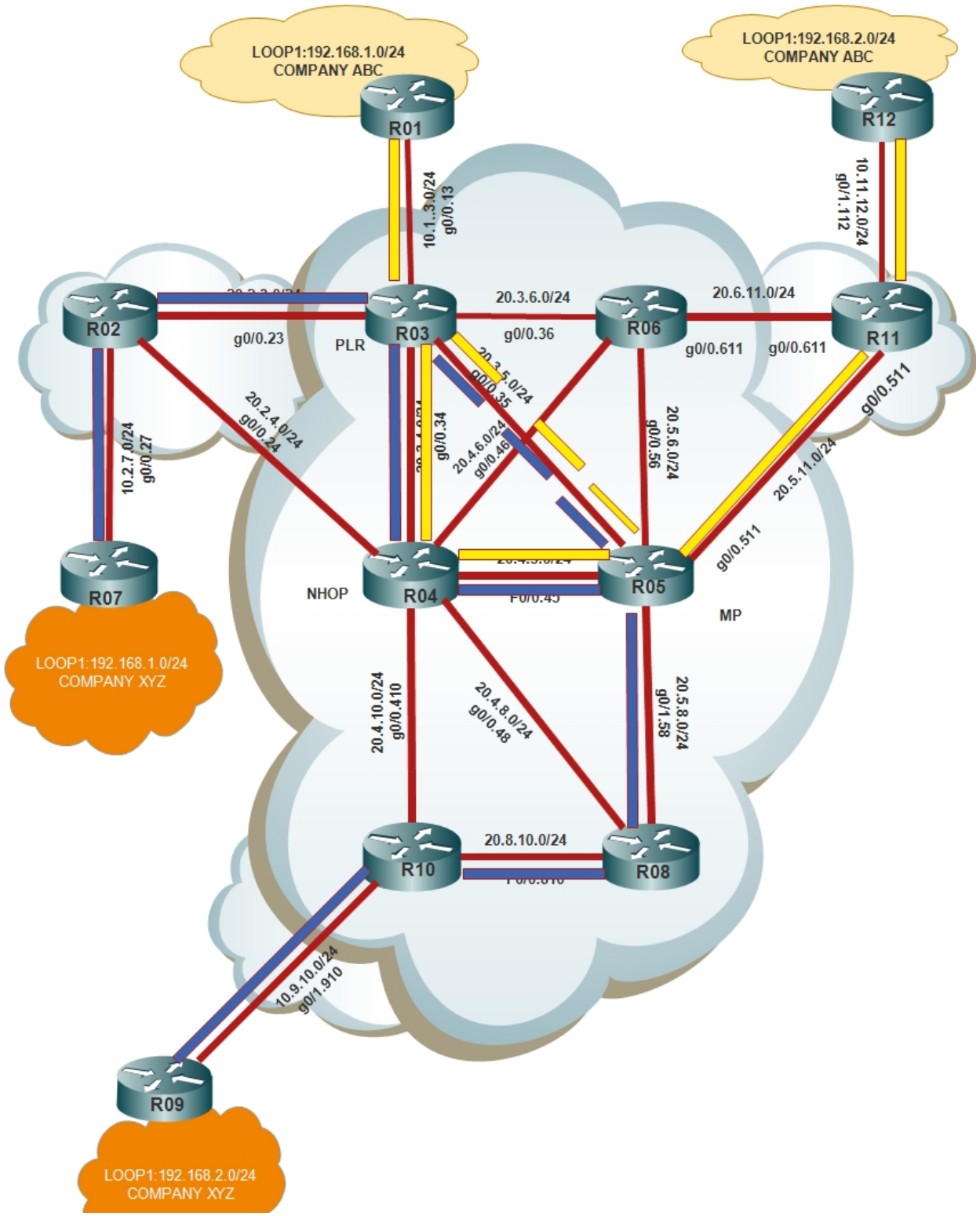
TERMINOLOGIES COMMON IN LOCAL PROTECTION:

PLR (Point of Local Repair) is where the backup starts, also known as the head end. In network diagram R03 is the Point of Local Repair.[19][2]

MP (**Merge Point**) is the point where the backup path ends and connects back to the network which was part of the primary path. In network diagram R05 is the MP.[19][2]

NHop (**Next-hop**) is a router one hop away from the PLR. In network diagram R04 is the NHop on the primary path.[19][2]

NNHop (**Next-next-hop**) is a router two hops away from the PLR. In network diagram R5 is the NNHop on the primary path.[19][2]



NETWORK DIAGRAM 14: ELEMENTS OF A LOCAL PROTECTION

Protection Schemes In Local Protection

Different protection schemes are:

N:1 (N > 1) protection

N:1 protection (many-to-one protection or facility protection) is a protection technique in which N primary LSPs are protected by single backup LSP. High priority traffic is sent through the primary LSPs, low priority traffic can be sent through the backup LSP. In case any of the N LSPs fails, the traffic will be rerouted to the backup LSP. [2]

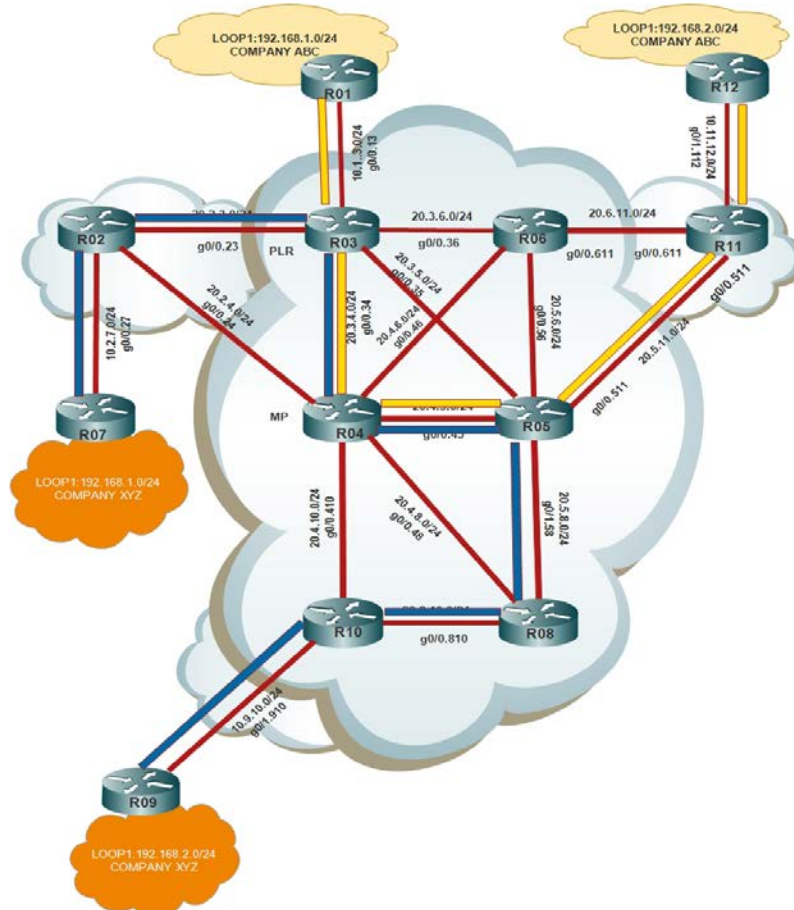
Link Protection

In Local protection link protection is of two types:

1. Link Protection In Facility Protection
2. Link Protection In 1:1 protection

Link Protection In Facility Protection

In link protection using facility protection case, the protection path created by a PLR is known as a bypass tunnel. The bypass tunnel shown in the network diagram is shared by 2 LSPs when the link between R3 and R4 fails. R3 must set up the bypass tunnel such that the MP is R04, the router immediately downstream of the link failure, this is usually the 'next-hop' node of the LSPs normally passing through R03(which avoids link between R03 and R04)[2]



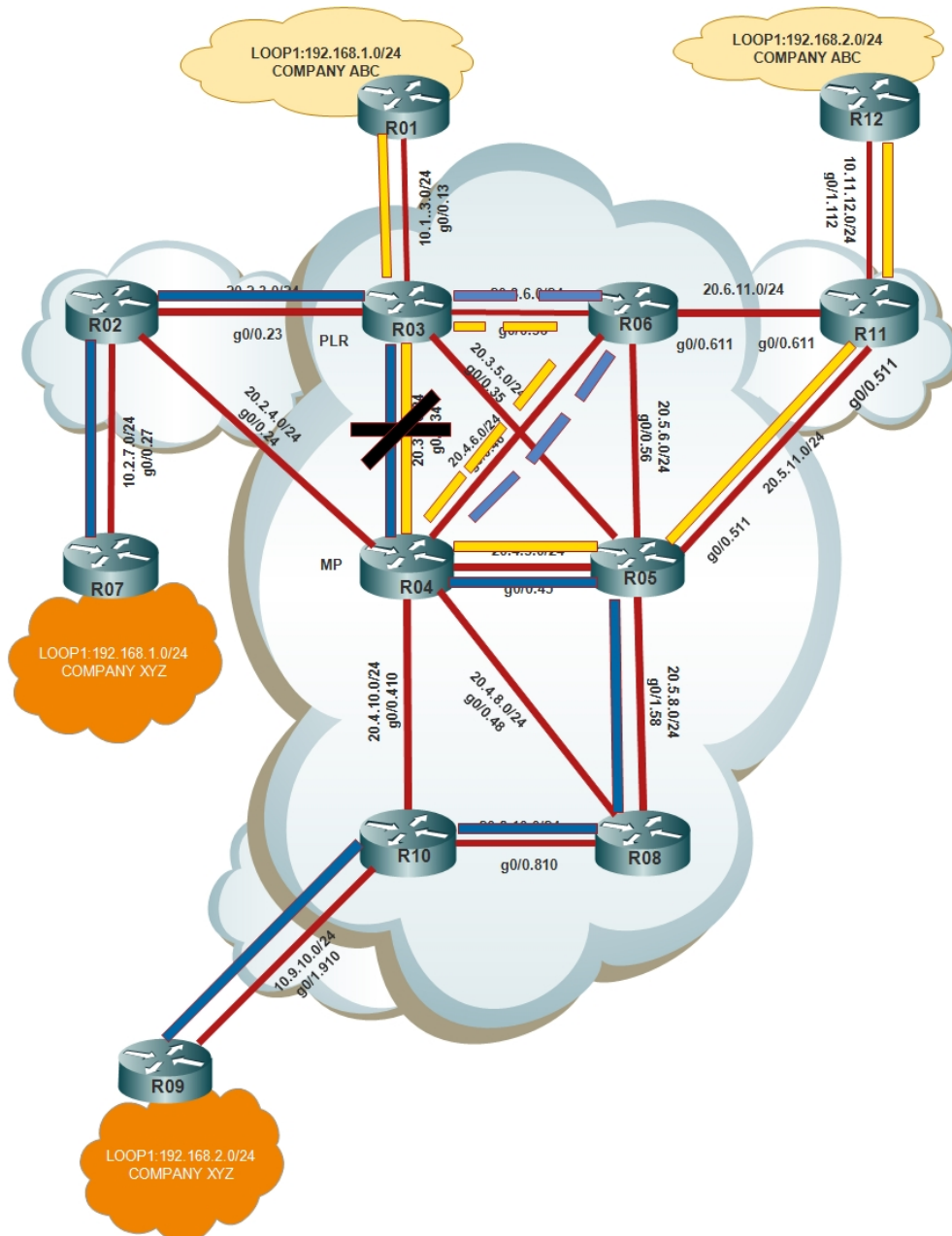
Network Diagram 15:For Local Protection Before Failure

towards R04, as R04 is a router in the topology that is guaranteed to lie along the main path of all the LSPs being protected. For a period of time that the bypass tunnel is in use, the overall path taken by some of the traffic from the PLR to the egress node of the LSP may not be optimal. [2]

For example, traffic using LSP (R02--R10) follows the path

R02, R03, R06, R04, R05, R08, R10 because of the nature of this variant of protection means the traffic must pass through R04.

Traffic using LSP (R03--R11) follows the path R03, R06, R04, R05, R11



NETWORK DIAGRAM 16: Link Protection For Facility Protection Case


```

File Edit View Options Transfer Script Tools Window Help
Enter host <Alt+R>
MINT R1 | MINT R2 | MINT R3 x | MINT R4 | MINT R5 | MINT R6 | MINT R7 | MINT R9 | MINT R10
R3#show mpls traffic-eng tunnels tunnel 1
Name: R3_t1 (Tunnel1) Destination: 4.4.4.4
Status:
  Admin: up oper: up Path: valid Signalling: connected
  path option 10, type explicit LINK_FACILITY (Basis for Setup, path weight 20)

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 10 is active
  BandwidthOverride: disabled LockDown: disabled Verbatim: disabled

InLabel : -
OutLabel : GigabitEthernet0/0.36, 618
RSVP Signalling Info:
  Src 3.3.3.3, Dst 4.4.4.4, Tun_Id 1, Tun_Instance 3
RSVP Path Info:
  My Address: 20.3.6.3
  Explicit Route: 20.3.6.6 20.4.6.6 20.4.6.4 4.4.4.4
  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: 20.3.4.3 20.3.4.4 4.4.4.4
History:
  Tunnel:
    Time since created: 1 minutes, 42 seconds
    Time since path change: 1 minutes, 41 seconds
    Number of LSP IDs (Tun_Instances) used: 3
  Current LSP:
    Uptime: 1 minutes, 41 seconds
  Prior LSP:
    ID: path option 10 [2]
    Removal Trigger: configuration changed
R3#

```

TUNNEL 1 CREATED AT ROUTER R03 TO R04 AVOIDING LINK BETWEEN R03 TO R04

```

File Edit View Options Transfer Script Tools Window Help
Enter host <Alt+R>
MINT R1 | MINT R2 | MINT R3 x | MINT R4 | MINT R5 | MINT R6 | MINT R7 | MINT R9
R3#show mpls traffic-eng tunnels tunnel 0
Name: R3_t0 (Tunnel0) Destination: 11.11.11.11
Status:
  Admin: up oper: up Path: valid Signalling: connected
  path option 10, type explicit TO_R11 (Basis for Setup, path weight 30)

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 10 is active
  BandwidthOverride: disabled LockDown: disabled Verbatim: disabled

InLabel : -
OutLabel : GigabitEthernet0/0.34, 420
FRR OutLabel : Tunnel1, 420
RSVP Signalling Info:
  Src 3.3.3.3, Dst 11.11.11.11, Tun_Id 0, Tun_Instance 6
RSVP Path Info:
  My Address: 20.3.4.3
  Explicit Route: 20.3.4.4 20.4.5.4 20.4.5.5 20.5.11.5
                  20.5.11.11 11.11.11.11
  Record Route: NONE
  Tspec: ave rate=0 kbits, burst=1000 bytes, peak rate=0 kbits
RSVP Resv Info:
  Record Route: 4.4.4.4(420) 5.5.5.5(518)
                  11.11.11.11(0)
  Fspec: ave rate=0 kbits, burst=1000 bytes, peak rate=0 kbits
Shortest Unconstrained Path Info:
  Path weight: 20 (TE)
  Explicit Route: 20.3.5.3 20.3.5.5 20.5.11.5 20.5.11.11
                  11.11.11.11
History:
  Tunnel:
    Time since created: 3 minutes, 53 seconds
    Time since path change: 3 minutes, 52 seconds
    Number of LSP IDs (Tun_Instances) used: 6
  Current LSP:
    Uptime: 3 minutes, 52 seconds
    Selection: reoptimization
  Prior LSP:
    ID: path option 10 [5]
    Removal Trigger: configuration changed
R3#

```

TUNNEL0 AT R03 FOR COMPANY ABC FOR TRAFFIC ENGINEERING

```

File Edit View Options Transfer Script Tools Window Help
Enter host <Alt+R>
MINT R1 MINT R2 x MINT R3 MINT R4 MINT R5 MINT R6 MINT R7 MINT R9
R2#show mpls traffic-eng tunnels tunnel 0
Name: R2_t0 (Tunnel0) Destination: 10.10.10.10
Status:
Admin: up Oper: up Path: valid Signalling: connected
path option 10, type explicit TO_R9 (Basis for setup, path weight 50)
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 10 is active
BandwidthOverride: disabled LockDown: disabled Verbatim: disabled
InLabel : -
OutLabel : GigabitEthernet0/0.23, 326
RSVP Signalling Info:
Src 2.2.2.2, Dst 10.10.10.10, Tun_Id 0, Tun_Instance 12
RSVP Path Info:
My Address: 20.2.3.2
Explicit Route: 20.2.3.3 20.3.4.3 20.3.4.4 20.4.5.4
20.4.5.5 20.5.8.5 20.5.8.8 20.8.10.8
20.8.10.10 10.10.10.10
Record Route: NONE
Tspec: ave rate=0 kbits, burst=1000 bytes, peak rate=0 kbits
RSVP Resv Info:
Record Route: 3.3.3.3(326) 4.4.4.4(426)
5.5.5.5(523) 8.8.8.8(825)
10.10.10.10(0)
Fspec: ave rate=0 kbits, burst=1000 bytes, peak rate=0 kbits
Shortest Unconstrained Path Info:
Path weight: 20 (TE)
Explicit Route: 20.2.4.2 20.2.4.4 20.4.10.4 20.4.10.10
10.10.10.10
History:
Tunnel:
Time since created: 5 minutes, 32 seconds
Time since path change: 5 minutes, 21 seconds
Number of LSP IDs (Tun_Instances) used: 12
Current LSP:
Uptime: 3 minutes, 36 seconds
R2#
R2#
R2#

```

TUNNEL0 AT R02 FOR COMPANY XYZ FOR TRAFFIC ENGINEERING

```

File Edit View Options Transfer Script Tools Window Help
Enter host <Alt+R>
MINT R1 MINT R2 MINT R3 x MINT R4 MINT R5 MINT R6 MINT R7 MINT R9 MINT
R3#show mpls traffic-eng tunnels tunnel 0
Name: R3_t0 (Tunnel0) Destination: 11.11.11.11
Status:
Admin: up Oper: up Path: valid Signalling: connected
path option 10, type explicit TO_R11 (Basis for setup, path weight 0)
change in required resources detected: reroute pending
currently Signalled Parameters:
Bandwidth: 0 kbps (Global) Priority: 7 7 Affinity: 0x0/0xFFFF
Metric Type: TE (default)
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 10 is active
BandwidthOverride: disabled LockDown: disabled Verbatim: disabled
InLabel : -
OutLabel : GigabitEthernet0/0.34, 420
FRR OutLabel : Tunnel11, 420 (in use)
RSVP Signalling Info:
Src 3.3.3.3, Dst 11.11.11.11, Tun_Id 0, Tun_Instance 6
RSVP Path Info:
My Address: 20.3.4.3
Explicit Route: 4.4.4.4 20.4.5.4 20.4.5.5 20.5.11.5
20.5.11.11 11.11.11.11
Record Route: NONE
Tspec: ave rate=0 kbits, burst=1000 bytes, peak rate=0 kbits
RSVP Resv Info:
Record Route: 4.4.4.4(420) 5.5.5.5(518)
11.11.11.11(0)
Fspec: ave rate=0 kbits, burst=1000 bytes, peak rate=0 kbits
Shortest Unconstrained Path Info:
Path weight: 20 (TE)
Explicit Route: 20.3.5.3 20.3.5.5 20.5.11.5 20.5.11.11
11.11.11.11
History:
Tunnel:
Time since created: 6 minutes, 24 seconds
Time since path change: 6 minutes, 23 seconds
Number of LSP IDs (Tun_Instances) used: 6
Current LSP:
Uptime: 6 minutes, 23 seconds
Selection: reoptimization
Last Error: PCALC:: Explicit path has unknown address, 20.3.4.3
Prior LSP:
ID: path option 10 [5]
Removal Trigger: configuration changed
Last Error: PCALC:: Explicit path has unknown address, 20.3.4.3

```

AFTER FAILURE OF LINK BETWEEN R03 AND R04 LSP FOR COMPANY ABC IS NOT TEARED DOWN AND LINK PROTECTION(TUNNEL 1) AT R03 TO R04 IS BEING USED

```

R2#show mpls traffic-eng tunnels tunnel 0
Name: R2_t0 (Tunnel0) Destination: 10.10.10.10
Status:
  Admin: up Oper: up Path: valid Signalling: connected
  path option 10, type explicit TO_R9 (Basis for Setup, path weight 10)
  change in required resources detected: reroute pending
  Currently Signalled Parameters:
    Bandwidth: 0 kbps (Global) Priority: 7 7 Affinity: 0x0/0xFFFF
    Metric Type: TE (default)

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 10 is active
  BandwidthOverride: disabled Lockdown: disabled verbatim: disabled

InLabel : -
OutLabel : GigabitEthernet0/0.23, 326
RSVP Signalling Info:
  Src 2.2.2.2, Dst 10.10.10.10, Tun_Id 0, Tun_Instance 12
RSVP Path Info:
  My Address: 20.2.3.2
  Explicit Route: 20.2.3.3 20.3.4.3 20.3.4.4 20.4.5.4
                  20.4.5.5 20.5.8.5 20.5.8.8 20.8.10.8
                  20.8.10.10 10.10.10.10
  Record Route: NONE
  Tspec: ave rate=0 kbits, burst=1000 bytes, peak rate=0 kbits
RSVP Resv Info:
  Record Route: 3.3.3.3(326) 4.4.4.4(426)
                  5.5.5.5(523) 8.8.8.8(825)
                  10.10.10.10(0)
  Fspec: ave rate=0 kbits, burst=1000 bytes, peak rate=0 kbits
Shortest Unconstrained Path Info:
  Path weight: 20 (TE)
  Explicit Route: 20.2.4.2 20.2.4.4 20.4.10.4 20.4.10.10
                  10.10.10.10

History:
Tunnel:
  Time since created: 7 minutes, 1 seconds
  Time since path change: 6 minutes, 50 seconds
  Number of LSP IDs (Tun_Instances) used: 12
Current LSP:
  Uptime: 15 seconds
  Last Error: PCALC:: Explicit path has unknown address, 20.3.4.3
R2#
R2#
R2#

```

AFTER FAILURE OF LINK BETWEEN R03 AND R04 LSP FOR COMPANY XYZ IS NOT TEARED DOWN AND LINK PROTECTION(TUNNEL 1) AT R03 TO R04 IS BEING USED

```

R3#show mpls traffic-eng fast-reroute database
Headend frr information:
Protected tunnel          In-label  Out intf/label  FRR intf/label  Status
Tunnel0                  Tun hd    Gi0/0.34:427   Tu1:427         ready

LSP midpoint frr information:
LSP identifier           In-label  Out intf/label  FRR intf/label  Status
2.2.2.2 0 [24]          322      Gi0/0.34:428   Tu1:428         ready
R3#
R3#
R3#
R3#

```

BACKUP TUNNEL1 IS PRECOMPUTED AT R03 AND IN READY STATE

```

R3#show mpls traffic-eng fast-reroute database
Headend frr information:
Protected tunnel          In-label  Out intf/label  FRR intf/label  Status
Tunnel0                  Tun hd    Gi0/0.34:427   Tu1:427         active

LSP midpoint frr information:
LSP identifier           In-label  Out intf/label  FRR intf/label  Status
2.2.2.2 0 [24]          322      Gi0/0.34:428   Tu1:428         active
R3#

```

PRECOMPUTED BACKUP TUNNEL 1 IN ACTIVE STATE WHEN LINK BETWEEN R03 AND R04 FAILS

```

File Edit View Options Transfer Script Tools Window Help
Enter host <Alt+R>
MINT R1 x MINT R2 MINT R3 MINT R4 MINT R5 MINT R6 MINT R7
R1#traceroute 12.12.12.12
Type escape sequence to abort.
Tracing the route to 12.12.12.12
VRF info: (vrf in name/id, vrf out name/id)
 1 10.1.3.3 0 msec 0 msec 0 msec
 2 20.3.4.4 [MPLS: Labels 427/11021 Exp 0] 0 msec 0 msec 4 msec
 3 20.4.5.5 [MPLS: Labels 521/11021 Exp 0] 0 msec 0 msec 4 msec
 4 10.11.12.11 [MPLS: Label 11021 Exp 0] 0 msec 0 msec 4 msec
 5 10.11.12.12 0 msec * 0 msec
R1#traceroute 12.12.12.12
Type escape sequence to abort.
Tracing the route to 12.12.12.12
VRF info: (vrf in name/id, vrf out name/id)
 1 10.1.3.3 0 msec 0 msec 4 msec
 2 20.3.6.6 [MPLS: Labels 618/427/11021 Exp 0] 0 msec 0 msec 4 msec
 3 20.4.6.4 [MPLS: Labels 427/11021 Exp 0] 0 msec 0 msec 4 msec
 4 20.4.5.5 [MPLS: Labels 521/11021 Exp 0] 0 msec 0 msec 4 msec
 5 10.11.12.11 [MPLS: Label 11021 Exp 0] 0 msec 0 msec 4 msec
 6 10.11.12.12 0 msec * 0 msec
R1#
R1#
R1#

```

TRACEROUTE FOR COMPANY ABC BEFORE FAILURE AND AFTER FAILURE OF LINK BETWEEN R03 AND R04

```

File Edit View Options Transfer Script Tools Window Help
Enter host <Alt+R>
MINT R1 MINT R2 MINT R3 MINT R4 MINT R5 MINT R6 MINT R7 x
R7#traceroute 9.9.9.9
Type escape sequence to abort.
Tracing the route to 9.9.9.9
VRF info: (vrf in name/id, vrf out name/id)
 1 10.2.7.2 0 msec 0 msec 0 msec
 2 20.2.3.3 [MPLS: Labels 322/10022 Exp 0] 0 msec 0 msec 0 msec
 3 20.3.4.4 [MPLS: Labels 428/10022 Exp 0] 4 msec 0 msec 0 msec
 4 20.4.5.5 [MPLS: Labels 526/10022 Exp 0] 4 msec 0 msec 0 msec
 5 20.5.8.8 [MPLS: Labels 819/10022 Exp 0] 4 msec 0 msec 0 msec
 6 10.9.10.10 [MPLS: Label 10022 Exp 0] 4 msec 0 msec 0 msec
 7 10.9.10.9 4 msec 0 msec *
R7#traceroute 9.9.9.9
Type escape sequence to abort.
Tracing the route to 9.9.9.9
VRF info: (vrf in name/id, vrf out name/id)
 1 10.2.7.2 0 msec 0 msec 0 msec
 2 20.2.3.3 [MPLS: Labels 322/10022 Exp 0] 0 msec 0 msec 0 msec
 3 20.3.6.6 [MPLS: Labels 618/428/10022 Exp 0] 4 msec 0 msec 0 msec
 4 20.4.6.4 [MPLS: Labels 428/10022 Exp 0] 4 msec 0 msec 0 msec
 5 20.4.5.5 [MPLS: Labels 526/10022 Exp 0] 4 msec 0 msec 0 msec
 6 20.5.8.8 [MPLS: Labels 819/10022 Exp 0] 4 msec 0 msec 0 msec
 7 10.9.10.10 [MPLS: Label 10022 Exp 0] 4 msec 0 msec 0 msec
 8 10.9.10.9 4 msec 0 msec *
R7#
R7#
R7#
R7#

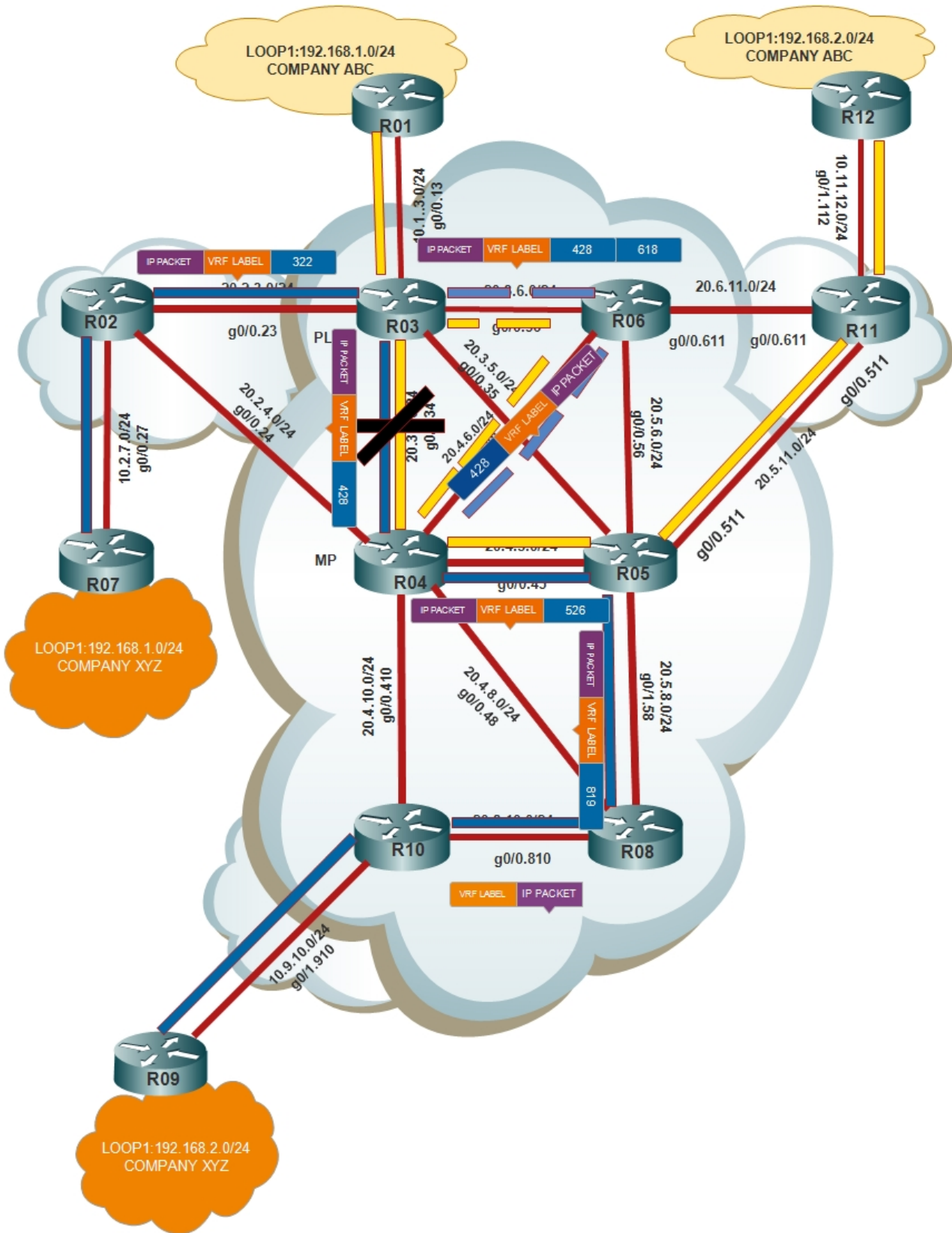
```

TRACEROUTE FOR COMPANY XYZ BEFORE FAILURE AND AFTER FAILURE OF LINK BETWEEN R03 AND R04

Traffic arrives over the backup tunnel with the same label as it would if it arrived over the failed link. The traffic arrives at the MP over different interfaces when arriving over the backup. To ensure that traffic arrives at the MP with the same label as it would have arrived before the failure, packet is tunnel into the backup by pushing the backup tunnel label on top of the protected LSP label at the PLR (label stacking) and do penultimate hop-popping for the backup tunnel label before the MP. [2]

Features of link protection in facility protection

1. No new forwarding state is installed at the MP. At the PLR, the forwarding state must be set in place to push the label of the backup path (label 618 in the example) on to the labeled traffic from the protected LSP in the event of a failure.[2]
2. Any number of LSPs crossing link R03-R04 can be protected by the backup shown in the network diagram. [2]
3. LSP protected at the MP and the action taken by the PLR is always the same: push the backup tunnel label on to the label stack of the main LSP. [2]
4. The label that is advertised by the MP is an implicit null label and therefore penultimate hop popping is performed for the backup tunnel. Thus, traffic arrives at the MP with the same label with which it would have arrived over the main LSP.[2]



NETWORK DIAGRAM 17:SHOWS PACKET FLOW IN LINK PROTECTION IN FACILITY PROTECTION CASE WHEN LINK BETWEEN R03 AND R04 BREAKS

ADVANTAGE:

1. Rapid repair as soon as error is detected(failure is locally repaired)
2. Any Resource can be selectively chosen to protect; drawbacks of end to end protection can be avoided
3. The ability for several LSPs to share the same protection path is an important scaling property of facility backup.[2]
4. Advantage of link protection in facility protection case over Path protection is that Network resources such as bandwidth are properly utilized since the backup LSP is shared by many primary LSPs and it can still be used to transmit other data when the network is working normally.[2]

DISADVANTAGE:

1. Link backup pre- allocated. Need a backup for each protected link(MANUAL CONFIGURATION)[6]
2. Label distribution is limited to the global label space.
3. Data path extended by length of backup tunnel.[6]
4. Label stacking is done to forward the primary traffic over the backup path hence the depth of the label stack increases when traffic is forwarded over the backup tunnel.[2]
5. The period of time that the bypass tunnel is in use, the overall path taken by some of the traffic from the PLR to the egress node of the LSP may not be optimal.[2]
6. If more than one LSP fails, backup tunnel will support limited number of traffic depending on available resources and traffic from the other LSP will be dropped. [19][2]

QUALITATIVE ANALYSIS OF LOCAL PROTECTION ON CISCO ROUTERS(4. reference Advanced MPLS Design and Implementation Cisco

Press)

1. Pre-failure configuration
2. Failure detection
3. Connectivity restoration
4. Post-failure signaling

Pre-failure Configuration[4]

Enabling Link Protection on a Tunnel Interface

tunnel mpls traffic-eng fast-reroute configuration under the primary tunnel interface at the headend

```
MINT R1 | ✓ MINT R2 x | ✓ MINT R3 | ⓘ MINT R4 | ✓ MINT R5 | ⓘ MINT R6 | ⓘ M
R2#show running-config interface tunnel 0
Building configuration...

Current configuration : 230 bytes
!
interface Tunnel0
 ip unnumbered Loopback0
 tunnel mode mpls traffic-eng
 tunnel destination 10.10.10.10
 tunnel mpls traffic-eng path-option 10 explicit name TO_R9
 tunnel mpls traffic-eng fast-reroute
 no routing dynamic
end
```

After **tunnel mpls traffic-eng fast-reroute** is configured, three flags are set

Flag

Local Prot desired: This is how the headend indicates to any downstream nodes that it would like local protection of some sort (either link or node) for this LSP.[4]

Label Recording: Not used in link protection, it is used in node protection as labels to next-next hop are required for protection in node protection case.[4]

SE Style: Stays the same as before **tunnel mpls traffic-eng fast-reroute** was configured.[4]

Enabling Link Protection at the PLR[4]

Enabling FRR at the PLR involves two things:[4]

- Creating a backup tunnel to the NHop

```
File Edit View Options Transfer Script Tools Window Help
Enter host <Alt+R>
MINT R1 | ✓ MINT R2 | ✓ MINT R3 x | ⓘ MINT R4 | ✓ MINT R5 | ⓘ MINT R6 | ⓘ MINT R7
R3#show running-config interface tunnel 1
Building configuration...

Current configuration : 196 bytes
!
interface Tunnel1
 ip unnumbered Loopback0
 tunnel mode mpls traffic-eng
 tunnel destination 4.4.4.4
 tunnel mpls traffic-eng path-option 10 explicit name LINK_FACILITY
 no routing dynamic
end
```

- Configuring the protected link to use the backup tunnel upon failure


```
R3#show running-config interface g0/0.34
Building configuration...

Current configuration : 239 bytes
!
interface GigabitEthernet0/0.34
 encapsulation dot1Q 34
 ip address 20.3.4.3 255.255.255.0
 ip router isis 1
 mpls traffic-eng tunnels
 mpls traffic-eng backup-path Tunnel1
 bfd interval 60 min_rx 60 multiplier 4
 ip rsvp bandwidth
end
```

Creating a Backup Tunnel to the NHop

In local protection, a backup tunnel needs to be built from the PLR to the MP. In link protection, the MP is the node on the other end of the protected link. The primary LSP goes from R03-R04-R05.[4]

Link to be protected is between routers R03 and R04[4]

```
R3#show ip explicit-paths name LINK_FACILITY
PATH LINK_FACILITY (strict source route, path complete, generation 25)
 1: next-address 20.3.6.3
 2: next-address 20.4.6.6
R3#show running-config interface tunnel 1
Building configuration...

Current configuration : 196 bytes
!
interface Tunnel1
 ip unnumbered Loopback0
 tunnel mode mpls traffic-eng
 tunnel destination 4.4.4.4
 tunnel mpls traffic-eng path-option 10 explicit name LINK_FACILITY
 no routing dynamic
end
R3#
```

Failure Detection[4]

Failure detection is very important because the longer it takes to detect a failure, the longer it takes to kick in the protection mechanism designed to circumvent that failure.[4]

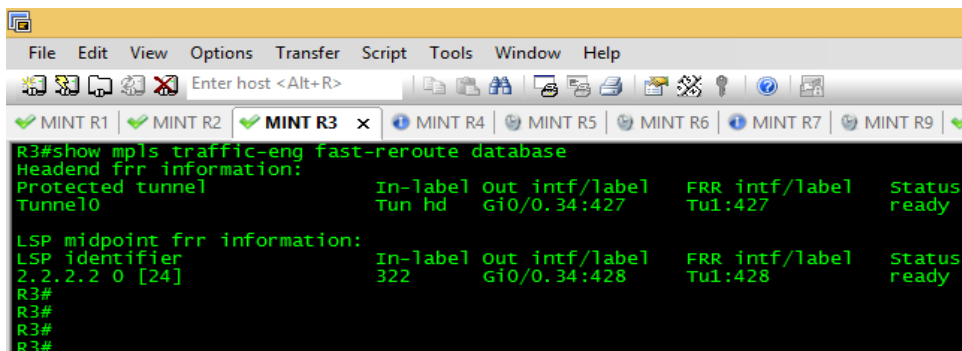
RSVP hellos and BFD can be used for failure detection.[4]

Connectivity Restoration[4]

PLR is responsible for switching traffic to the backup tunnel. The internal processing performed on the PLR involves the following:[4]

Making sure a pre-sigaled backup LSP is in place. This includes the new label provided by a new downstream neighbor.[4]

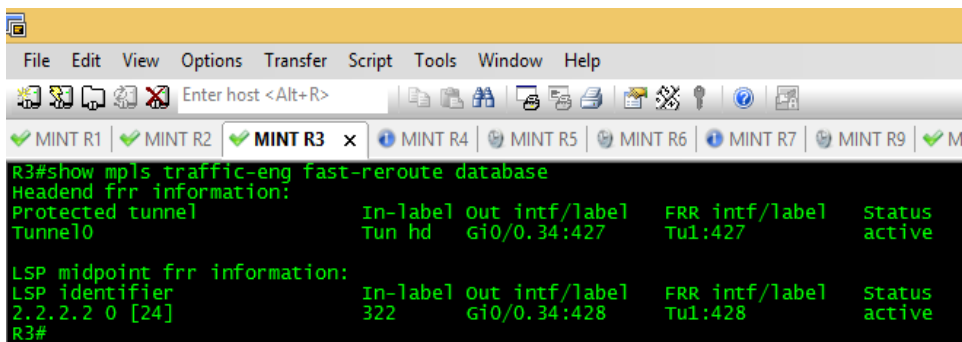
New adjacency information (Layer 2 encapsulation) is computed based on the backup tunnel's outgoing physical interface. This information is pre-computed and ready to be installed in the FIB/LFIB as soon as the failure is detected this is referred to as the ready state. After the failure is detected, FRR is in active state[4]



```
R3#show mpls traffic-eng fast-reroute database
Headend frr information:
Protected tunnel          In-label  Out intf/label  FRR intf/label  Status
Tunnel0                  Tun hd    Gi0/0.34:427   Tu1:427         ready

LSP midpoint frr information:
LSP identifier          In-label  Out intf/label  FRR intf/label  Status
2.2.2.2 0 [24]         322      Gi0/0.34:428   Tu1:428         ready
R3#
R3#
R3#
R3#
```

BACKUP TUNNEL1 IS PRECOMPUTED AT R03 AND IN READY STATE



```
R3#show mpls traffic-eng fast-reroute database
Headend frr information:
Protected tunnel          In-label  Out intf/label  FRR intf/label  Status
Tunnel0                  Tun hd    Gi0/0.34:427   Tu1:427         active

LSP midpoint frr information:
LSP identifier          In-label  Out intf/label  FRR intf/label  Status
2.2.2.2 0 [24]         322      Gi0/0.34:428   Tu1:428         active
R3#
```

PRECOMPUTED BACKUP TUNNEL 1 IN ACTIVE STATE WHEN LINK BETWEEN R03 AND R04 FAILS

while the protection is active and the backup tunnel is forwarding traffic, the primary LSP continues to stay up.

Post-Failure Signaling[4]

RSVP signaling that happens after FRR protection in place includes:

1. Upstream signaling
2. IGP notification
3. Downstream signaling

Upstream Signaling[4]

When a link goes down along an LSP, the node that is upstream of the failed link signals a path error to the headends of the LSPs traversing the failed link after the link between R03 and R04 fails, R03 sends a PathErr message to TUNNEL 0 at R02 and R03, which is the headend of the primary tunnel for company XYZ and ABC respectively.[4]

According to RFC 3209 when fast reroute is enabled PathErr will be send with ERROR_SPEC containing error code 25, "Notification," and a subcode of 3, "Tunnel locally repaired." to the headend of tunnel.[4]

When an LSP headend receives such a message, it knows that it does not need to immediately stop using its primary LSP, just that this LSP might be following a suboptimal path until it can be rerouted. The headend is free to reroute the LSP when it computes the more optimal path.[4]

When a protected link fails and is switched down the backup tunnel, the PLR also sends Path messages for the protected LSPs down the backup tunnel. This is so that the MP doesn't time out the protected tunnel, in the unlikely event that the protected tunnel headend can't reroute the LSP.[4]

In order to keep sessions alive, RSVP refresh messages are sent periodically. These refresh messages are sent between RSVP neighbors by sending Path and Resv messages. LSP tunnels are identified by a combination of the SESSION and SENDER_TEMPLATE objects in these Path and Resv messages SENDER_TEMPLATE object is modified by the PLR so that the sender IPv4 address now contains the PLR's IP address rather than that of the headend. Doing so allows the tail to see this Path message as coming from a new sender but still belonging to the same session.[4]

Now, the refresh messages can flow over the backup tunnel. The original state maintained by the tail for this session is eventually torn down because of timeout (by any LSR downstream of the failed link, including the tail), but the altered Path message from the PLR is enough to effectively maintain the bandwidth reservation for as long as necessary. [4]

Related to the refresh messages is the fact that Path messages would have to be forwarded down the backup tunnel by the PLR. But if the PLR did so using the contents of the ERO, as it would normally do, it would fail because the next IP address in the ERO would point to the failed link. This behavior has to change to make FRR work. In addition to the ERO, the RRO and phop objects are modified for refresh messages flowing over the backup tunnel according to the IETF draft.[4]

IGP Notification[4]

Although in many cases, RSVP messages reach either the headend or tailend ahead of any IGP notification, this is not guaranteed to be the case. When IGP information (such as OSPF/IS-IS LSA declaring a link down) for some reason makes it before the RSVP message on the head end, the headend

tears down the primary tunnel. After that, the headend can, if configured correctly, attempt to reroute the LSP.[4]

If the primary tunnel is configured for FRR, the link-down LSA has no effect. The headend tears down a protected LSP based only on RSVP error messages and ignores IGP's reporting a link down along the LSP. [4]

Downstream Signaling[4]

When the link between R03 and R04 goes down (when no local protection is in place), R04 sends a PathTear message to R10. In FRR the PathTear message needs to be suppressed for primary LSPs that have the "Local Protection Desired" flag on, in spite of the fact that you don't receive Path messages for the protected primary tunnel on the original incoming interface anymore. As long as R04 receives Path messages belonging to the original RSVP session on any interface, it does not time out and sends a PathTear on its downstream interface.[4]

As the tail of the primary tunnel, R10 does not know that the protected tunnel has failed unless one of the following things happens:[4]

1. It receives an IGP update about the link failure.
2. It receives a PathTear from R04.
3. It does not receive an RSVP refresh message (Path) that keeps the session alive within a certain period of time.
4. If the tail receives an IGP update about the link failure, it does not take any action from an MPLS TE perspective.

If the RSVP signaling state times out, the LSP is declared dead, and a ResvTear message is sent to the headend. This means that, apart from preventing PathTear from being sent by MP R04, you somehow need to make sure that the tail continues to receive the RSVP refresh messages even though one of the links that constituted the primary LSP is now down. This is achieved by making sure that the MP (R04) continues to receive PATH messages for the primary LSP over the backup tunnel.[4]

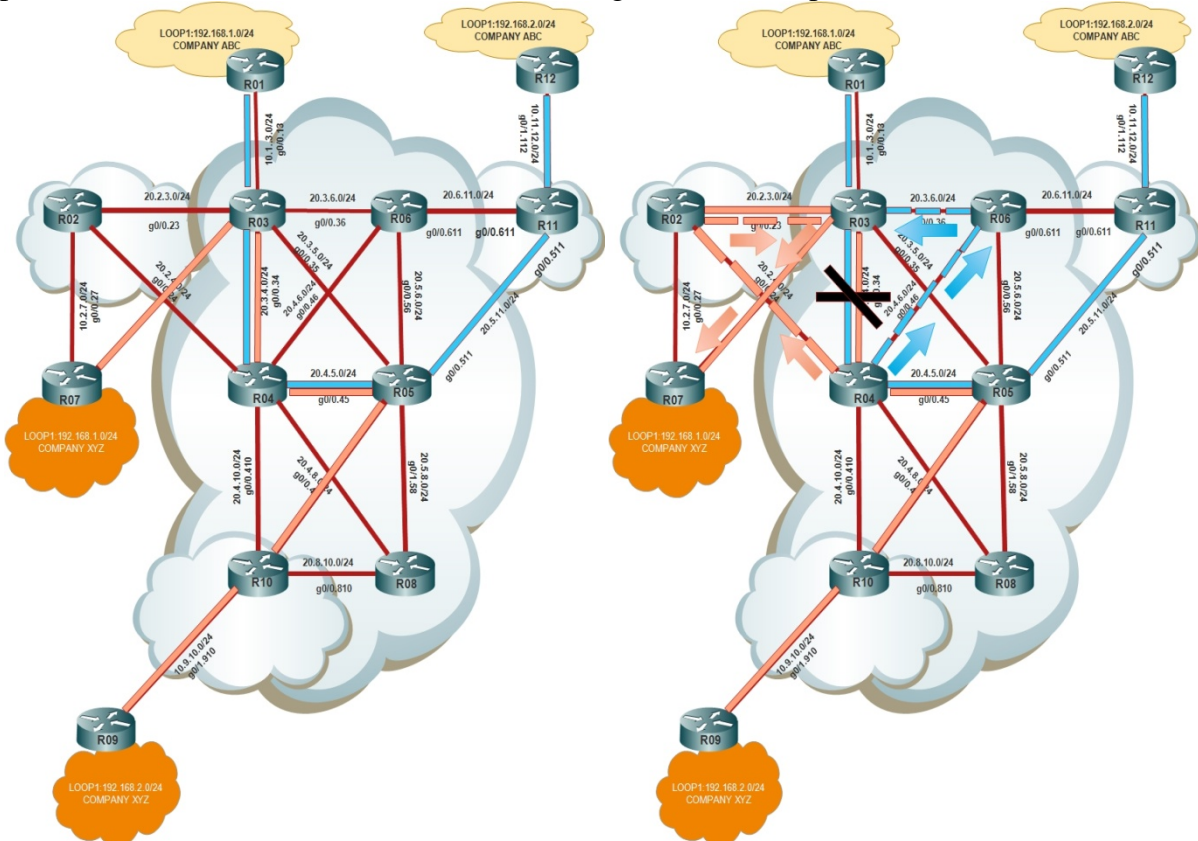
1:1 protection

For 1:1 protection (one-to-one protection) there is one primary LSP and one detour LSP. Unlike the Path protection, the tunnel at the head router is not permanent. When the primary LSP fails, the detour LSP takes over. During normal operation without failure, low priority traffic can be sent through the detour LSP. [2]

Link Protection For 1:1 Protection Case

In the 1:1 protection case, the protection paths created by a PLR are called detours. Network diagram shows the detour paths created for the LSPs by R04 for use should the link between R04 and R03 fail.[2]

A separate detour path is created for each LSP that uses the link between R04 and R03. As each detour path is dedicated to one LSP, it needs to follow the shortest path to the egress point of the LSP being protected (No need for the detour path to rejoin the main LSP at R3 if that would not give the optimum path to the egress node from the PLR). If the shortest path to the egress node intersects the path of the main LSP, the detour path merges with the main LSP at that point. This can be seen in the network diagram: the detour for LSP (R12-R01) follows the path R12-R11-R05-R04-R06-R03-R01 and merges with the main LSP at R03. As can also be seen from the network diagram, the detour LSPs for LSP (9-7) follow the path R09-R10-R05-R04-R02-R03-R07 and merge with their respective LSPs at R03. [2]



NETWORK DIAGRAM 18 :1:1 protection case company BEFORE Failure

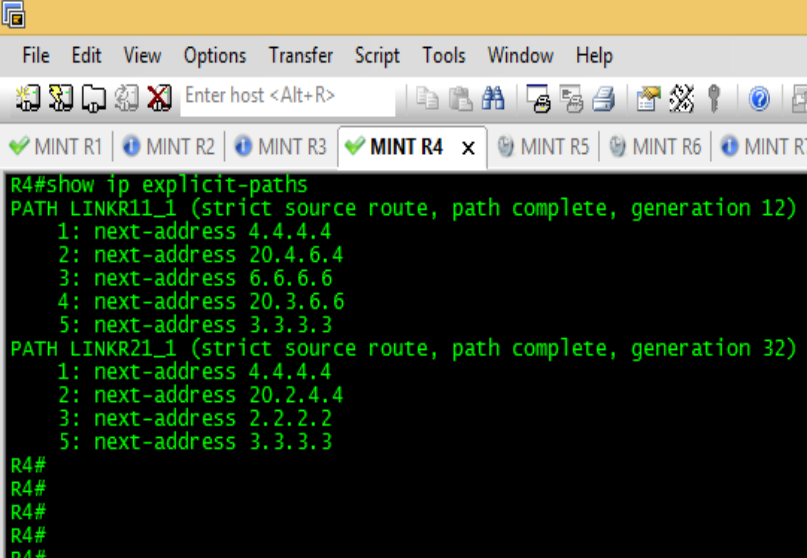
NETWORK DIAGRAM 19: Detour for ABC (BLUE ARROW) and XYZ (PINK ARROW)

ADVANTAGE:

1. As each detour services a single LSP, it allows tighter control over the detour tunnel and its properties. This is difficult with facility backup where multiple LSPs share the same backup.[2]
2. In normal conditions when there is no failure, detour tunnel can be used to transmit other low priority traffic during normal network operation.[2]

DISADVANTAGE:

1. The amount of state that the MP, the PLR and all the nodes in the detour path must maintain increases proportionally to the number of LSPs protected.[2]
2. A separate detour is required for each LSP being protected[2], hence more pre-configuration is required.



```
R4#show ip explicit-paths
PATH LINKR11_1 (strict source route, path complete, generation 12)
 1: next-address 4.4.4.4
 2: next-address 20.4.6.4
 3: next-address 6.6.6.6
 4: next-address 20.3.6.6
 5: next-address 3.3.3.3
PATH LINKR21_1 (strict source route, path complete, generation 32)
 1: next-address 4.4.4.4
 2: next-address 20.2.4.4
 3: next-address 2.2.2.2
 5: next-address 3.3.3.3
R4#
R4#
R4#
R4#
R4#
```

SEPARATE EXPLICIT PATH (DETOURS)FOR TRAFFIC FOR BOTH COMPANIES ABC AND XYZ IF THE LINK BETWEEN R04 AND R05 BREAKS

```

File Edit View Options Transfer Script Tools Window Help
Enter host <Alt+R>
MINT R1 MINT R2 MINT R3 MINT R4 x MINT R5 MINT R6 MINT R7
R4#show run int t1
Building configuration..

Current configuration : 192 bytes
!
interface Tunnel1
 ip unnumbered Loopback0
 tunnel mode mpls traffic-eng
 tunnel destination 3.3.3.3
 tunnel mpls traffic-eng path-option 10 explicit name LINKR11_1
 no routing dynamic
end

R4#show run int t2
Building configuration..

Current configuration : 232 bytes
!
interface Tunnel2
 ip unnumbered Loopback0
 tunnel mode mpls traffic-eng
 tunnel destination 3.3.3.3
 tunnel mpls traffic-eng backup-bw 5999
 tunnel mpls traffic-eng path-option 10 explicit name LINKR21_1
 no routing dynamic
end

R4#

```

TWO DETOUR TUNNELS (TUNNEL1 AND TUNNEL 2) CREATED FOR ABC AND XYZ RESPECTIVELY FOR PROTECTION OF LINK BETWEEN R04 AND R03

```

File Edit View Options Transfer Script Tools Window Help
Enter host <Alt+R>
MINT R1 MINT R2 MINT R3 MINT R4 x MINT R5 MINT R6 MINT R7 MINT R9
R4#show mpls traffic-eng tunnels tunnel 1
Name: R4_t1 (Tunnel1) Destination: 3.3.3.3
Status:
Admin: up Oper: up Path: valid Signalling: connected
path option 10, type explicit LINKR11_1 (Basis for Setup, path weight 20)

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 10 is active
BandwidthOverride: disabled LockDown: disabled verbatim: disabled

InLabel : -
OutLabel : GigabitEthernet0/0.46, 619
RSVP Signalling Info:
Src 4.4.4.4, Dst 3.3.3.3, Tun_Id 1, Tun_Instance 54
RSVP Path Info:
My Address: 20.4.6.4
Explicit Route: 20.4.6.6 20.3.6.6 20.3.6.3 3.3.3.3
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: 20.3.4.4 20.3.4.3 3.3.3.3
History:
Tunnel:
Time since created: 3 hours, 16 minutes
Time since path change: 18 minutes, 25 seconds
Number of LSP IDs (Tun_Instances) used: 54
Current LSP:
Uptime: 18 minutes, 25 seconds
Prior LSP:
ID: path option 10 [53]
Removal Trigger: tunnel shutdown

R4#
R4#

```

PRECOMPUTED DETOUR (TUNNEL 1)FOR TRAFFIC OF COMPANY ABC FLOWING FROM R11 TO R03


```

File Edit View Options Transfer Script Tools Window Help
Enter host <Alt+R>
MINT R1 | MINT R2 | MINT R3 | MINT R4 x | MINT R5 | MINT R6 | MINT R7 | MINT R9 |
R4#show mpls traffic-eng tunnels tunnel 2
Name: R4_t2 (Tunnel2) Destination: 3.3.3.3
Status:
Admin: up Oper: up Path: valid Signalling: connected
path option 10, type explicit LINKR21_1 (Basis for Setup, path weight 20)

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 10 is active
BandwidthOverride: disabled LockDown: disabled Verbatim: disabled

InLabel : -
OutLabel : GigabitEthernet0/0.24, 221
RSVP Signalling Info:
Src 4.4.4.4, Dst 3.3.3.3, Tun_Id 2, Tun_Instance 248
RSVP Path Info:
My Address: 20.2.4.4
Explicit Route: 20.2.4.2 20.2.3.2 20.2.3.3 3.3.3.3
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: 20.3.4.4 20.3.4.3 3.3.3.3
History:
Tunnel:
Time since created: 3 hours, 16 minutes
Time since path change: 18 minutes, 50 seconds
Number of LSP IDs (Tun_Instances) used: 248
Current LSP:
Uptime: 18 minutes, 50 seconds
Prior LSP:
ID: path option 10 [247]
Removal Trigger: tunnel shutdown
R4#

```

PRECOMPUTED DETOUR (TUNNEL 2) FOR TRAFFIC OF COMPANY XYZ FLOWING FROM R10 TO R03

```

File Edit View Options Transfer Script Tools Window He
Enter host <Alt+R>
MINT R1 | MINT R2 | MINT R3 | MINT R4 x | MINT R5
R4#show run int g0/0.34
Building configuration...

Current configuration : 277 bytes
!
interface GigabitEthernet0/0.34
 encapsulation dot1Q 34
 ip address 20.3.4.4 255.255.255.0
 ip router isis 1
 mpls traffic-eng tunnels
 mpls traffic-eng backup-path Tunnel1
 mpls traffic-eng backup-path Tunnel2
 bfd interval 60 min_rx 60 multiplier 4
 ip rsvp bandwidth
end

```

INSTALLATION OF DETOUR PATHS(TUNNEL 1 AND TUNNEL 2) FOR COMPANY ABC AND XYZ RESPECTIVELY

```

File Edit View Options Transfer Script Tools Window Help
Enter host <Alt+R>
MINT R1 MINT R2 MINT R3 MINT R4 MINT R5 MINT R6 MINT R7 MINT R9 MINT R10 x
R10#show mpls traffic-eng tunnels tunnel 0
Name: R10_t0 (Tunnel0) Destination: 3.3.3.3
Status:
  Admin: up Oper: up Path: valid Signalling: connected
  path option 10, type explicit TO_R7 (Basis for Setup, path weight 20)
  change in required resources detected: reroute pending
  Currently Signalled Parameters:
    Bandwidth: 4294 kbps (Global) Priority: 7 7 Affinity: 0x0/0xFFFF
    Metric Type: TE (default)
Config Parameters:
  Bandwidth: 4294 kbps (Global) Priority: 7 7 Affinity: 0x0/0xFFFF
  Metric Type: TE (default)
  AutoRoute: disabled LockDown: disabled Loadshare: 4294 bw-based
  auto-bw: disabled
Active Path Option Parameters:
  State: explicit path option 10 is active
  BandwidthOverride: disabled LockDown: disabled verbatim: disabled

InLabel : -
OutLabel : GigabitEthernet0/0.510, 519
RSVP Signalling Info:
  Src 10.10.10.10, Dst 3.3.3.3, Tun_Id 0, Tun_Instance 300
RSVP Path Info:
  My Address: 20.5.10.10
  Explicit Route: 20.5.10.5 20.4.5.5 20.4.5.4 20.3.4.4
                  20.3.4.3 3.3.3.3
  Record Route: NONE
  Tspec: ave rate=4294 kbits, burst=1000 bytes, peak rate=4294 kbits
RSVP Resv Info:
  Record Route: 5.5.5.5(519) 4.4.4.4(428)
                  3.3.3.3(0)
  Fspec: ave rate=4294 kbits, burst=1000 bytes, peak rate=4294 kbits
Shortest Unconstrained Path Info:
  Path weight: 20 (TE)
  Explicit Route: 20.5.10.10 20.5.10.5 20.3.5.5 20.3.5.3
                  3.3.3.3
History:
  Tunnel:
    Time since created: 3 hours, 46 minutes
    Time since path change: 22 minutes, 42 seconds
    Number of LSP IDs (Tun_Instances) used: 300
  Current LSP:
    Uptime: 10 seconds
    Selection: reoptimization
    Last Error: PCALC:: Explicit path has unknown address, 20.3.4.4
  Prior LSP:
    ID: path option 10 [261]
    Removal Trigger: re-route path error
    Last Error: PCALC:: Explicit path has unknown address, 20.3.4.4
R10#

```

WHEN LINK BETWEEN R04 AND R03 BREAKS LSP FOR CUSTOMER XYZ COMPUTED EXPLICITLY AT R10 IS NOT TEARED DOWN AND DETOUR FOR TRAFFIC PRECOMPUTED AT R04(TUNNEL 2) IS BEING USED UNTIL LSP AT R10 COMPUTES OPTIMAL REROUTE

```

R11#show mpls traffic-eng tunnels tunnel 0
Name: R11_t0 (Tunnel0) Destination: 3.3.3.3
Status:
  Admin: up oper: up Path: valid Signalling: connected
  path option 10, type explicit TO_R3 (Basis for Setup, path weight 20)
  change in required resources detected: reroute pending
  Currently signalled Parameters:
    Bandwidth: 0 kbps (Global) Priority: 7 7 Affinity: 0x0/0xFFFF
    Metric Type: TE (default)
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 10 is active
  Bandwidthoverride: disabled LockDown: disabled verbatim: disabled

InLabel : -
OutLabel : GigabitEthernet0/0.511, 517
RSVP Signalling Info:
  Src 11.11.11.11, Dst 3.3.3.3, Tun_Id 0, Tun_Instance 288
RSVP Path Info:
  My Address: 20.5.11.11
  Explicit Route: 20.5.11.5 20.4.5.5 20.4.5.4 20.3.4.4
                  20.3.4.3 3.3.3.3
  Record Route: NONE
  Tspec: ave rate=0 kbits, burst=1000 bytes, peak rate=0 kbits
RSVP Resv Info:
  Record Route: 5.5.5.5(517) 4.4.4.4(423)
                  3.3.3.3(0)
  Fspec: ave rate=0 kbits, burst=1000 bytes, peak rate=0 kbits
Shortest Unconstrained Path Info:
  Path weight: 20 (TE)
  Explicit Route: 20.5.11.11 20.5.11.5 20.3.5.5 20.3.5.3
                  3.3.3.3
History:
  Tunnel:
    Time since created: 3 hours, 50 minutes
    Time since path change: 23 minutes, 6 seconds
    Number of LSP IDs (Tun_Instances) used: 288
  Current LSP:
    Uptime: 30 seconds
    Selection: reoptimization
    Last Error: PCALC:: Explicit path has unknown address, 20.3.4.4
  Prior LSP:
    ID: path option 10 [249]
    Removal Trigger: re-route path error
    Last Error: PCALC:: Explicit path has unknown address, 20.3.4.4
R11#
R11#

```

WHEN LINK BETWEEN R04 AND R03 BREAKS LSP FOR CUSTOMER ABC COMPUTED EXPLICITLY AT R11 IS NOT TEARED DOWN AND DETOUR FOR TRAFFIC PRECOMPUTED AT R04(TUNNEL 1) IS BEING USED UNTIL LSP AT R11 COMPUTES OPTIMAL REROUTE

```

R12#traceroute 1.1.1.1
Type escape sequence to abort.
Tracing the route to 1.1.1.1
VRF info: (vrf in name/id, vrf out name/id)
 1 10.11.12.11 0 msec 0 msec 0 msec
 2 20.5.11.5 [MPLS: Labels 517/319 Exp 0] 4 msec 0 msec 0 msec
 3 20.4.5.4 [MPLS: Labels 423/319 Exp 0] 4 msec 0 msec 0 msec
 4 10.1.3.3 [MPLS: Label 319 Exp 0] 4 msec 0 msec 0 msec
 5 10.1.3.1 4 msec * 0 msec
R12#traceroute 1.1.1.1
Type escape sequence to abort.
Tracing the route to 1.1.1.1
VRF info: (vrf in name/id, vrf out name/id)
 1 10.11.12.11 0 msec 0 msec 0 msec
 2 20.5.11.5 [MPLS: Labels 517/319 Exp 0] 4 msec 0 msec 0 msec
 3 20.4.5.4 [MPLS: Labels 423/319 Exp 0] 4 msec 0 msec 0 msec
 4 20.4.6.6 [MPLS: Labels 619/319 Exp 0] 4 msec 0 msec 4 msec
 5 10.1.3.3 [MPLS: Label 319 Exp 0] 0 msec 0 msec 4 msec
 6 10.1.3.1 0 msec * 0 msec
R12#
R12#
R12#

```

TRACEROUTE FOR COMPANY ABC BEFORE AND AFTER FAILURE OF LINK BETWEEN R04 AND R03

```

R9#traceroute 7.7.7.7
Type escape sequence to abort.
Tracing the route to 7.7.7.7
 1 10.9.10.10 0 msec 0 msec 0 msec
 2 20.5.10.5 [MPLS: Labels 519/322 Exp 0] 0 msec 0 msec 0 msec
 3 20.4.5.4 [MPLS: Labels 428/322 Exp 0] 4 msec 0 msec 0 msec
 4 10.3.7.3 [MPLS: Label 322 Exp 0] 4 msec 0 msec 0 msec
 5 10.3.7.7 4 msec 0 msec *
R9#traceroute 7.7.7.7
Type escape sequence to abort.
Tracing the route to 7.7.7.7
 1 10.9.10.10 0 msec 0 msec 0 msec
 2 20.5.10.5 [MPLS: Labels 519/322 Exp 0] 0 msec 0 msec 0 msec
 3 20.4.5.4 [MPLS: Labels 428/322 Exp 0] 4 msec 0 msec 0 msec
 4 20.2.4.2 [MPLS: Labels 221/322 Exp 0] 4 msec 0 msec 0 msec
 5 10.3.7.3 [MPLS: Label 322 Exp 0] 4 msec 0 msec 0 msec
 6 10.3.7.7 4 msec 0 msec *
R9#
R9#
R9#

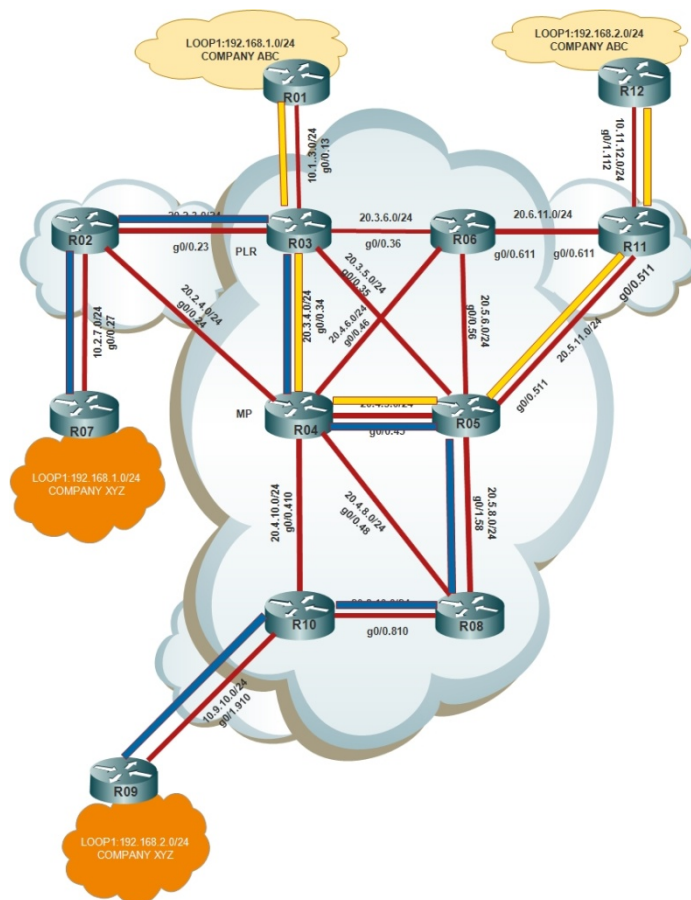
```

TRACEROUTE FOR COMPANY XYZ BEFORE AND AFTER FAILURE OF LINK BETWEEN R04 AND R03

NODE PROTECTION

NODE PROTECTION(FACILITY PROTECTION)

The link protection mechanisms will not work when whole router crashes, if it rely on the adjacent node to act as the MP. Hence backup tunnel around the protected node is computed to the next next-hop in the path, in the case of node facility protection. [2] Network Diagram shows LSP(R07-R09) from R02 to R10, along the path R02-R03-R04-R05-R08-R010. LSP(7-9) is protected against R04 failure by a backup tunnel taking the path R03-R06-R05 that merges back into LSP(7-9) at R05 downstream from



NETWORK DIAGRAM 21:NORMAL FLOW OF PACKET FOR TWO COMPANY TRAFFIC ABC(SHOWN IN YELLOW) AND XYZ (SHOWN IN BLUE)

node R04. When R04, traffic from LSP(7-9) (the protected path) is placed on this backup at R03 and delivered to R05, where it continues on its normal path to R10.

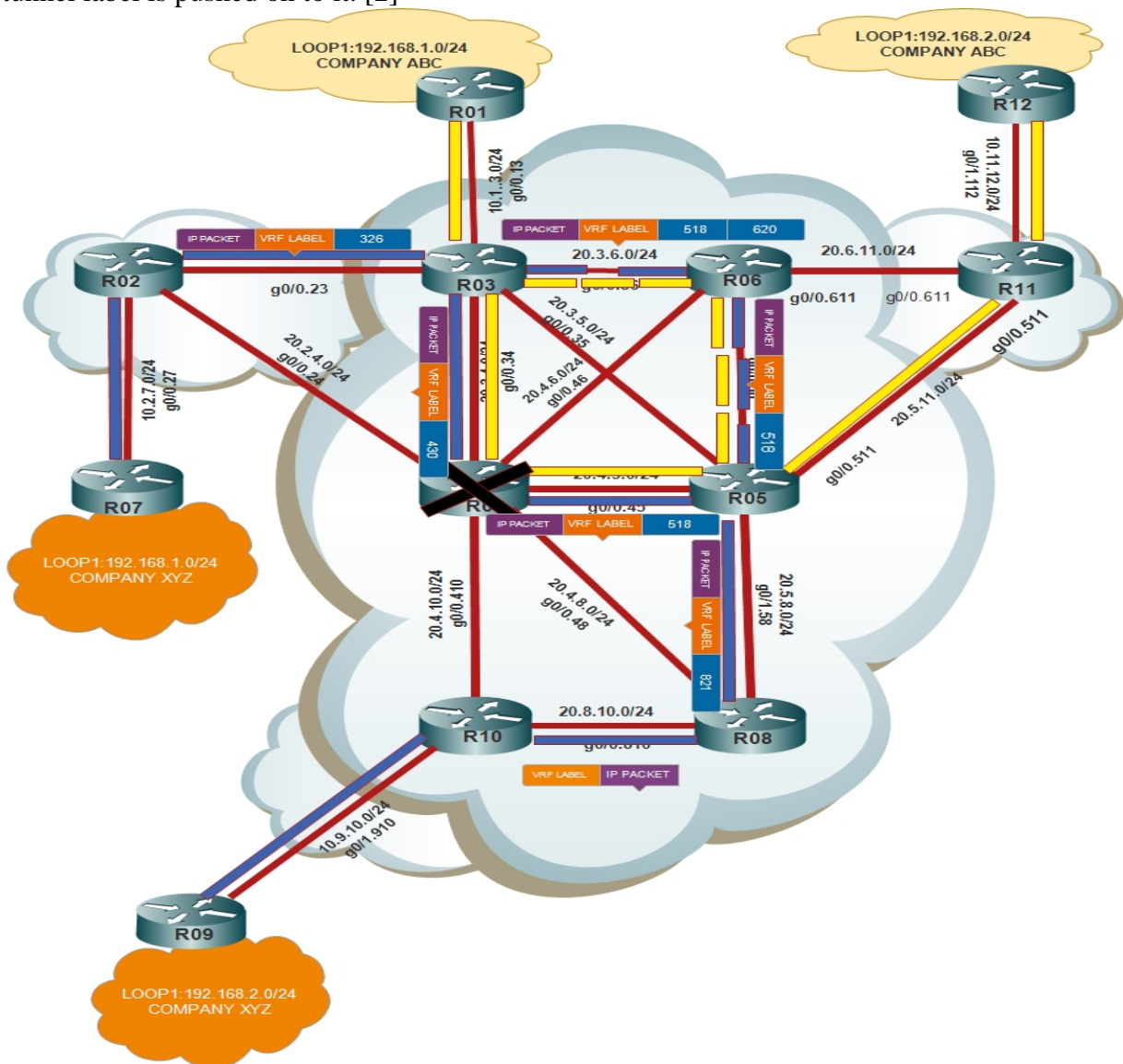
For node protection in facility protection case R03 must have two pieces of information to set up the backup tunnel.[2]

The address of node R05, the tail end of the backup tunnel. This information can be obtained from the Record Route Object (RRO). This address is used as a loose hop for reaching the MP. It can be a router ID or an interface address belonging to the MP.[2]

In the case of node protection in facility protection , the label used by the main LSP at node R04 to send traffic to R05 should be known that is R03 must be able to prepend the packet with label 518 and other label 620 which is expected by R06 rather than the label 430, which is the one used in normal forwarding along the main LSP. [2]

R03 use a similar approach as for the discovery of the downstream node and rely on the information in the RRO, in RRO the new flag ‘label recording desired’ is defined for use in the Session Attribute Object. Setting this flag indicates that the label information should be included in the RRO. Hence, labels are recorded in the RRO and becomes available to the PLR.[2]

With this information, the backup tunnel can be established. Network diagram shows forwarding of traffic over the backup tunnel, assuming node protection in facility protection case. Note that at R03 traffic is already labeled with the label expected by R05 before the tunnel label is pushed on to it. [2]



NETWORK DIAGRAM 22:PACKET FLOW IN CASE OF NODE PROTECTION IN FACILITY PROTECTION CASE WHEN R04 CRASHES(PACKET FLOW FOR XYZ COMAPANY IS SHOWN SIMILAR PROCEDURE IS FOLLOWED FOR ABC COMPANY TRAFFIC)

```

File Edit View Options Transfer Script Tools Window Help
Enter host <Alt+R>
MINT R1 x MINT R2 MINT R3 MINT R4 MINT R5 MINT R6 MINT R7

R1#traceroute 12.12.12.12
Type escape sequence to abort.
Tracing the route to 12.12.12.12
VRF info: (vrf in name/id, vrf out name/id)
 1 10.1.3.3 0 msec 0 msec 0 msec
 2 20.3.4.4 [MPLS: Labels 424/11021 Exp 0] 4 msec 0 msec 0 msec
 3 20.4.5.5 [MPLS: Labels 520/11021 Exp 0] 4 msec 0 msec 0 msec
 4 10.11.12.11 [MPLS: Label 11021 Exp 0] 4 msec 0 msec 0 msec
 5 10.11.12.12 4 msec * 0 msec

R1#traceroute 12.12.12.12
Type escape sequence to abort.
Tracing the route to 12.12.12.12
VRF info: (vrf in name/id, vrf out name/id)
 1 10.1.3.3 0 msec 0 msec 0 msec
 2 20.3.6.6 [MPLS: Labels 620/520/11021 Exp 0] 0 msec 4 msec 0 msec
 3 20.5.6.5 [MPLS: Labels 520/11021 Exp 0] 0 msec 4 msec 0 msec
 4 10.11.12.11 [MPLS: Label 11021 Exp 0] 0 msec 4 msec 0 msec
 5 10.11.12.12 0 msec * 0 msec

R1#
R1#

```

TRACEROUTE FOR COMPANY ABC BEFORE AND AFTER FAILURE OF NODE R04

```

File Edit View Options Transfer Script Tools Window Help
Enter host <Alt+R>
MINT R1 MINT R2 MINT R3 MINT R4 MINT R5 MINT R6 MINT R7 x

R7#traceroute 9.9.9.9
Type escape sequence to abort.
Tracing the route to 9.9.9.9
VRF info: (vrf in name/id, vrf out name/id)
 1 10.2.7.2 0 msec 0 msec 0 msec
 2 20.2.3.3 [MPLS: Labels 326/10022 Exp 0] 0 msec 0 msec 0 msec
 3 20.3.4.4 [MPLS: Labels 430/10022 Exp 0] 4 msec 0 msec 0 msec
 4 20.4.5.5 [MPLS: Labels 518/10022 Exp 0] 4 msec 0 msec 0 msec
 5 20.5.8.8 [MPLS: Labels 821/10022 Exp 0] 4 msec 0 msec 0 msec
 6 10.9.10.10 [MPLS: Label 10022 Exp 0] 4 msec 0 msec 0 msec
 7 10.9.10.9 4 msec 0 msec *

R7#
R7#traceroute 9.9.9.9
Type escape sequence to abort.
Tracing the route to 9.9.9.9
VRF info: (vrf in name/id, vrf out name/id)
 1 10.2.7.2 0 msec 0 msec 0 msec
 2 20.2.3.3 [MPLS: Labels 326/10022 Exp 0] 0 msec 0 msec 0 msec
 3 20.3.6.6 [MPLS: Labels 620/518/10022 Exp 0] 4 msec 0 msec 0 msec
 4 20.5.6.5 [MPLS: Labels 518/10022 Exp 0] 4 msec 0 msec 0 msec
 5 20.5.8.8 [MPLS: Labels 821/10022 Exp 0] 4 msec 0 msec 0 msec
 6 10.9.10.10 [MPLS: Label 10022 Exp 0] 4 msec 0 msec 0 msec
 7 10.9.10.9 4 msec 0 msec *

R7#
R7#

```

TRACEROUTE FOR COMPANY XYZ BEFORE AND AFTER FAILURE OF NODE R04

```

File Edit View Options Transfer Script Tools Window Help
Enter host <Alt+R>
MINT R1 MINT R2 MINT R3 x MINT R4 MINT R5 MINT R6 MINT R7 MINT R9 M

R3#show mpls traffic-eng fast-reroute database
Headend frf information:
Protected tunnel      In-label out intf/label  FRR intf/label  Status
Tunnel0              Tun hd   Gi0/0.34:418    Tu2:523         ready

LSP midpoint frf information:
LSP identifier        In-label out intf/label  FRR intf/label  Status
2.2.2.2 0 [168]      320      Gi0/0.34:429    Tu2:524         ready
R3#
R3#
R3#

```

BACKUP TUNNEL1 IS PRECOMPUTED AT R03 AND IN READY STATE

```

File Edit View Options Transfer Script Tools Window Help
Enter host <Alt+R>
MINT R1 MINT R2 MINT R3 x MINT R4 MINT R5 MINT R6 MINT R7 MINT R9 MINT R10

R3#show mpls traffic-eng fast-reroute database
Headend frf information:
Protected tunnel      In-label out intf/label  FRR intf/label  Status
Tunnel0              Tun hd   Gi0/0.34:418    Tu2:523         active

LSP midpoint frf information:
LSP identifier        In-label out intf/label  FRR intf/label  Status
2.2.2.2 0 [168]      320      Gi0/0.34:429    Tu2:524         active
R3#
R3#
R3#

```

PRECOMPUTED BACKUP TUNNEL 1 IN ACTIVE STATE WHEN NODE R04 FAILS

ADVANTAGE:

1. Backup tunnels that terminate at the next-next hop protect both the downstream link and node. This provides protection for both link and node failures. [30]
2. Rapid repair as soon as error is detected[6](Path is locally repaired and no need to compute new path at headend).

DISADVANTAGE:

1. Single backup path is used to protect two customers (ABC AND XYZ) traffic hence bandwidth protection for each customer traffic may not be possible.
2. Node backup pre-allocated. Need a backup for each protected node[6](manual protection required for each node protection)
3. Requires reporting of labels in Record Route Object.
4. Data path extended by length of backup tunnel.[2]
5. May be limited to the global label space.[2]
6. Extra label stacking is performed to route primary LSP traffic over the backup tunnel.

Node Protection, For The 1:1 Protection Case

In network links ,nodes both can fail hence node protection is required in which all the links connected to node goes down, network diagram shows the detour paths created for the LSPs(both for company ABC and XYZ) by R5 for use should node R4 fail.Separate detour path is created for each LSP that uses the link between R4 and R5. As each detour path is dedicated to one LSP, it simply needs to follow the shortest path to the egress point of the LSP being protected. Thus for LSP(9-7), the detour follows the path R09-R10-R05-R03-R07[2]

The detour paths for LSP (R12-R1) follow the path R12-R11-R05-R06-R03-R01

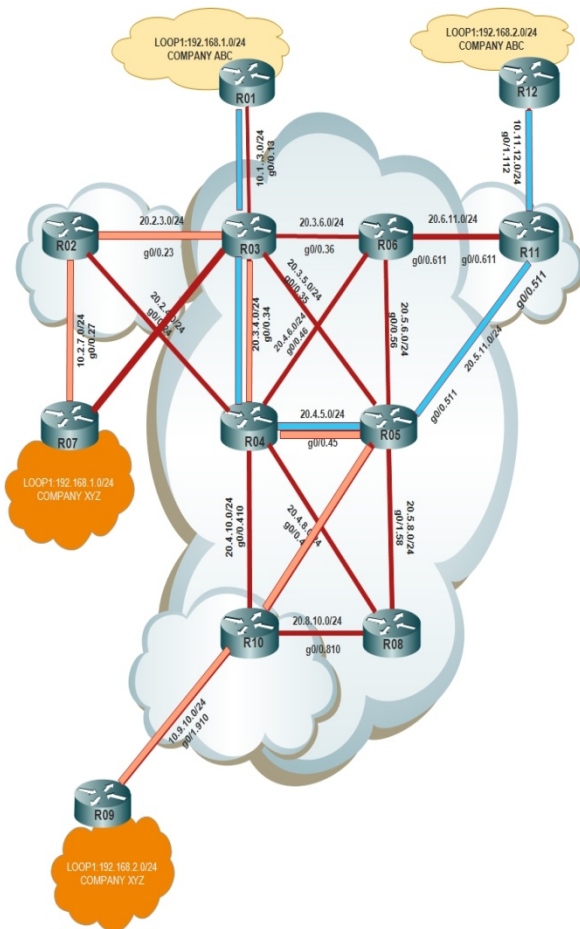
Each PLR(in this lab R05) needs to create several detour tunnels, one for each next next-hop node. [2]

The link protection mechanisms described in the link protection in 1:1 protection case will not work if they rely on the adjacent node to act as the MP. Hence Node protection in 1:1 protection case is required to make the detour tunnel around the protected node to the next next-hop in the path towards the egress point of the main LSP.[2]

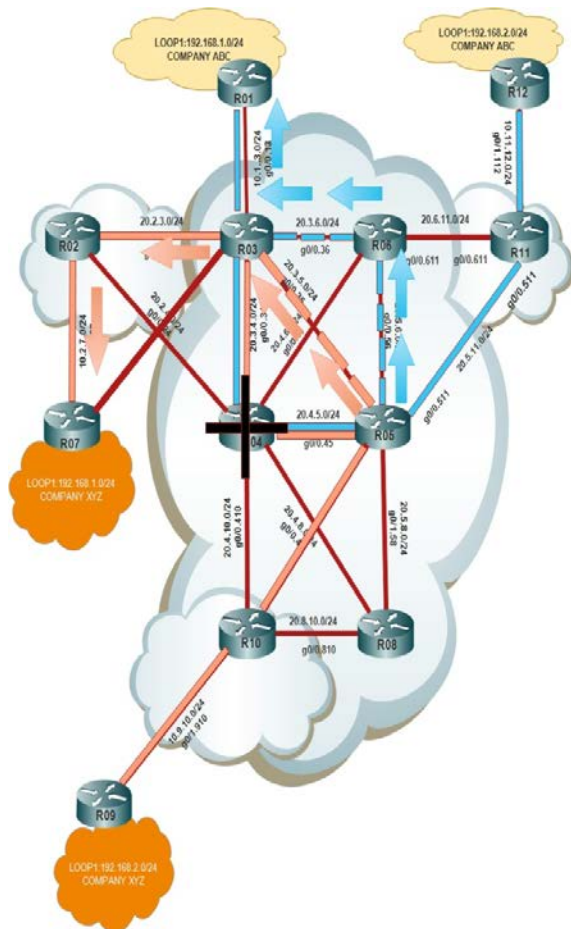
In network diagram when R04 fails, traffic from LSP(9-7) (the protected path) is placed on detour at R05 and delivered to R03 following path R05-To link between R05 and R03, where it continues on its normal path to destination R07. [2]

Similarly LSP(R11-R03) from R11 to R03, along the path R12-R11-R5-R06-R03-R01. When R04 fails, traffic (the protected path) is placed on this detour at R05 and delivered to R03 following path R05-R06-R03, where it continues on its normal path to destination R01.

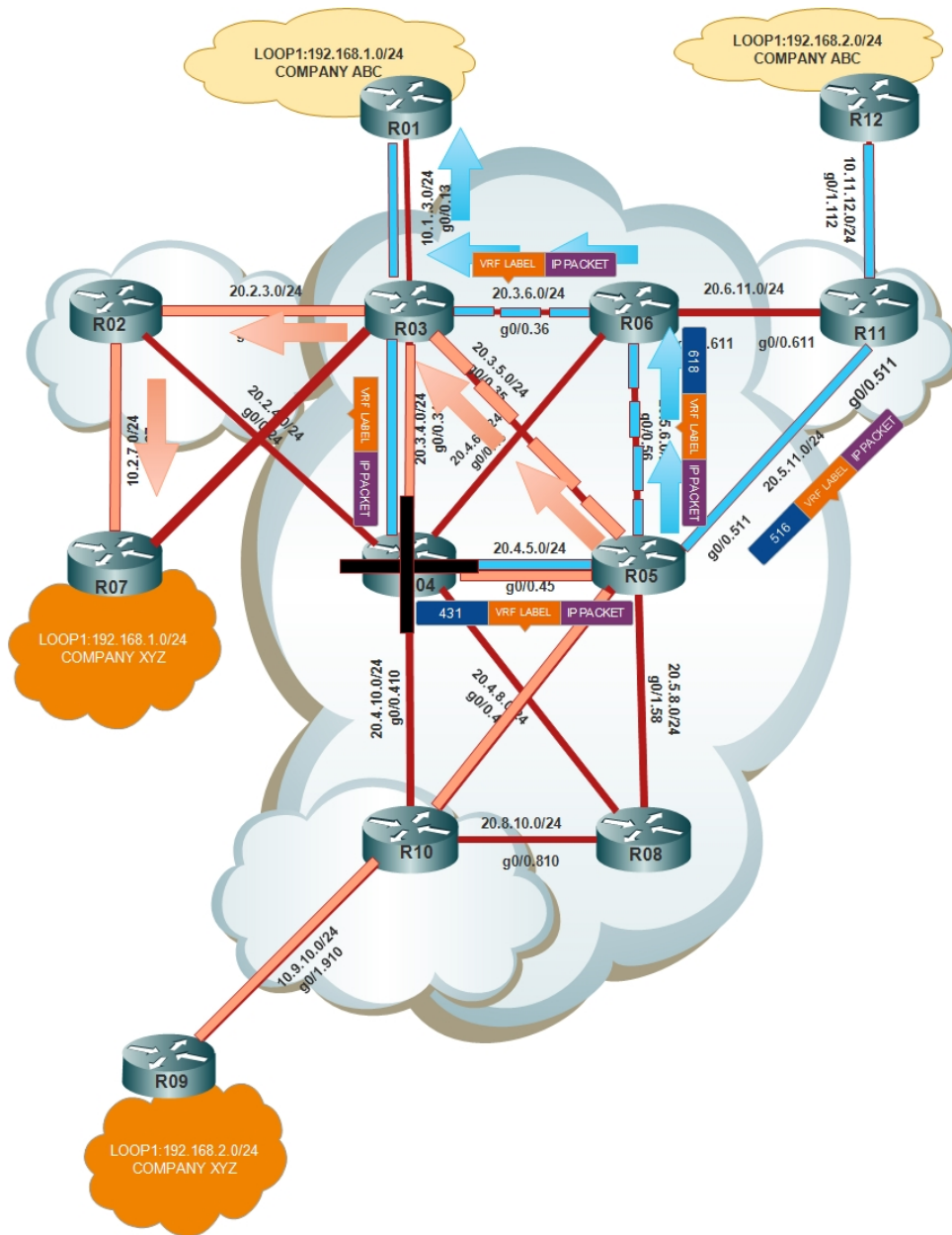
For protection from failure of node R04.R05 must pre-compute the detour paths for the LSP's of two companies ABC and XYZ ,and all the labels for detour to two tunnels created from R05 to R03 for two Company traffic should be in forwarding state.



NETWORK DIAGRAM 23:
LSP PINK(COMPANY XYZ)AND BLUE
(COMPANY ABC) REPRESENT FLOW OF
TRAFFIC BEFORE FAILURE OF NODE R04



NETWORK DIAGRAM 24:
ARROWS PINK(COMPANY XYZ)AND BLUE
(COMPANY ABC) REPRESENT FLOW OF
TRAFFIC AFTER FAILURE OF NODE R04



NETWORK DIAGRAM 25:SHOWS THE FLOW OF TRAFFIC ALONG THE DETOUR TUNNEL FOR COMPANY XYZ WHEN NODE R04 CRASHES IN NODE PROTECTION IN 1:1 PROTECTION CASE

```
File Edit View Options Transfer Script Tools Window Help
Enter host <Alt+R>
MINT R1 MINT R2 MINT R3 MINT R4 MINT R5 x MINT R6 MINT R7
R5#show ip explicit-paths
PATH LINKR21_1 (strict source route, path complete, generation 6)
  1: next-address 4.4.4.4
  2: next-address 20.4.6.4
  3: next-address 20.3.6.6
  4: next-address 3.3.3.3
PATH LINKR31_1 (strict source route, path complete, generation 13)
  1: next-address 4.4.4.4
  2: next-address 20.2.4.4
  3: next-address 2.2.2.2
  4: next-address 20.2.3.2
  5: next-address 3.3.3.3
PATH NODE1_11 (strict source route, path complete, generation 20)
  1: next-address 5.5.5.5
  2: next-address 20.5.6.5
  3: next-address 6.6.6.6
  4: next-address 20.3.6.6
  5: next-address 3.3.3.3
PATH NODE1_17 (strict source route, path complete, generation 25)
  1: next-address 5.5.5.5
  2: next-address 20.3.5.5
  3: next-address 3.3.3.3
```

SEPARATE EXPLICIT PATH (DETOURS)FOR TRAFFIC FOR BOTH COMPANIES ABC AND XYZ IF THE NODE R04 BREAKS

```
File Edit View Options Transfer Script Tools Window Help
Enter host <Alt+R>
MINT R1 MINT R2 MINT R3 MINT R4 MINT R5 x MINT R6 MINT R7
R5#show running-config interface tunnel 1
Building configuration...

Current configuration : 191 bytes
!
interface Tunnel1
 ip unnumbered Loopback0
 tunnel mode mpls traffic-eng
 tunnel destination 3.3.3.3
 tunnel mpls traffic-eng path-option 10 explicit name NODE1_11
 no routing dynamic
end

R5#show running-config interface tunnel 2
Building configuration...

Current configuration : 231 bytes
!
interface Tunnel2
 ip unnumbered Loopback0
 tunnel mode mpls traffic-eng
 tunnel destination 3.3.3.3
 tunnel mpls traffic-eng backup-bw 4294
 tunnel mpls traffic-eng path-option 10 explicit name NODE1_17
 no routing dynamic
end
```

TWO DETOUR TUNNELS (TUNNEL1 AND TUNNEL 2) CREATED FOR ABC AND XYZ RESPECTIVELY FOR PROTECTION OF NODE FAILURE R04

```

File Edit View Options Transfer Script Tools Window Help
Enter host <Alt+R>
MINT R1 MINT R2 MINT R3 MINT R4 MINT R5 x MINT R6 MINT R7
R5#show running-config interface gigabitEthernet 0/0.45
Building configuration...

Current configuration : 287 bytes
!
interface GigabitEthernet0/0.45
 encapsulation dot1q 45
 ip address 20.4.5.5 255.255.255.0
 ip router isis 1
 shutdown
 mpls traffic-eng tunnels
 mpls traffic-eng backup-path Tunnel1
 mpls traffic-eng backup-path Tunnel2
 bfd interval 60 min_rx 60 multiplier 4
 ip rsvp bandwidth
end

```

INSTALLATION OF DETOUR PATHS(TUNNEL 1 AND TUNNEL 2) FOR COMPANY ABC AND XYZ RESPECTIVELY AT G0/0.45 OF R05

```

File Edit View Options Transfer Script Tools Window Help
Enter host <Alt+R>
MINT R1 MINT R2 MINT R3 MINT R4 MINT R5 x MINT R6 MINT R7 MINT R9 M
R5#show mpls traffic-eng fast-reroute database
Headend frr information:
Protected tunnel          In-label out intf/label  FRR intf/label  Status

LSP midpoint frr information:
LSP identifier           In-label out intf/label  FRR intf/label  Status
10.10.10.10 0 [2]       517     Gi0/0.45:422   Tu2:323         ready
11.11.11.11 0 [341]    516     Gi0/0.45:431   Tu1:implicit-nu ready

```

DETOUR TUNNELS ARE PRECOMPUTED AT R05 FOR NODE PROTECTION IN 1:1 PROTECTION CASE AND THEY ARE IN READY STATE

```

File Edit View Options Transfer Script Tools Window Help
Enter host <Alt+R>
MINT R1 MINT R2 MINT R3 MINT R4 MINT R5 x MINT R6 MINT R7 MINT R9 M
R5#show mpls traffic-eng fast-reroute database
Headend frr information:
Protected tunnel          In-label out intf/label  FRR intf/label  Status

LSP midpoint frr information:
LSP identifier           In-label out intf/label  FRR intf/label  Status
10.10.10.10 0 [2]       517     Gi0/0.45:422   Tu2:323         active
11.11.11.11 0 [341]    516     Gi0/0.45:431   Tu1:implicit-nu active
R5#
R5#

```

DETOUR TUNNELS ARE PRECOMPUTED AT R05 FOR NODE PROTECTION IN 1:1 PROTECTION CASE AND THEY ARE IN ACTIVE STATE

```

R12#traceroute 1.1.1.1
Type escape sequence to abort.
Tracing the route to 1.1.1.1
VRF info: (vrf in name/id, vrf out name/id)
 1 10.11.12.11 0 msec 0 msec 0 msec
 2 20.5.11.5 [MPLS: Labels 516/319 Exp 0] 0 msec 4 msec 0 msec
 3 20.4.5.4 [MPLS: Labels 431/319 Exp 0] 0 msec 4 msec 0 msec
 4 10.1.3.3 [MPLS: Label 319 Exp 0] 0 msec 0 msec 4 msec
 5 10.1.3.1 0 msec * 0 msec
R12#traceroute 1.1.1.1
Type escape sequence to abort.
Tracing the route to 1.1.1.1
VRF info: (vrf in name/id, vrf out name/id)
 1 10.11.12.11 4 msec 0 msec 0 msec
 2 20.5.11.5 [MPLS: Labels 516/319 Exp 0] 0 msec 4 msec 0 msec
 3 20.5.6.6 [MPLS: Labels 618/319 Exp 0] 0 msec 4 msec 0 msec
 4 10.1.3.3 [MPLS: Label 319 Exp 0] 0 msec 4 msec 0 msec
 5 10.1.3.1 0 msec * 0 msec
R12#

```

TRACEROUTE FOR COMPANY ABC BEFORE AND AFTER FAILURE OF NODER04

```

R9#traceroute 7.7.7.7
Type escape sequence to abort.
Tracing the route to 7.7.7.7
 1 10.9.10.10 0 msec 0 msec 0 msec
 2 20.5.10.5 [MPLS: Labels 518/223 Exp 0] 0 msec 0 msec 0 msec
 3 20.4.5.4 [MPLS: Labels 432/223 Exp 0] 4 msec 0 msec 0 msec
 4 20.3.4.3 [MPLS: Labels 309/223 Exp 0] 4 msec 0 msec 0 msec
 5 10.2.7.2 [MPLS: Label 223 Exp 0] 4 msec 0 msec 0 msec
 6 10.2.7.7 4 msec 0 msec *
R9#traceroute 7.7.7.7
Type escape sequence to abort.
Tracing the route to 7.7.7.7
 1 10.9.10.10 0 msec 0 msec 0 msec
 2 20.5.10.5 [MPLS: Labels 517/223 Exp 0] 0 msec 0 msec 0 msec
 3 20.3.5.3 [MPLS: Labels 323/223 Exp 0] 4 msec 0 msec 0 msec
 4 10.2.7.2 [MPLS: Label 223 Exp 0] 4 msec 0 msec 0 msec
 5 10.2.7.7 0 msec 0 msec *
R9#

```

TRACEROUTE FOR COMPANY XYZ BEFORE AND AFTER FAILURE OF NODER04

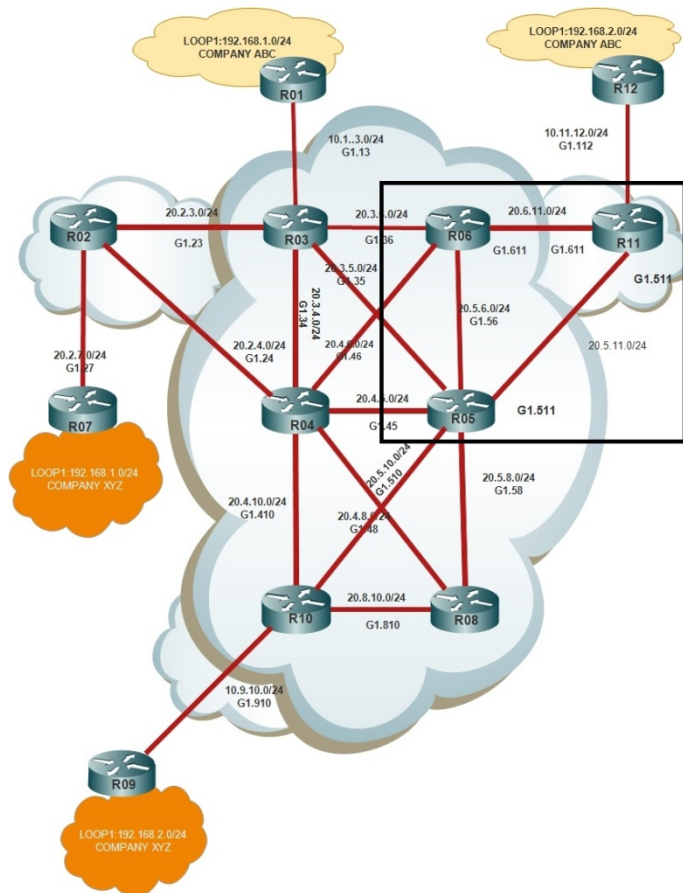
ADVANTAGE:

1. More optimal paths for the protected traffic, as compared with node protection in facility protection case.
2. As each detour services a single LSP, it allows tighter control over the detour tunnel and its properties. This is difficult with facility backup where multiple LSPs share the same backup.[2]
3. In normal conditions when there is no failure, detour tunnel can be used to transmit other low priority traffic during normal network operation.[2]
4. It provides protection against both link failure and node failure which was not possible in link protection in 1:1 protection.

DISADVANTAGE

1. A separate detour is required for each LSP being protected – in most cases this will result in more protection paths being created than in case of node protection in facility protection case but with the benefit of having more optimal paths for the protected traffic.[2]
2. The amount of state that the MP, the PLR and all the nodes in the detour path must maintain increases proportionally to the number of LSPs protected.[2]
3. A separate detour is required for each LSP being protected ,hence more pre-configuration is required.[2]

In below Network Diagram if link failure between R11 and R06, R11 has LFA FRR enabled and immediately redirects traffic to R05 without waiting for underlying routing protocol to converge network topology after failure. LFA FRR redirect traffic to the pre-computed repair path in less than 50 milliseconds once the failure event is detected.[23][2][9]



NETWORK DIAGRAM 27: SHOWS IF LINK BETWEEN R06 AND R11 FAILS R11 USES PRE-COMPUTED REPAIR PATH TO R05

```

R11#show ip route repair-paths 3.3.3.3
Routing entry for 3.3.3.3/32
  Known via "isis", distance 115, metric 20, type level-2
  Redistributing via isis 1
  Last update from 20.6.11.6 on GigabitEthernet1.611, 00:02:30 ago
  Routing Descriptor Blocks:
    20.6.11.6, from 3.3.3.3, 00:02:30 ago, via GigabitEthernet1.611
    Route metric is 20, traffic share count is 1
    Repair Path: 20.5.11.5, via GigabitEthernet1.511
    * 20.5.11.5, from 3.3.3.3, 00:02:30 ago, via GigabitEthernet1.511
    Route metric is 20, traffic share count is 1
    Repair Path: 20.6.11.6, via GigabitEthernet1.611
  
```

REPAIR PATH PRE-COMPUTED AT R11

PRECALCULATED REPAIR-PATHS ON R11

```

R11#show ip route repair-paths
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, H - NHRP, I - LISP
a - application route
+ - replicated route, % - next hop override

Gateway of last resort is not set

i L2 2.0.0.0/32 is subnetted, 1 subnets
      2.2.2.2 [115/30] via 20.6.11.6, 00:03:21, GigabitEthernet1.611
          Repair Path: 20.5.11.5, via GigabitEthernet1.511
          [115/30] via 20.5.11.5, 00:03:21, GigabitEthernet1.511
          Repair Path: 20.6.11.6, via GigabitEthernet1.611
i L2 3.0.0.0/32 is subnetted, 1 subnets
      3.3.3.3 [115/20] via 20.6.11.6, 00:03:21, GigabitEthernet1.611
          Repair Path: 20.5.11.5, via GigabitEthernet1.511
          [115/20] via 20.5.11.5, 00:03:21, GigabitEthernet1.511
          Repair Path: 20.6.11.6, via GigabitEthernet1.611
i L2 4.0.0.0/32 is subnetted, 1 subnets
      4.4.4.4 [115/20] via 20.6.11.6, 00:03:21, GigabitEthernet1.611
          Repair Path: 20.5.11.5, via GigabitEthernet1.511
          [RPR][115/30] via 20.5.11.5, 00:03:21, GigabitEthernet1.511
i L2 5.0.0.0/32 is subnetted, 1 subnets
      5.5.5.5 [115/10] via 20.5.11.5, 00:03:21, GigabitEthernet1.511
          Repair Path: 20.6.11.6, via GigabitEthernet1.611
          [RPR][115/20] via 20.6.11.6, 00:03:21, GigabitEthernet1.611
i L2 6.0.0.0/32 is subnetted, 1 subnets
      6.6.6.6 [115/10] via 20.6.11.6, 00:03:21, GigabitEthernet1.611
          Repair Path: 20.5.11.5, via GigabitEthernet1.511
          [RPR][115/20] via 20.5.11.5, 00:03:21, GigabitEthernet1.511

```

```

i L2 8.0.0.0/32 is subnetted, 1 subnets
      8.8.8.8 [115/20] via 20.5.11.5, 00:03:21, GigabitEthernet1.511
          Repair Path: 20.6.11.6, via GigabitEthernet1.611
          [RPR][115/30] via 20.6.11.6, 00:03:21, GigabitEthernet1.611
i L2 10.0.0.0/32 is subnetted, 1 subnets
      10.10.10.10 [115/20] via 20.5.11.5, 00:03:21, GigabitEthernet1.511
          Repair Path: 20.6.11.6, via GigabitEthernet1.611
          [RPR][115/30] via 20.6.11.6, 00:03:21, GigabitEthernet1.611
C 11.0.0.0/32 is subnetted, 1 subnets
      11.11.11.11 is directly connected, Loopback0
i L2 20.0.0.0/8 is variably subnetted, 17 subnets, 2 masks
      20.2.3.0/24 [115/30] via 20.6.11.6, 00:03:21, GigabitEthernet1.611
          Repair Path: 20.5.11.5, via GigabitEthernet1.511
          [115/30] via 20.5.11.5, 00:03:21, GigabitEthernet1.511
          Repair Path: 20.6.11.6, via GigabitEthernet1.611
i L2 20.2.4.0/24 [115/30] via 20.6.11.6, 00:03:21, GigabitEthernet1.611
          Repair Path: 20.5.11.5, via GigabitEthernet1.511
          [RPR][115/40] via 20.5.11.5, 00:03:21, GigabitEthernet1.511
i L2 20.3.4.0/24 [115/30] via 20.6.11.6, 00:03:21, GigabitEthernet1.611
          Repair Path: 20.5.11.5, via GigabitEthernet1.511
          [115/30] via 20.5.11.5, 00:03:21, GigabitEthernet1.511
          Repair Path: 20.6.11.6, via GigabitEthernet1.611
i L2 20.3.5.0/24 [115/20] via 20.5.11.5, 00:03:21, GigabitEthernet1.511
          Repair Path: 20.6.11.6, via GigabitEthernet1.611
          [RPR][115/30] via 20.6.11.6, 00:03:21, GigabitEthernet1.611
i L2 20.3.6.0/24 [115/20] via 20.6.11.6, 00:03:21, GigabitEthernet1.611
          Repair Path: 20.5.11.5, via GigabitEthernet1.511
          [RPR][115/30] via 20.5.11.5, 00:03:21, GigabitEthernet1.511
i L2 20.4.5.0/24 [115/20] via 20.5.11.5, 00:03:21, GigabitEthernet1.511
          Repair Path: 20.6.11.6, via GigabitEthernet1.611
          [RPR][115/30] via 20.6.11.6, 00:03:21, GigabitEthernet1.611
i L2 20.4.6.0/24 [115/20] via 20.6.11.6, 00:03:21, GigabitEthernet1.611
          Repair Path: 20.5.11.5, via GigabitEthernet1.511
          [RPR][115/30] via 20.5.11.5, 00:03:21, GigabitEthernet1.511
i L2 20.4.8.0/24 [115/30] via 20.6.11.6, 00:03:21, GigabitEthernet1.611
          Repair Path: 20.5.11.5, via GigabitEthernet1.511
          [115/30] via 20.5.11.5, 00:03:21, GigabitEthernet1.511
          Repair Path: 20.6.11.6, via GigabitEthernet1.611
i L2 20.4.10.0/24 [115/30] via 20.6.11.6, 00:03:21, GigabitEthernet1.611
          Repair Path: 20.5.11.5, via GigabitEthernet1.511
          [115/30] via 20.5.11.5, 00:03:21, GigabitEthernet1.511
          Repair Path: 20.6.11.6, via GigabitEthernet1.611
i L2 20.5.6.0/24 [115/20] via 20.6.11.6, 00:03:21, GigabitEthernet1.611
          Repair Path: 20.5.11.5, via GigabitEthernet1.511
          [115/20] via 20.5.11.5, 00:03:21, GigabitEthernet1.511
          Repair Path: 20.6.11.6, via GigabitEthernet1.611
i L2 20.5.8.0/24 [115/20] via 20.5.11.5, 00:03:21, GigabitEthernet1.511
          Repair Path: 20.6.11.6, via GigabitEthernet1.611
          [RPR][115/30] via 20.6.11.6, 00:03:21, GigabitEthernet1.611
i L2 20.5.10.0/24 [115/20] via 20.5.11.5, 00:03:21, GigabitEthernet1.511
          Repair Path: 20.6.11.6, via GigabitEthernet1.611
          [RPR][115/30] via 20.6.11.6, 00:03:21, GigabitEthernet1.611
C 20.5.11.0/24 is directly connected, GigabitEthernet1.511
L 20.5.11.11/32 is directly connected, GigabitEthernet1.511
C 20.6.11.0/24 is directly connected, GigabitEthernet1.611
L 20.6.11.19/32 is directly connected, GigabitEthernet1.611
i L2 20.8.10.0/24 [115/30] via 20.5.11.5, 00:03:21, GigabitEthernet1.511
          Repair Path: 20.6.11.6, via GigabitEthernet1.611
          [RPR][115/40] via 20.6.11.6, 00:03:21, GigabitEthernet1.611
R11#

```



```

File Edit View Options Transfer Script Tools Window Help
Enter host <Alt+R>
R1 R2 R3 R4 R5 R6 R7 R8 R9 R10 R11 x R12

R11#show ip route repair-paths 3.3.3.3
Routing entry for 3.3.3.3/32
  Known via "isis", distance 115, metric 20, type level-2
  Redistributing via isis 1
  Last update from 20.6.11.6 on GigabitEthernet1.611, 00:02:30 ago
  Routing Descriptor Blocks:
    20.6.11.6, from 3.3.3.3, 00:02:30 ago, via GigabitEthernet1.611
      Route metric is 20, traffic share count is 1
      Repair Path: 20.5.11.5, via GigabitEthernet1.511
    * 20.5.11.5, from 3.3.3.3, 00:02:30 ago, via GigabitEthernet1.511
      Route metric is 20, traffic share count is 1
      Repair Path: 20.6.11.6, via GigabitEthernet1.611
  R11#

```

LOOP FREE ALTERNATE PATH ON R03 FOR COMPANY ABC TREAFFIC

```

File Edit View Options Transfer Script Tools Window Help
Enter host <Alt+R>
R1 R2 R3 x R4 R5 R6 R7 R8 R9 R10 R11 R12

R3#show ip route 11.11.11.11
Routing entry for 11.11.11.11/32
  Known via "isis", distance 115, metric 20, type level-2
  Redistributing via isis 1
  Last update from 20.3.6.6 on GigabitEthernet1.36, 00:00:12 ago
  Routing Descriptor Blocks:
    20.3.6.6, from 11.11.11.11, 00:00:12 ago, via GigabitEthernet1.36
      Route metric is 20, traffic share count is 1
      Repair Path: 20.3.5.5, via GigabitEthernet1.35
    * 20.3.5.5, from 11.11.11.11, 00:00:12 ago, via GigabitEthernet1.35
      Route metric is 20, traffic share count is 1
      Repair Path: 20.3.6.6, via GigabitEthernet1.36
  R3#

```

LOOP FREE ALTERNATE PATH ON R11 FOR COMPANY ABC TREAFFIC

```

File Edit View Options Transfer Script Tools Window Help
Enter host <Alt+R>
R1 R2 R3 R4 R5 R6 R7 R8 R9 R10 x R11 R12

R10#
R10#show ip route 2.2.2.2
Routing entry for 2.2.2.2/32
  Known via "isis", distance 115, metric 20, type level-2
  Redistributing via isis 1
  Last update from 20.4.10.4 on GigabitEthernet1.410, 00:08:44 ago
  Routing Descriptor Blocks:
    * 20.4.10.4, from 2.2.2.2, 00:08:44 ago, via GigabitEthernet1.410
      Route metric is 20, traffic share count is 1
      Repair Path: 20.5.10.5, via GigabitEthernet1.510
  R10#
R10#
R10#
R10#
R10#show ip route 3.3.3.3
Routing entry for 3.3.3.3/32
  Known via "isis", distance 115, metric 20, type level-2
  Redistributing via isis 1
  Last update from 20.5.10.5 on GigabitEthernet1.510, 00:09:18 ago
  Routing Descriptor Blocks:
    20.5.10.5, from 3.3.3.3, 00:09:18 ago, via GigabitEthernet1.510
      Route metric is 20, traffic share count is 1
      Repair Path: 20.4.10.4, via GigabitEthernet1.410
    * 20.4.10.4, from 3.3.3.3, 00:09:18 ago, via GigabitEthernet1.410
      Route metric is 20, traffic share count is 1
      Repair Path: 20.5.10.5, via GigabitEthernet1.510
  R10#
R10#
R10#
R10#
R10#show ip route 11.11.11.11
Routing entry for 11.11.11.11/32
  Known via "isis", distance 115, metric 20, type level-2
  Redistributing via isis 1
  Last update from 20.5.10.5 on GigabitEthernet1.510, 00:07:35 ago
  Routing Descriptor Blocks:
    * 20.5.10.5, from 11.11.11.11, 00:07:35 ago, via GigabitEthernet1.510
      Route metric is 20, traffic share count is 1
      Repair Path: 20.4.10.4, via GigabitEthernet1.410
  R10#

```

LOOP FREE ALTERNATE PATH ON R10 FOR COMPANY XYZ TREAFFIC

```

File Edit View Options Transfer Script Tools Window Help
Enter host <Alt+R>
R1 R2 x R3 R4 R5 R6 R7 R8 R9 R10 R11 R12

R2#show ip route 10.10.10.10
Routing entry for 10.10.10.10/32
  Known via "isis", distance 115, metric 20, type level-2
  Redistributing via isis 1
  Last update from 20.2.4.4 on GigabitEthernet1.24, 00:06:22 ago
  Routing Descriptor Blocks:
    * 20.2.4.4, from 10.10.10.10, 00:06:22 ago, via GigabitEthernet1.24
      Route metric is 20, traffic share count is 1
      Repair Path: 20.2.3.3, via GigabitEthernet1.23
  R2#

```

LOOP FREE ALTERNATE PATH ON R02 FOR COMPANY XYZ TREAFFIC

FAST-REROUTE PROTECTION COVERAGE FOR THE FAILURE IN THE NETWORK

```

File Edit View Options Transfer Script Tools Window Help
Enter host <Alt+R>
R1 R2 x R3 R4 R5 R6 R7 R8 R9 R10 R11
R2#show isis fast-reroute summary
Tag 1:
Microloop Avoidance State: Enabled for protected
IPv4 Fast-Reroute Protection Summary:

Prefix Counts:          Total      Protected  Coverage
High priority:          0         0          0%
Normal priority:        22        20         90%
Total:                   22        20         90%
    
```

```

File Edit View Options Transfer Script Tools Window Help
Enter host <Alt+R>
R1 R2 R3 x R4 R5 R6 R7 R8 R9 R10 R11
R3#show isis fast-reroute summary
Tag 1:
Microloop Avoidance State: Enabled for protected
IPv4 Fast-Reroute Protection Summary:

Prefix Counts:          Total      Protected  Coverage
High priority:          0         0          0%
Normal priority:        22        18         81%
Total:                   22        18         81%
    
```

```

File Edit View Options Transfer Script Tools Window Help
Enter host <Alt+R>
R1 R2 R3 R4 R5 R6 R7 R8 R9 R10 R11
R11#show isis fast-reroute summary
Tag 1:
Microloop Avoidance State: Enabled for protected
IPv4 Fast-Reroute Protection Summary:

Prefix Counts:          Total      Protected  Coverage
High priority:          0         0          0%
Normal priority:        22        20         90%
Total:                   22        20         90%
    
```

```

File Edit View Options Transfer Script Tools Window Help
Enter host <Alt+R>
R1 R2 R3 R4 R5 R6 R7 R8 R9 R10 x R11 R12
R10#show isis fast-reroute summary
Tag 1:
Microloop Avoidance State: Enabled for protected
IPv4 Fast-Reroute Protection Summary:

Prefix Counts:          Total      Protected  Coverage
High priority:          0         0          0%
Normal priority:        22        19         86%
Total:                   22        19         86%
    
```

TERMINOLOGY COMMON IN LOOP FREE ALTERNATE FAST-REROUTE

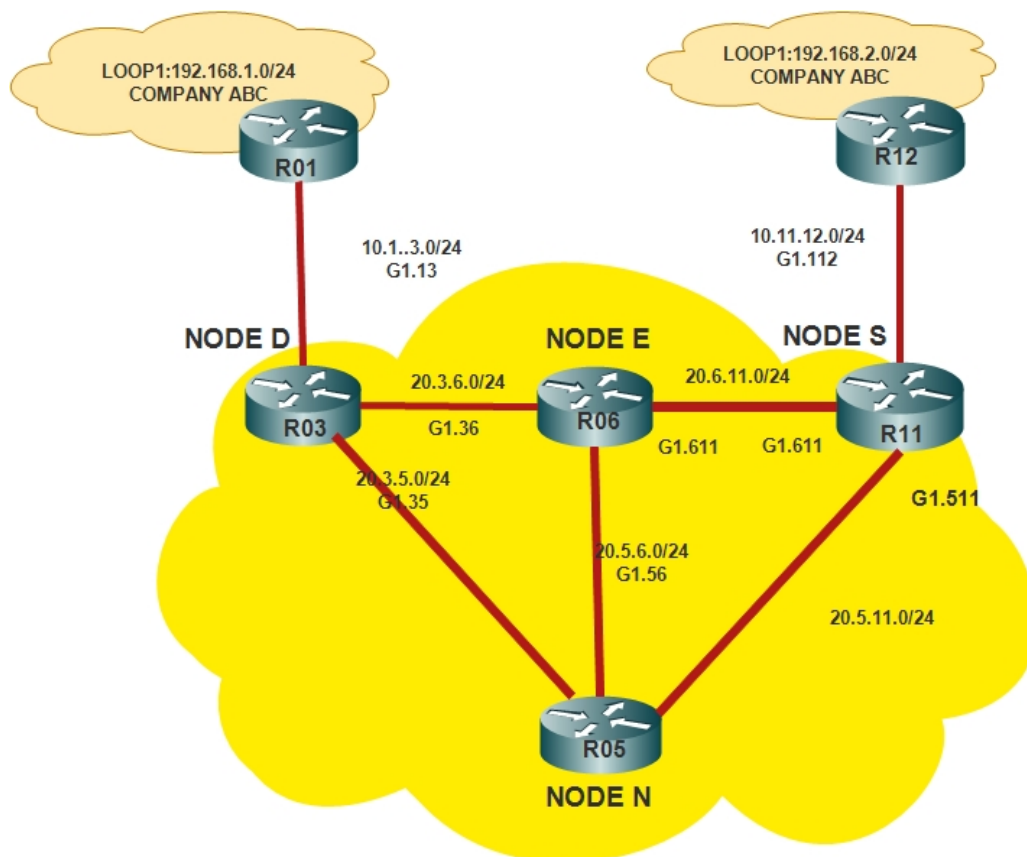
NODE S = Source router

NODE D = Destination router

NODE N = Neighbor router

NODE E = Neighbor router being protected

NODE PN = Pseudo-Node



NOTE 1: IN THE LAB TOPOLOGY ALL LINKS HAVE EQUAL COST

NOTE 2: FOR LAB DEMONSTRATION ALL LINKS ARE MADE POINT-TO-POINT BY IS-IS NETWORK POINT-TO-POINT COMMAND

For the path to be the repair path following conditions should be satisfied:

Inequality 1: Loop Free.[23][2][9]

The neighboring router (Node N) should not expect that the protecting node (Node S) has the better path to reach the destination (Node D).

$\text{Distance (Node N, Node D)} < \text{Distance (Node S, Node D)} + \text{Distance (Node N, Node S)}$

Inequality 2: Downstream Path[23][2][9]

The neighboring router (Node N) is closer to the destination (Node D) than the local router (Node S). By satisfying this condition in multiple failures the neighbor router (Node N) will not form a loop and send traffic back to the source router (Node S).

Distance (Node N, Node D) < Distance (Node S, Node D)

Inequality 3: Node-Protecting Loop-Free Alternate[23][2][9]

The primary path between the source router (Node S) and the destination router (Node D) passes through the neighboring router (Node E). For node protection repair path should not pass through Node E.

Distance (Node N, Node D) < Distance (Node N, Node E) + Distance (Node E, Node D)

Inequality 4: Loop-Free Link Protection for Broadcast Links[23][2][9]

The repair path should not cross the same broadcast network (switch) as the primary path.

LFA FRR Protection Modes

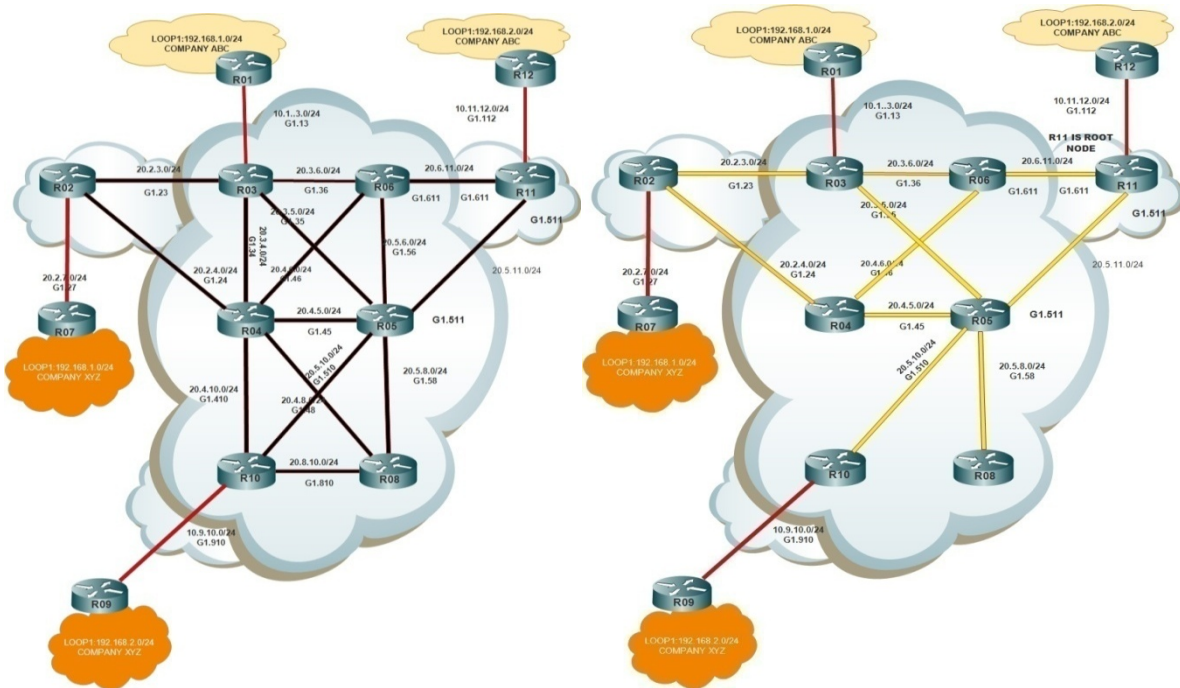
The two modes for creating the LFA FRR repair path are:

Per-link: All routes reachable through the primary protected link's next-hop address share the same repair path. Therefore, either all the prefixes using the net-hop address of the primary link are protected or none of the prefixes are protected. [9]

Per-prefix: Per-prefix LFA performs repair path computation for every prefix. This allows for an optimal repair path to be created for each destination network. Each prefix may have multiple candidate repair paths, the eligible repair paths (having all attributes common) are distributed among the prefixes to provide load sharing. [9]

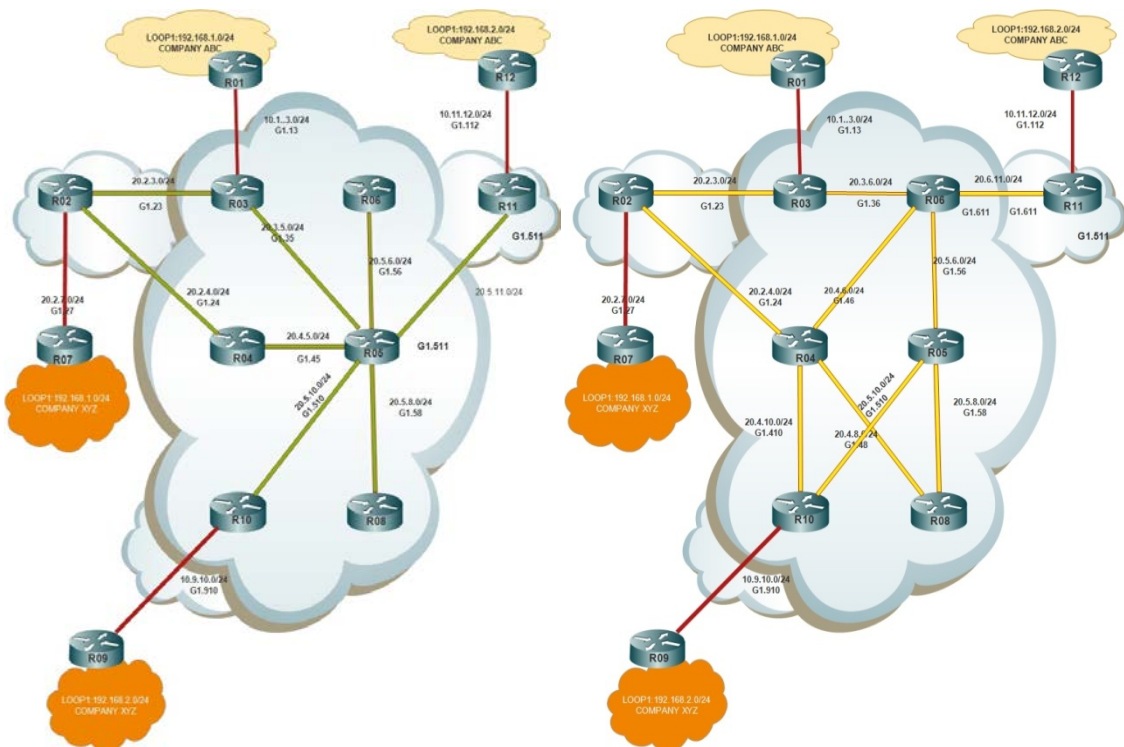
Per-link LFA protection examines the directly connected routers of the source router to determine whether a packet can be forwarded to another neighboring router without that neighbor in turn sending it back and forming a temporary routing loop while the underlying IGP converges. [9]

MECHANISM FOR CALCULATION OF LOOP FREE ALTERNATES



NETWORK DIAGRAM 28 :FOR SHORTEST PATH AS ROOT FOR NETWORK CALCULATION(LINKS IN BLACK)

NETWORK DIAGRAM 29: SHORTEST PATH TREE(R11 AS ROOT FOR NETWORK CALCULATION(TREE CALCULATION(LINKS IN YELLOW)



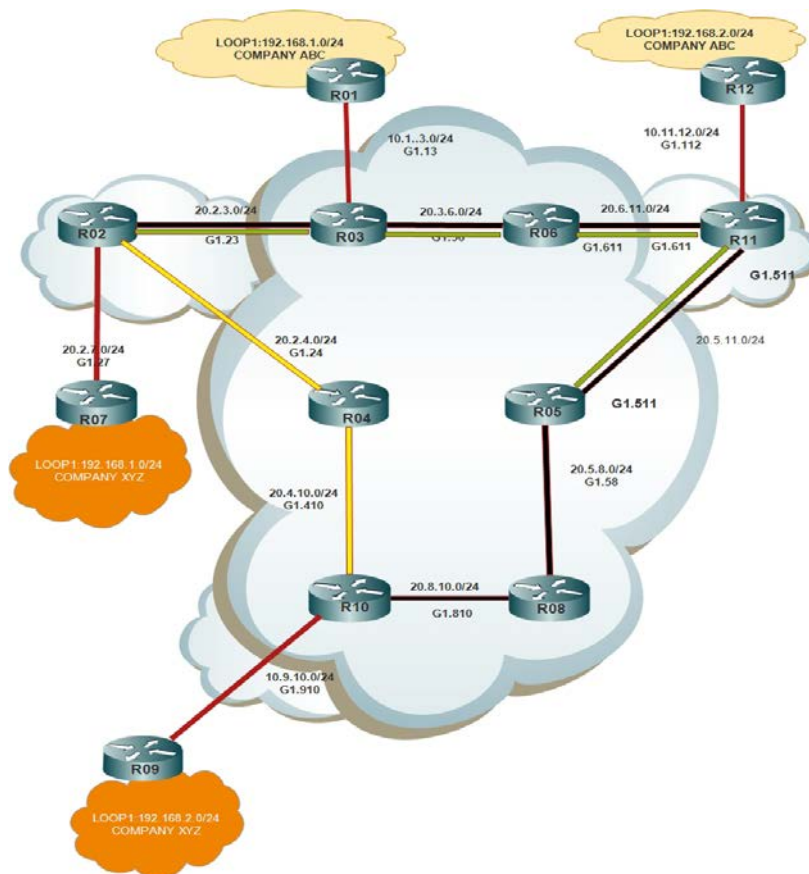
Network Diagram 30: R11 Calculating rSPF With R05 As Root

Network Diagram 31: R11 Calculating rSPF With R06 As Root

NOTE: IN LFA ROOT R11 CALCULATE rSPF WITH ITS NEIGHBORING ROUTERS AS ROOT FOR PRECOMPUTING REPAIR PATHS

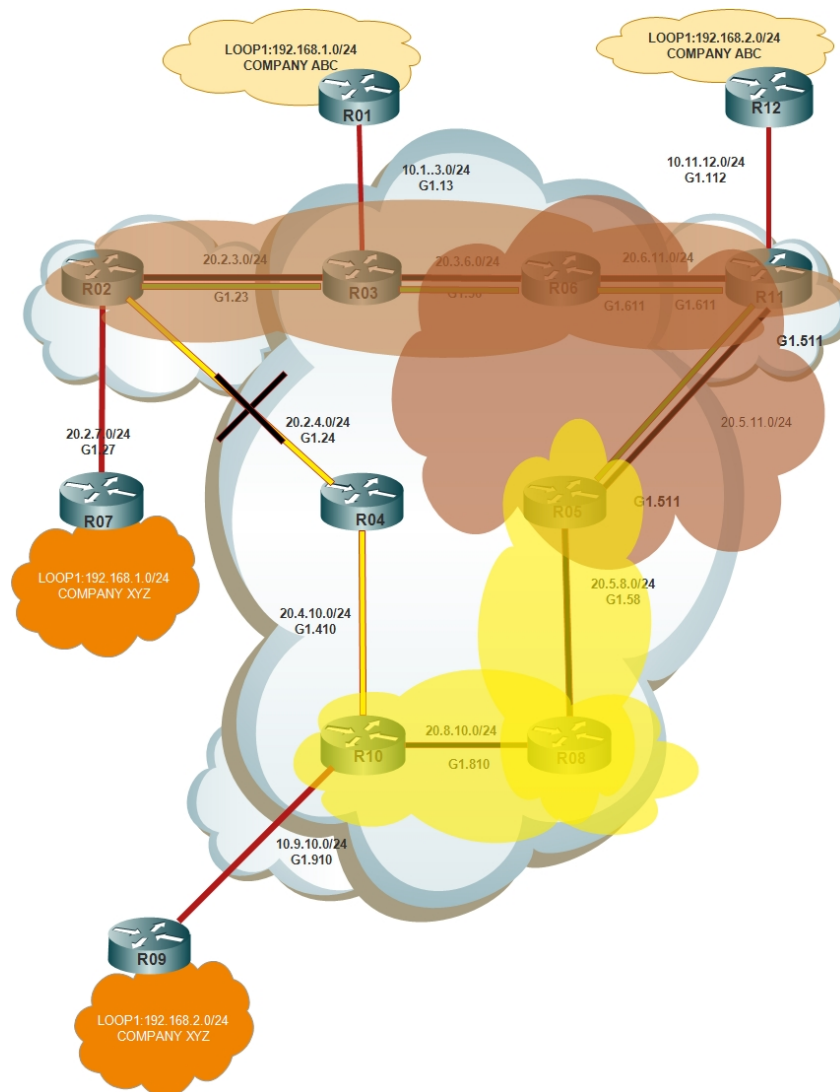
Remote Loop Free Alternate Fast Re-Route

The LFA-FRR is a mechanism that provides local protection for traffic, some topologies require protection that is not provided by LFA FRR. The Remote LFA FRR extends the basic behavior of LFA FRR by forwarding the traffic around a failed node to a remote LFA that can be more than one hop away. In Remote LFA FRR, a node dynamically computes its LFA(PQ) node (by finding nodes that are common to P-Space and Q-Space). After determining the repairing node (repairing node is not directly connected to repair path calculating node), the node establishes a directed Label Distribution Protocol (LDP) session to the repairing node (Repairing node should allow targeted LDP hello). The targeted LDP session exchanges labels over the tunnel for the prefixes that are to be protected. When the link fails, the node uses label stacking to tunnel the traffic to the remote LFA node, to forward the traffic to the destination. The Network Diagram shows the repair path (shown in black links) that is automatically created by the Remote LFA-FRR (R02 to R05) feature to bypass looping (that occurs if packet by router R02 is forwarded to R03 or R06). In Network Diagram, the traffic is flowing between CE nodes (R07 to R09) through the PE nodes (protected link - R02 and R04). When the link fails (R02--R04), the repair path (R02 - R03 - R06 - R11 - R05 - R08 - R10) is used to route the traffic between PE nodes using tunnel from R02 to R05. [23][2][9]



NETWORK DIAGRAM 32: SHOWS PRIMARY PATH(YELLOW LINKS) TRAFFIC FORWARDED OVER THE REPAIR PATH(BLACK LINKS) USING TUNNEL FROM R02 TO R05(GREEN LINKS)

REMOTE LFA MECHANISM TO FIND THE TUNNEL END POINTS



NETWORK DIAGRAM 33: SHOWS P-SPACE COMPUTED BY R02(IN BROWN) AND Q-SPACE(IN YELLOW) COMPUTED BY R10 WHEN LINK BETWEEN R02 AND R04 BREAKS

In this R02 is the source router(S) and R10 is the destination router(D). When the link between R02 and R04 breaks then R02 and R10 compute P-Space(It is the set of routers that S can reach without passing link R02 and R04) and Q space(It is the set of routers D can reach without passing link R02 and R04) respectively. All routers under brown color are P-space routers and all routers under yellow color are Q-space routers.

If the link R02 and R04 breaks ,if R02 forwards packet to R03 then it will not reach destination until network converges for IS-IS protocol and R03 will pass packet to R02 creating the loop until network converges, similarly R06 will forward packet back to R03 and then to R02 creating loop until network converges by IS-IS protocol.

P-space and Q-space helps in finding routers that have access to both routers S and D without passing through the failed link, that router which has access to both S and D is called PQ router(Intersection of P-space and Q-space which is R05 in lab topology) ,when packet is passed from source(R02) to PQ router(R05), then PQ router will forward it to the destination

without passing it back to the source router(R02) .[23][2][9]

```

R7#traceroute 9.9.9.9
Type escape sequence to abort.
Tracing the route to 9.9.9.9
VRF info: (vrf in name/id, vrf out name/id)
 1 10.2.7.2 4 msec 1 msec 1 msec
 2 20.2.4.4 [MPLS: Labels 402/10020 Exp 0] 3 msec 1 msec 10 msec
 3 10.9.10.10 [MPLS: Label 10020 Exp 0] 20 msec 20 msec 20 msec
 4 10.9.10.9 20 msec * 2 msec
R7#traceroute 9.9.9.9
Type escape sequence to abort.
Tracing the route to 9.9.9.9
VRF info: (vrf in name/id, vrf out name/id)
 1 10.2.7.2 7 msec 1 msec 9 msec
 2 20.2.3.3 [MPLS: Labels 312/10020 Exp 0] 8 msec 4 msec 12 msec
 3 20.3.6.6 [MPLS: Labels 610/10020 Exp 0] 31 msec 31 msec 31 msec
 4 20.6.11.19 [MPLS: Labels 11006/10020 Exp 0] 31 msec 31 msec 31 msec
 5 20.5.11.5 [MPLS: Labels 500/10020 Exp 0] 37 msec 31 msec 31 msec
 6 20.5.8.8 [MPLS: Labels 805/10020 Exp 0] 31 msec 31 msec 31 msec
 7 10.9.10.10 [MPLS: Label 10020 Exp 0] 16 msec 15 msec 22 msec
 8 10.9.10.9 19 msec * 4 msec
R7#

```

TRACEROUTE SHOWS FLOW OF TRAFFIC BEFORE FAILURE OF LINK BETWEEN R04 AND R02 AND FLOW OF TRAFFIC AFTER FAILURE OF THE LINK BETWEEN R04 AND R02

```

R2#show ip int br
Interface                IP-Address      OK? Method Status Protocol
GigabitEthernet1         unassigned      YES NVRAM  up       up
GigabitEthernet1.12     unassigned      YES manual deleted   down
GigabitEthernet1.20     unassigned      YES NVRAM  deleted   down
GigabitEthernet1.23     20.2.3.2        YES manual  up        up
GigabitEthernet1.24     20.2.4.2        YES manual  up        up
GigabitEthernet1.25     unassigned      YES NVRAM  deleted   down
GigabitEthernet1.26     unassigned      YES NVRAM  deleted   down
GigabitEthernet1.27     10.2.7.2        YES manual  up        up
GigabitEthernet1.28     unassigned      YES manual  deleted   down
GigabitEthernet1.210   unassigned      YES manual  deleted   down
GigabitEthernet2        192.168.1.2     YES NVRAM  up        up
GigabitEthernet2.28    unassigned      YES unset  deleted   down
Loopback0                2.2.2.2         YES manual  up        up
MPLS-Remote-Lfa39        20.2.4.2        YES unset  up        up
MPLS-Remote-Lfa42        20.2.3.2        YES unset  up        up
R2#show ip route 10.10.10.10
Routing entry for 10.10.10.10/32
  Known via "isis", distance 115, metric 20, type level-2
  Redistributing via isis 1
  Last update from 20.2.4.4 on GigabitEthernet1.24, 00:00:17 ago
  Routing Descriptor Blocks:
  * 20.2.4.4, from 10.10.10.10, 00:00:17 ago, via GigabitEthernet1.24
    Route metric is 20, traffic share count is 1
    Repair Path: 5.5.5.5, via MPLS-Remote-Lfa42
R2#

```

TUNNEL INTERFACE CREATED BETWEEN R02 AND R05 (MPLS-Remote-Lfa FOR REMOTE LOOP FREE ALTERNATE)

```

R2#show isis fast-reroute remote-lfa tunnels
Tag 1 - Fast-Reroute Remote-LFA Tunnels:

MPLS-Remote-Lfa39: use Gi1.24, nexthop 20.2.4.4, end point 5.5.5.5
MPLS-Remote-Lfa42: use Gi1.23, nexthop 20.2.3.3, end point 5.5.5.5

```

TUNNEL CREATED BETWEEN R02 AND R05 FOR REMOTE LOOP FREE ALTERNATE

Advantages of Remote LFA-FRR[23][2][9]

1. Manual configuration required is very less as compared with MPLS-TE FRR.
2. No need to configure RSVP-TE as required in MPLS-TE FRR.
3. PQ node is selected dynamically.
4. Remote LFA-FRR supports the following:
 - i. Basic LFA-FRR
 - ii. IP, L2VPN, and L3VPN

MICRO-LOOPS

Micro-loops are short duration loops that is caused (failure of resources in the network) due to difference in updating speed of different routers in the network topology. This generally happens when source router converges , before other routers converge and hence some routers forward traffic based on the old forwarding table and some routers (mostly source router) forward traffic using new forwarding table. These loops are resolved when link state protocol convergences (first Shortest Path First happens)[23][2][9]

COMPARISON OF LOOP FREE ALTERNATE AND MPLS TE FAST-REROUTE.[23][2][9]

1)Repair path are calculated according to least cost whereas in MPLS-TE FRR repair path are manually configured keeping in mind different constraints like bandwidth guarantee and path control.

2)Loop Free Alternate don't provide path protection whereas MPLS-TE FRR provide path protection.

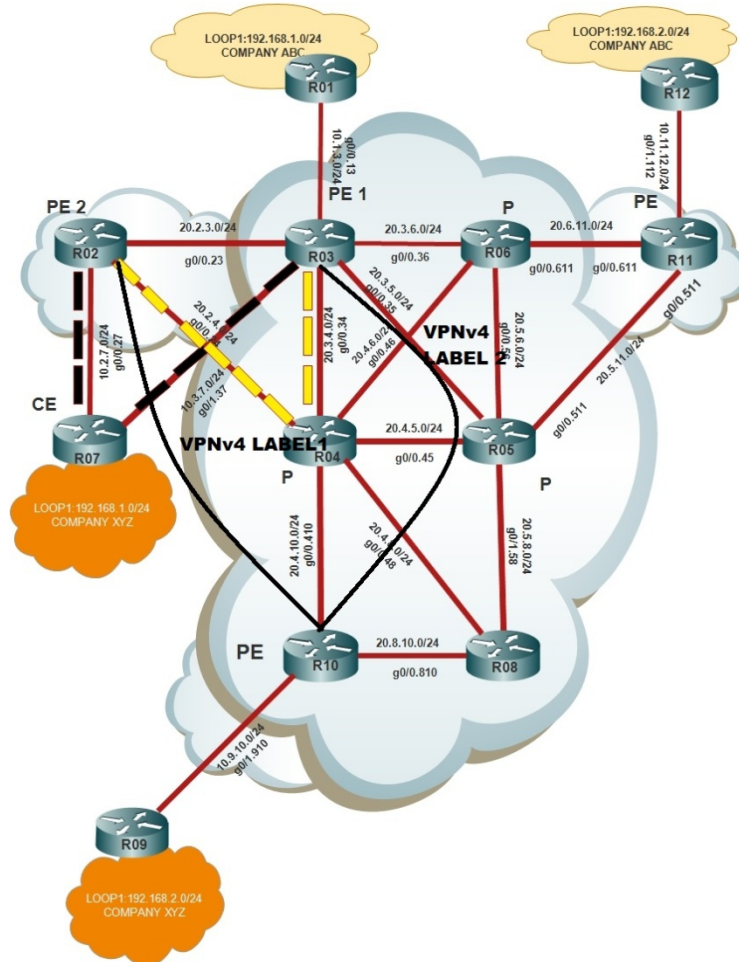
3)Control plane requirements for LFA are none whereas RSVP-TE is required for MPLS-TE FRR (Only configuration of Remote LFA need tunnels and targeted LDP HELLO, and requirement of enabling MPLS-LDP between source and destination of the tunnel)

COMPARISON OF LOOP FREE ALTERNATE AND RSVP-TE(shared by supervisor)

	LFA	RSVP-TE
Repair path	Least Cost	Constraint based with BW guarantee and path control
SRLG	Yes	Yes
Link Protection	Yes	Yes
Node Protection	Yes	Yes
Path Protection	No	Yes
Control Plain Requirements	None with LFA	RSVP-TE
Load Distribution over multiple paths	Yes	No
Provisioning Complexity	Minimal, if any	Significant
Topology dependency	Yes	No
BW Capacity Mgmt	No	Yes

CE-PE PROTECTION

In network any resource can failure ,ISP provide protection for failures in their network, so customer should not be worried about failure in core network but PE-CE link can also fail. To solve this issue CE can be made dual homed. In lab CE(R07) is dual homed to demonstrate PE-CE failure and recovery methodology. CE(R07) is dual-homed to PE1 and PE2. The primary LSP from remote end P(R04) ends on PE1, and the backup ends on PE2. An alternate path, set up with the required bandwidth guarantees, is available and can be used once the failure is detected. There is a single VPN, VPN XYZ, with two sites, 1 and 2. Traffic flowing from site 2(R10) towards site 1 is considered. Only site 1 is shown as dual-homed . Both PE1 and PE2 advertise 192.168.1.0/24 as a VPN route, and each of them also advertises



NETWORK DIAGRAM 34:SHOW R07 IS DUAL HOMED AT R02 AND R03 FOR PE-CE PROTECTION

the PE's loopback in LDP. As a result, PE(R10) has LDP LSPs to PE1 and PE2 and has two BGP routes for 192.168.1.0/24. PE(R10) performs path selection, and assuming it chooses PE1 as the more preferred path, it installs forwarding state corresponding to the VPN label received from PE1, and the LDP transport tunnel to PE1. Although the alternate path through PE2 is available, it remains unused on the remote PE(R10).When either PE1 or the link PE1-CE(R07) fails, to recover from a failure at PE1, PE(R10) must send the traffic on the LSP to PE2 so that it continues to reach destination CE(R07). [2][4][9]

If PE1 itself fails, PE(R10) learns of the failure via MP-BGP (through a route withdrawal).

PE(R10) knows that PE2 is an alternate exit point towards the destination CE(R07), as soon as it learns about the failure, it tells the forwarding plane to send traffic using the VPN tunnel and transport tunnel appropriate for PE2. [2][4][9]

SOLUTION 2:USE DIFFERENT ROUTE DISTINGUISHERS(RD)

By using two different RD at PE1 AND PE2 ,R10 will learn about CE(R07) from both PE1 and PE2 and will install both the routes. Hence when PE1 will fail R10 will be able to reach CE(R07) by PE2. [2][4][9]

```

R10#show ip bgp vpnv4 all
BGP table version is 162, local router ID is 10.10.10.10
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale, m multipath, b backup-path, x best-external, f RT-Filter
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop        Metric LocPrf weight Path
Route Distinguisher: 2:2 (default for vrf XYZ)
*>i 7.7.7.7/32      3.3.3.3         0      100      0 i
*>i 7.7.7.7/32      2.2.2.2         2      100      0 ?
*>y 9.9.9.9/32      10.9.10.9       2              32768 ?
*>y 10.2.7.0/24     2.2.2.2         0      100      0 i
*>y 10.3.7.0/24     3.3.3.3         0      100      0 i
*>y 10.9.10.0/24    0.0.0.0         0              32768 i
*>y 192.168.1.0     3.3.3.3         0      100      0 i
*>y 192.168.2.0     2.2.2.2         2      100      0 ?
*>y 192.168.2.0     10.9.10.9       2              32768 ?
Route Distinguisher: 3:2
*>i 7.7.7.7/32      3.3.3.3         0      100      0 i
*>i 10.3.7.0/24     3.3.3.3         0      100      0 i
*>i 192.168.1.0     3.3.3.3         0      100      0 i
  
```

R10 HAS TWO ROUTES TO 7.7.7.7/32

```

R8#show ip bgp vpnv4 all
BGP table version is 219, local router ID is 8.8.8.8
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
               x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

   Network          Next Hop        Metric LocPrf weight Path
Route Distinguisher: 1:1
*>y i 1.1.1.1/32     3.3.3.3         2      100      0 ?
*>y i 10.1.3.0/24    3.3.3.3         0      100      0 i
*>y i 10.11.12.0/24  11.11.11.11     0      100      0 i
*>y i 12.12.12.12/32 11.11.11.11     2      100      0 ?
*>y i 192.168.1.0    3.3.3.3         2      100      0 ?
*>y i 192.168.2.0    11.11.11.11     2      100      0 ?
Route Distinguisher: 2:2
*>y i 7.7.7.7/32     2.2.2.2         2      100      0 ?
*>y i 9.9.9.9/32     10.10.10.10     2      100      0 ?
*>y i 10.2.7.0/24    2.2.2.2         0      100      0 i
*>y i 10.9.10.0/24   10.10.10.10     0      100      0 i
*>y i 192.168.1.0    2.2.2.2         2      100      0 ?
*>y i 192.168.2.0    10.10.10.10     2      100      0 ?
Route Distinguisher: 3:2
*>y i 7.7.7.7/32     3.3.3.3         0      100      0 i
*>y i 10.3.7.0/24    3.3.3.3         0      100      0 i
*>y i 192.168.1.0    3.3.3.3         0      100      0 i
R8#
R8#
  
```

TWO SEPERATE ROUTE DISTINGUISHERS FOR 7.7.7.7/32

RECENT WORK IN MPLS TRAFFIC ENGINEERING

Resource Reservation Protocol-Traffic Engineering (RSVP-TE) Path Diversity using Exclude Route(reference [12] draft-ietf-teas-lsp-diversity-01.txt)

This draft discuss about Path diversity for multiple connections in Service Provider. Diversity constraints ensure that Label-Switched Paths (LSPs) can be established without sharing resources, thus greatly reducing the probability of simultaneous connection failures.[12]

RSVP-TE Signaling Procedure for End-to-End GMPLS Restoration and Resource Sharing(reference [13] draft-ietf-teas-gmpls-resource-sharing-proc-01)

This draft discuss about transport networks, where there are requirements that Generalized Multi-Protocol Label Switching (GMPLS) end-to-end recovery scheme needs to employ restoration Label Switched Path (LSP) while keeping resources for the working and/or protecting LSPs reserved in the network after the failure occurs.[13]

This document reviews how the LSP association is to be provided using Resource Reservation Protocol - Traffic Engineering (RSVP-TE) signaling in the context of GMPLS end-to-end recovery scheme when using restoration LSP where failed LSP is not torn down. This document clarifies the RSVP-TE signaling procedure to support resource sharing-based setup and teardown of LSPs as well as LSP reversion. No new extensions are defined by this document, and it is strictly informative in nature.[13]

YANG Data Model for TE Topologies(reference [14] <https://tools.ietf.org/html/draft-liu-teas-yang-te-topo-01>)

This draft discuss about YANG [RFC6020],it is a data definition language that was introduced to define the contents of a conceptual data store that allows networked devices to be managed using NETCONF [RFC6241]. YANG is proving relevant beyond its initial confines, as bindings to other interfaces (e.g. ReST) and encoding other than XML (e.g. JSON) are being defined. YANG data models can be used as the basis of implementation for other interface, such as CLI and programmatic APIs. This document defines a YANG data model for representing and manipulating TE Topologies. This model contains technology agnostic TE Topology building blocks that can be augmented and used by other technology-specific TE Topology models.[14]

A YANG Data Model for Traffic Engineering Tunnels and Interfaces(reference [16] draft-saad-teas-yang-te-01)

This document defines a YANG data model for the configuration and management of Traffic Engineering (TE) interfaces and tunnels. The model defines generic data that is reusable across multiple data and control plane protocols.[16]

The data model covers the configuration, operational state, remote procedural calls, and event notifications data for TE data. The goal of this document is to define a TE data model that can represent such different implementations, while adhering to standard terminology and behavior when resolving differences in implementations.[16]

MPLS / TE Model for Service Provider Networks draft-openconfig-mpls-consolidated-model-00(reference [18] <https://tools.ietf.org/html/draft-openconfig-mpls-consolidated-model-00>)

The focus area of the first version of the model is to set forth a framework for MPLS, with hooks into which information specific to various signaling-protocols can be added. The framework is built around functionality from a network operator perspective rather than a signaling protocol-centric approach. For example, a traffic-engineered LSP will have configuration relating to its path computation method, regardless of whether it is signaled with RSVP-TE or with segment routing. Thus, rather than creating separate per-signaling protocol models and trying to stitch them under a common umbrella, this framework focuses on functionality, and adds signaling protocol-specific information under it where applicable.[18]

Framework for Abstraction and Control of Transport Networks(reference [20] draft-ceccarelli-actn-framework-07.txt)

Transport networks have a variety of mechanisms to facilitate separation of data plane and control plane including distributed signaling for path setup and protection, centralized path computation for planning and traffic engineering, and a range of management and provisioning protocols to configure and activate network resources. These mechanisms represent key technologies for enabling flexible and dynamic networking.[20]

Transport networks in this draft refer to a set of different type of connection-oriented networks, primarily Connection-Oriented Circuit Switched (CO-CS) networks and Connection-Oriented Packet Switched (CO-PS) networks. [20]

One of the characteristics of these network types is the ability of dynamic provisioning and traffic engineering such that resource guarantees can be provided to their clients.[20]

One of the main drivers for Software Defined Networking (SDN) is a decoupling of the network control plane from the data plane. This separation of the control plane from the data plane has been already achieved with the development of MPLS/GMPLS [GMPLS] and PCE [PCE] for TE-based transport networks. One of the advantages of SDN is its logically centralized control regime that allows a global view of the underlying network under its control. Centralized control in SDN helps improve network resources utilization from a distributed network control. For TE-based transport network control, PCE is essentially equivalent to a logically centralized control for path computation function.[20]

Two key aspects that need to be solved by SDN are:

1. Network and service abstraction[20]
2. End to end coordination of multiple SDN and pre-SDN domains e.g. NMS, MPLS-TE or GMPLS.[20]

RSVP-TE Scalability - Recommendations (reference [21] draft-beeram-mpls-rsvp-te-scaling-01)

RSVP-TE [RFC3209] describes the use of standard RSVP [RFC2205] to establish Label Switched Paths (LSPs). As such, RSVP-TE inherited some properties of RSVP that adversely affect its control plane scalability. Specifically these properties are (a) reliance on periodic refreshes for state synchronization between RSVP neighbors and for recovery from lost RSVP messages, (b) reliance on refresh timeout for stale state cleanup, and (c) lack of any mechanisms by which a receiver of RSVP messages can apply back pressure to the sender(s)

of these messages.[21]

Subsequent to [RFC2205] and [RFC3209] further enhancements to RSVP and RSVP-TE have been developed. In this document discussion is done about how an implementation of RSVP-TE can use these enhancements to address the above mentioned properties to improve RSVP-TE control plane scalability.[21]

RSVP Setup Retry - BCP (reference [22] draft-ravisingh-teas-rsvp-setup-retry-00

In an RSVP-TE network with a very large number of LSPs, link/node failure(s) may produce a noticeable increase in RSVP-TE control traffic. As a result, RSVP-TE messages might get delayed by virtue of being stuck in a queue that is overwhelmed with messages to be sent or they might get lost forever. For example, a Path message intended to be sent by a transit router might be stuck in the output queue to be sent to the next-hop. Alternately, it might have got dropped on the receive side due to queue overflows. The same could happen for a Resv message in the reverse direction. Also, in the absence of reliable delivery of Path-Error messages [RFC2961], an error that gets generated at transit/egress for an LSP that is in the process of being setup may never make it to the ingress.[22]

Lost/delayed RSVP-TE messages cause the following problems for an ingress router:[22]

In the absence of an error indication, how is an ingress to know that an LSP for which signaling was (re-)initiated and a Resv has not yet been received, is ever going to come up?[22]

In the absence of any indication, what action should the ingress take to support low-latency LSP-setup?[22]

The above problems essentially boil-down to: how long should the ingress continue to wait before giving up on its attempt to bring up the LSP, and take some alternative course of action (e.g., try to bring up the LSP on an alternate path)?. To mitigate this problem, some implementations use a setup-retry timer mechanism. This document discusses the issues associated with a particular implementation of this timer and makes some specific recommendations to get around these issues.[22]

CONCLUSION

The project helped in analysis and design of different protection and restoration techniques that are used in MPLS networks.

For lab demonstration Layer 3 VPN was used between customers ABC and XYZ sites, and analysis was done on the path followed by the packets when no traffic engineering was implemented, which resulted in some of the paths being over utilized and some underutilized. To overcome this problem traffic engineering was implemented for both companies traffic and in both directions (traffic going and traffic coming for the different sites), which resulted in the optimal utilization of the networking resources. To achieve optimal traffic engineering detailed analysis of different signaling protocols was done that includes RSVP-TE, LDP, MP-BGP.

Due to dynamic nature of Internet, resources fails but due to convergence of voice, video streaming and data into one composite network, information loss and delay is not acceptable; therefore the traffic on the MPLS network needs to be protected against network failures. In this lab work all the protection techniques including path protection and local protection, loop free alternate fast re-route were discussed. In local protection all the 4 local protection techniques were discussed in detail and advantages and disadvantages of each techniques were discussed. Therefore I personally think that the objective of the project is accomplished. Further research could be done to find the efficiency of different protection techniques that were used for MPLS networks using different cases, rerouting patterns and packet drop during the switchover from primary LSP to backup LSP in case of facility protection and to detours in case of 1:1 protection can be tested and analyses using different test patterns.

FUTUTE WORK

1. Impact of Transport Optical Network on MPLS restoration.
2. The efficiency of different protection techniques that were used for MPLS networks using different test cases can be performed.
3. Rerouting patterns and packet drop during the switchover from primary LSP to backup LSP in case of facility protection and to detours in case of 1:1 protection can be analyzed using different test patterns.

REFERENCES

- 1) http://etd.lsu.edu/docs/available/etd-04122005-160920/unrestricted/Aniker_thesis.pdf
- 2) MPLS-Enabled Applications: Emerging Developments and New Technologies, Third Edition
- 3) http://www.h3c.com/portal/res/200705/31/20070531_107755_MPLS%20Basics%20Introduction_201197_57_0.pdf
- 4) 2002 Cisco Press book, "Advanced MPLS Design and Implementation" by Vivek Alwayn
- 5) <http://tools.ietf.org/html/draft-ietf-teas-lsp-diversity-01>
- 6) <http://www.hit.bme.hu/~jakab/edu/litr/MPLS/mplsprotwp2.pdf>
- 7) <http://www.ietf.org/download/id-abstract.txt>
- 8) <http://img.lightreading.com/2001/12/opticalmplswhitepaper.pdf>
- 9) Cisco Press IP Routing on Cisco IOS, IOS XE, and IOS XR: An Essential Guide to Understanding and Implementing IP Routing Protocols by Ramiro Garza Rios, Aaron Foss, Brad Edgeworth
- 10) <http://www.watersprings.org/pub/id/draft-makam-mpls-protection-00.txt>
- 11) Cisco Press MPLS Fundamentals By Luc De Ghein
- 12) <https://tools.ietf.org/html/draft-ietf-teas-lsp-diversity-01>
- 13) <https://tools.ietf.org/html/draft-ietf-teas-gmpls-resource-sharing-proc-01>
- 14) <https://tools.ietf.org/html/draft-liu-teas-yang-te-topo-01>
- 15) http://mynetworkingwiki.com/index.php/Types_of_Protection_for_MPLS_TE
- 16) <https://tools.ietf.org/html/draft-saad-teas-yang-te-01>
- 17) <http://datatracker.ietf.org/doc/draft-ietf-mpls-rsvp-egress-protection/>
- 18) <https://tools.ietf.org/html/draft-openconfig-mpls-consolidated-model-00>
- 19) http://publications.theseus.fi/bitstream/handle/10024/59339/Peter_Kimani.pdf?sequence=1
- 20) <https://tools.ietf.org/html/draft-ceccarelli-actn-framework-07>
- 21) <https://tools.ietf.org/html/draft-beeram-mpls-rsvp-te-scaling-01>
- 22) <https://tools.ietf.org/html/draft-ravisingh-teas-rsvp-setup-retry-00>
- 23) https://www.ciscolive.com/online/connect/sessionDetail.wv?SESSION_ID=76557&tclass=popup
- 24) <https://tools.ietf.org/html/rfc4364>

25) <https://tools.ietf.org/html/rfc5462>

26) <http://www.rfc-editor.org/info/rfc3031>

27) <http://www.rfc-editor.org/info/rfc5036>

28) <http://www.rfc-editor.org/info/rfc3209>

29) Traffic Engineering with MPLS By Eric Osborne, Ajay Simha

30) http://www.okena.com/en/US/products/hw/routers/ps368/prod_bulletin09186a00802849a4.html (http://newsroom.cisco.com/dlls/corp_012403.html)