Lab 7
TLEN 5460 – TELECOMMUNICATIONS SYSTEMS LABORATORY
MPLS, LDP & RSVP

Summer 2014

Introduction

Multi-Protocol Label Switching (MPLS) uses labels to forward packets to their destination completely avoiding a Routing Table lookup at the Routers. The labels are assigned by the router and have a local significance to the router generating it. Different traffic flows can be assigned labels based on source, destination IP addresses QoS bits etc. and are forwarded through the MPLS domain based on these labels. Thus, only the edge router in a MPLS Network needs to do a Routing Table lookup. All routers in the core can forward traffic by looking up the label in the MPLS header at ingress and inserting a new label at egress. These different paths through a MPLS network are called Label Switched Paths

(LSPs). LSP's in MPLS allow a service provider to perform traffic engineering and monitor different flows in the network allowing more flexibility and easy management than IP Routing Protocols. The downstream router tells the upstream router to use a specific label for a set of packets based on certain criteria which can be defined by the administrator. Every router in the MPLS domain swaps the label before forwarding it to the next router. This process continues till the edge router receives the packets, at which point it strips the label and does a Routing Table lookup to determine the next hop.

Terminology

The following terms are important to understand the working of MPLS. The definitions provided are as per RFC3031.

Forwarding equivalence class (FEC): A group of IP packets which are forwarded in the same manner (e.g. over the same path, with the same forwarding treatment)

Label: A short fixed length physically contiguous identifier which is used to identify a FEC, usually of local significance.

Label swap: The basic forwarding operation consisting of looking up an incoming label to determine the outgoing label, encapsulation, port, and other data handling information.

Label swapping: A forwarding paradigm allowing streamlined forwarding of data by using labels to identify classes of data packets which are treated indistinguishably when forwarding.

Label switched hop: The hop between two MPLS nodes, on which forwarding is done using labels.
Label Switched Path (LSP): The path through one or more LSRs at one level of the hierarchy followed by a packets in a particular FEC.

Label switching router (LSR): An Router which forwards packets depending on the label received in the MPLS header.

MPLS domain: A contiguous set of nodes which operate MPLS routing and forwarding and which are also in one Routing or Administrative Domain

Edge Router: An MPLS Edge Router connects an MPLS domain with a Router which is outside of the domain, either because it does not run MPLS, and/or because it is in a different domain. If an LSR has a neighboring host, which is not running MPLS, then that LSR is an MPLS edge Router.

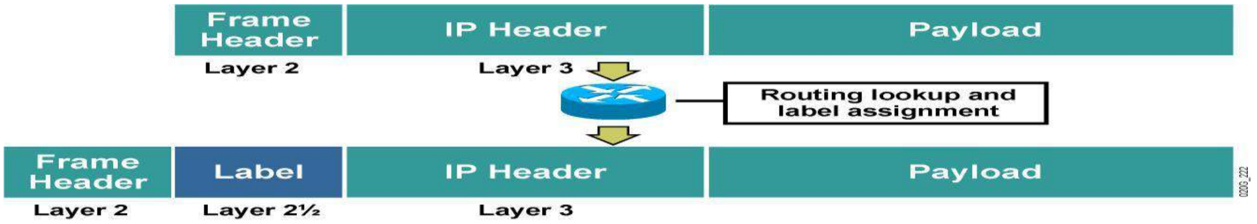
MPLS egress node: An MPLS edge node in its role in handling traffic as it leaves an MPLS domain.
MPLS ingress node: An MPLS edge node in its role in handling traffic as it enters an MPLS domain.
Label Distribution Protocol (LDP): A protocol used to distribute labels between neighbors.

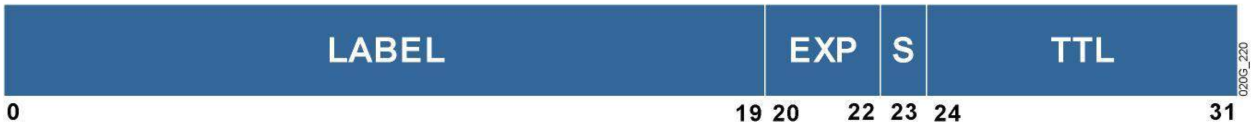
Resource Reservation Protocol (RSVP): A protocol used to reserve resources such as bandwidth along the LSP.

Push and Pop: The possible label operations are swap, push, and pop. By looking at the top label of the received labeled packet and the corresponding entry in the LFIB, the LSR knows how to forward the packet. The LSR determines what label operation needs to be performed—swap, push, or pop— and what the next hop is to which the packet needs to be forwarded. The swap operation means that the top label in the label stack is replaced with another, and the push operation means that the top label is replaced with another and then one or more additional labels are pushed onto the label stack. The pop operation means that the top label is removed.

MPLS Labels

A MPLS domain consists of Routers which are able to switch or route packets based on labels inserted between the Layer 2 and Layer 3 headers of a Packet. The MPLS header is 32 bits long and has a 20bit long label. The following figure shows a standard MPLS header.



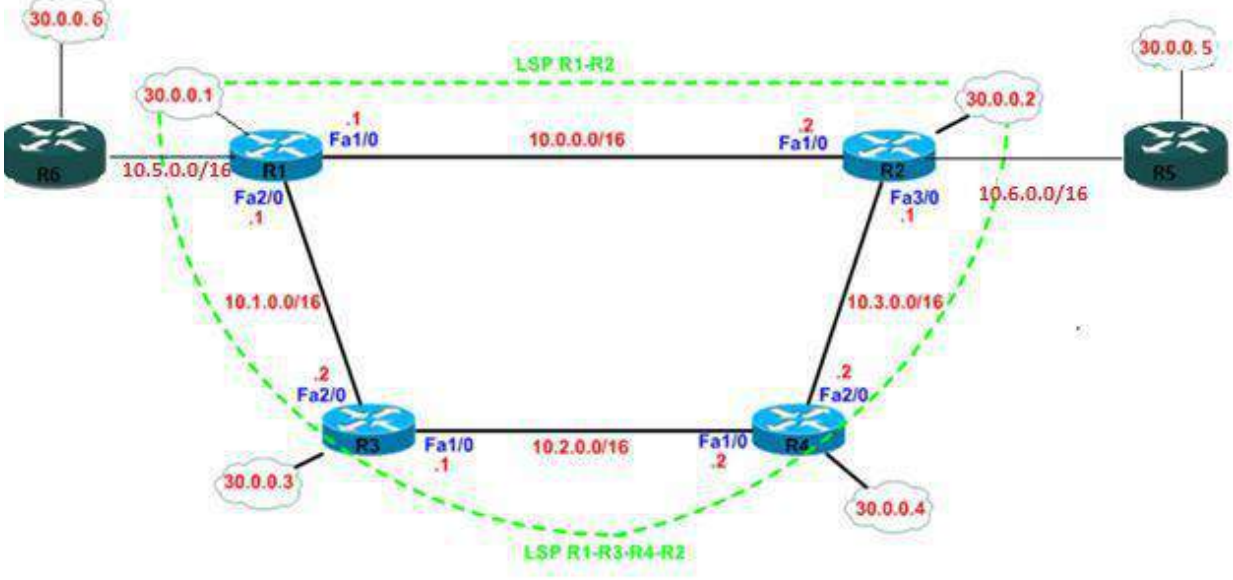


The Network

This lab setup uses the network as shown in the figure below. We create several Label Switched Paths (LSP) through the network by using traffic engineering tunnels and divert traffic through a path other than the one chosen by the traditional Routing Protocols. We also look at the convergence of the network after a link on a LSP goes down.

Network Diagram

Routers R3 and R4 are your core routers (P) that perform only label switching. Routers R6, R5, R1 and R2 are your provider edge (PE) routers that are responsible for label imposition. They perform both MPLS label switching and IP routing. **Assume that the link between routers R1 and R2(10.0.0.0/16) traverses the northern part of the U.S and the link between R1-R3-R4-R2 traverses the southern part of the U.S**. Make appropriate provisions for placing sniffer stations between the links R6-R1, R1-R2 and R3-R4 on the MPLS domain. Paste relevant configuration snippets wherever possible to support your answers. Answers without configuration snippets will not be considered.



Objective 1: Understanding LDP operation:

Step 1

Don't create loop back interfaces yet! Assign the physical interface IP addresses as given in the topology on all the six routers.

Step2

Enable MPLS and LDP on all
routers. In the global config mode,

mpls label protocol ldp
mpls ip
ip cef

In the interface config
mode, *mpls ip*

Step 3

Do not run any static or dynamic routing protocol.

Questions:

1) Explain the commands used in step2.

2) Did any of the routers form LDP neighbors? If so, mention the routers that are LDP neighbors.

Useful Commands:
sh mpls ldp discovery
sh mpls ldp neighbor

3) Explain why other routers could not form LDP neighbors. (Hint: Check the LDP ID's used by each of the router and the reachability to the LDP ID's)

4) Explain how LDP neighbors are discovered and maintained with necessary logs. Include protocol messages, transport protocol and port numbers. (Hint: debug mpls ldp and wireshark would suffice)

5) How can you achieve all the LDP neighborships in the topology? Do you need a routing protocol to achieve it?

Step 4

Now create loopback interfaces as mentioned in the topology and enable MD5 authentication between all LDP neighbors.

Step 5

Enable an optimal routing protocol to achieve end to end connectivity. You need to perform label switching and MPLS Traffic Engineering.

Questions:

6) What are the local and remote label bindings at R1? What is the start range of local bindings in cisco routers? How is the local label bindings advertised to neighbors? Show relevant debug output.

7) What is the remote label bindings at R2 and R3 for the network 30.0.0.1/32? Is it the same or different? Explain why ?

8) What label does R1 assign to the network 30.0.0.1? Does R2 use a label to forward packets to 30.0.0.1 on a steady state? Explain why or why not? (Hint: Compare "sh mpls forwarding table", "sh ip route" and "sh mpls ldp bindings"). Shut down the link between R1 and R2 and explain whether R2 would use labels to reach 30.0.0.1?

9) Bring up the link R1-R2. What is the outgoing label used by R4 to forward a packet to 30.0.0.1 network. How many label switched paths does R4 have to reach 30.0.0.1 network?

10) Does all the label bindings in the LIB go in to the LFIB table? Explain which mappings enter the LFIB table? Provide necessary logs to support your answer.

11) What is the current LDP hold time and keep alive interval? Paste relevant configuration snippets.

12) Ping 30.0.0.4 from R1 and answer the following questions.

i) How many label switched paths exist from R1 to reach 30.0.0.4? (Hint: sh ip route and sh mpls forwarding-table)

ii) Which path does your ping request use? Does it use both the paths? If not explain why?

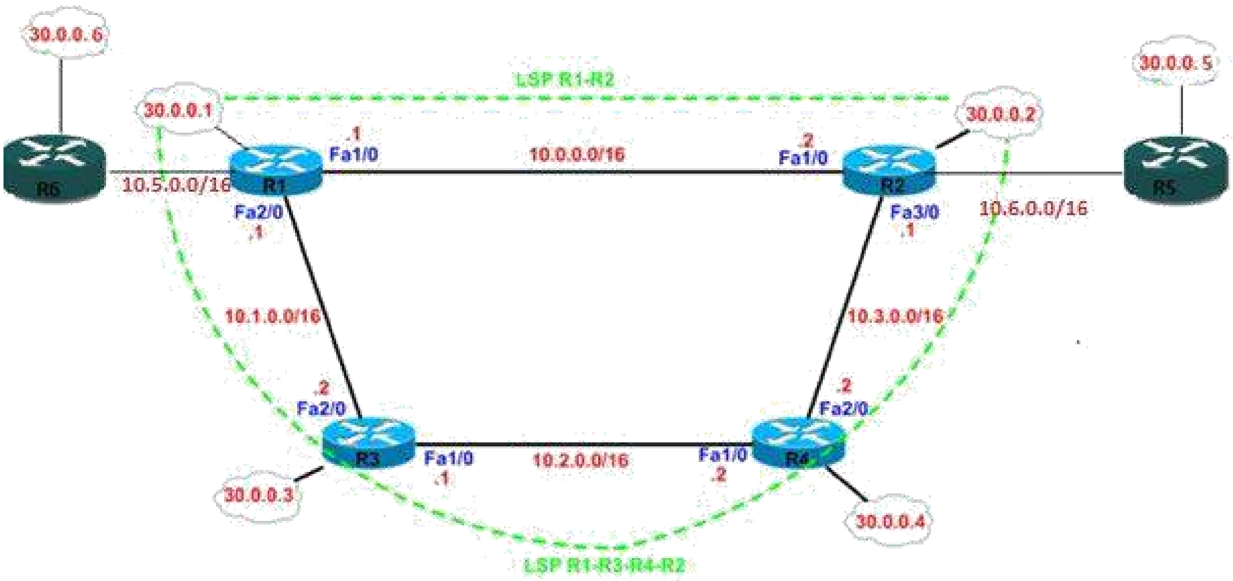
iii) Draw the LSP along with the labels used by each of the LSR's in the path.

iv) What is the penultimate router for the ping request you just sent? What operation did the penultimate router perform? (Swap/push/pop)

v) Is PHP (Penultimate hop popping) enabled by default?

vi) Is there a counter to see how many bytes of packet has been label switched? Paste relevant show commands.

13) Shut down any interface on R1 and no shut after a few seconds. Explain the sequence of events that occur. Is routing protocol convergence required before LDP neighbors can be formed?



Objective 2: Steps for configuring MPLS Traffic Engineering Tunnels (MPLS TE)

The above network diagram shows two LSP's from Router R1's loopback to Router R2's loopback interface. These LSP's are configured on Router R1 and are associated with a single tunnel interface to forward traffic through them using MPLS. We prefer the LSP traversing the southern path of the U.S over the northern path. This can be achieved using path options of the tunnel configuration. We will configure RSVP on all the interfaces, enable TE extension for OSPF and set the Router-ID on all routers for OSPF TE extensions.

NOTE: The below guide shows the configuration required for a creating a uni-directional TE tunnel from R1 to R2 named "Tunnel1" using two path options.

Step 1

Enable Cisco Express Forwarding as a first step to enable MPLS on the
routers. ip cef

Step 2

Enable MPLS Traffic engineering on all the routers. MPLS TE is enabled globally and on all the interfaces participating in the TE tunnel. Configuration is as shown below.

```
mpls traffic-eng tunnels
```

```
interface FastEthernet 1/0
mpls traffic-eng tunnels
```

Step 3

Enable TE extension for OSPF on all the routers R1-R6. TE expansions for OSPF need to be enabled to allow CSPF to calculate the best paths. OSPF uses LSA's of the type 10 to flood the TE metrics

```
router ospf 1
mpls traffic-eng area 0
```

Step 4

Set Router-id for TE extensions in OSPF

```
router ospf 1
mpls traffic-eng router-id Loopback<x>
```

Step 5

Create one explicit path from R1to R2 traversing the southern part. The explicit paths can be created from the global configuration mode. The paths need to be created only on the head end Router (R1 in this case).

In configuration mode:

For LSP1:

```
ip explicit-path name R1-R3-R4-R2(south) enable
next-address 10.1.0.2
next-address 10.2.0.2
next-address 10.3.0.1
```

For LSP 2:

We will use routing protocol to decide the best path by using “dynamic” path option. According to the routing protocol, what do you think is the best path to reach R2 from R1?

Step 6

Create a tunnel interface on the head end router (R1). The tunnel interface allows various LSP’s to be associated with it. The tail end of the tunnel is also specified as the destination. This is usually the loopback of the router at the egress of the tunnel. In this scenario R2 is the egress router.

```
interface Tunnel1
description Tunnel from Router R1 to Router
R2 tunnel destination 30.0.0.2
```

Step 7

Assign loopback interface as the source of tunnel interface. The tunnel interface is usually assigned the same addresses as the loopback interface to make the tunnel appear to originate from the loopback and terminate at the loopback of the other router.

```
interface Tunnel1
ip unnumbered Loopback<x>
```

Step 8

Enable MPLS traffic engineering on the Tunnel Interface

```
interface Tunnel1
tunnel mode mpls traffic-eng
```

Step 9:

Configure the tunnel to use both southern path and northern path, but preferring the southern path by setting different priorities. The explicit path created earlier in Step 5 are associated with the tunnel interface.

```
interface Tunnel1
tunnel mpls traffic-eng path-option 1 explicit name R1-R3-R4-
R2(south) tunnel mpls traffic-eng path-option 2 dynamic
```

Step 10

To specify that the Interior Gateway Protocol (IGP) should use the tunnel (if the tunnel is up) in its enhanced shortest path first (SPF) calculation, use the following command in the interface configuration mode. Without sepcifying “autoroute announce” on the tunnel interface, the tunnels would be signaled, but not used for routing automatically. Also record route is a useful option to see the exact details of the RSVP path and RSVP RESV messages.

```
interface Tunnel1
tunnel mpls traffic-eng autoroute announce
tunnel mpls traffic-eng record-route
```

Useful troubleshooting commands for tunnels:

```
sh mpls traffic-eng tunnels tunnel <tun no>
```

Once the tunnels are up and active, check whether the tunnels allow the traffic to pass through.
(Hint: Check the routing table for tunnel interface)

Questions:

1) Explain the useful parameters from the “sh mpls traffic-eng tunnels tunnel” output.

2) Although the tunnel’s head end is R1, does R4 know about the presence of TE tunnel 1? Explain with necessary logs.

3) Ping 30.0.0.5 from R1 and draw the LSP along with labels. Does this ping request use the traffic engineering tunnel? Confirm your findings using sniffers / configuration snippets. Show packet counters indicating the no of bytes label switched.

4) Ping 30.0.0.5 from R6 and draw the LSP along with labels. Does this ping request use the traffic engineering tunnel created in R1? Confirm your findings using sniffers / configuration

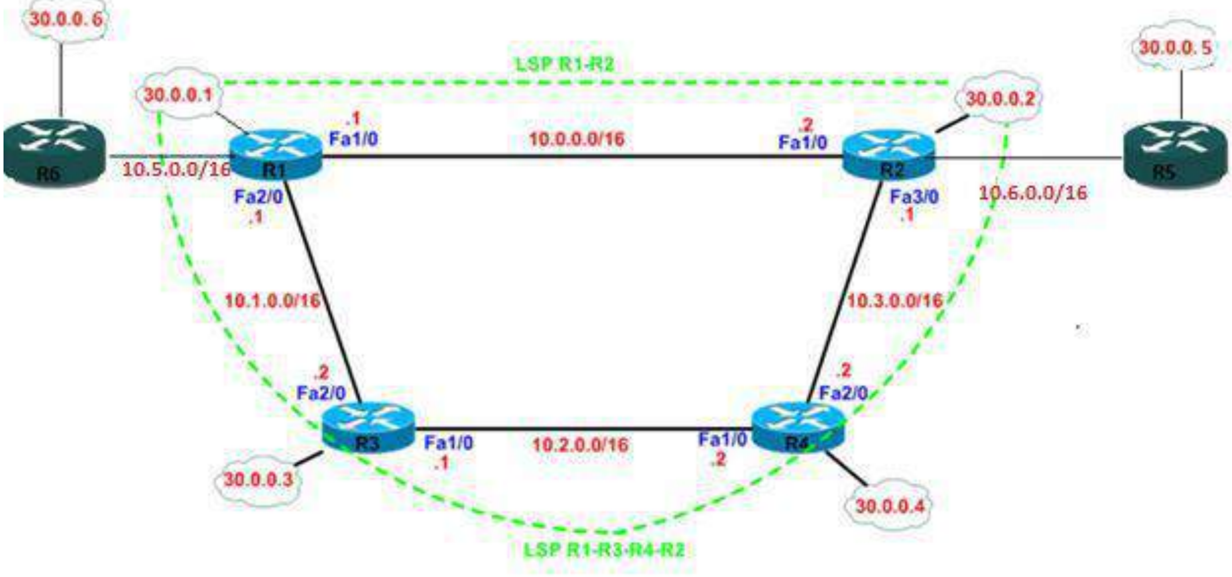
snippets. (If the ping doesn’t work, please troubleshoot by finding the point where the packet is dropped)

If you could not figure it out, ask your SA’s help by explaining them where the packet is dropped!

5) Explain the path used by ‘ping reply” used in the previous step (4) with appropriate label mappings. Does it use the TE tunnel you created?

6) Shut down one of the interfaces in R3 which is in the southern path of the tunnel. Since you have a second path option in your tunnel LSP, tunnel must be established via the northern path. Explain the sequence of events that occur after you shut down an interface in R3. Draw the new label switched path from R6 to R5. Does the label mappings change? Paste the necessary outputs to prove that the tunnel is signaled via the northern path.

7) Bring the interface up on R3 and check the tunnel’s path. Is the tunnel1 still signaled via the northern path or does it re-signal via the southern path. How can you ensure that the TE tunnel checks for optimal paths every 30 seconds and if a better path is available, it should re-signal the tunnel via that path? (Note: Remember that, for this network setup, southern path is always preferred than the northern path. So when any failures are recovered in the southern path, the LSP should be signaled via the southern path)



Objective 3: Understanding BANDWIDTH reservation and tunnel priorities:

The tunnel created in objective 2, doesn't reserve any bandwidth along the path. So let's reserve a guaranteed bandwidth along the LSP.

1) Reserve 20Mbps on all interfaces participating in MPLS TE for RSVP signaling. RSVP bandwidth to be reserved needs to be configured on all the participating interfaces.

```
interface FastEthernet1/0
ip rsvp bandwidth 20000
```

2) Let's request tunnel 1 to reserve 10Mbps along the LSP. Specify "tunnel 1" to reserve 10Mbps on the southern LSP.

```
int Tunnel1
tunnel mpls traffic-eng bandwidth 10000
```

3) Prove that the tunnel has a bandwidth reservation of 10Mbps and the path is via the southern part of your network.

4) Signal a longer hop, higher priority tunnel, "tunnel 10" requesting 15Mbps bandwidth from R6 to R2 via the southern path. Is there sufficient bandwidth available for this new tunnel? How can you ensure that tunnel 10 being a high priority tunnel, gets the necessary bandwidth, even though tunnel 1 was set up earlier? (Refer the configuration guide in the previous objective to signal the new tunnel from R6 and add the below command to configure this tunnel as a high priority tunnel)

```
int tun10
tunnel mpls traffic-eng priority 6 6
```

5) Once tunnel 10 is up (via the southern path), what happens to tunnel1?

6) Explain the significance of two values used in setting priorities of a tunnel10 in step 4.

Understanding global pool and sub pool bandwidth allocation

7) Revert all the bandwidth reservations made earlier to default settings. int fa<x/x>

```
no ip rsvp bandwidth
```

8) Create a global pool (that will be used for low priority tunnels) of 35 Mbps and a sub-pool derived from the global pool (that will be used by high priority tunnels) of 15 Mbps on all the interfaces.

```
int fa<x/x>
```

```
ip rsvp bandwidth XXXXXX sub-pool XXXXXXX
```

9) Signal Tunnel 1 to use 12 Mbps from global pool and tunnel 10 to use 13Mbps from the sub-pool. Ensure that both the tunnels use the southern path. Show relevant output to prove this.

10) Signal another tunnel, “tunnel 2” from R1 to R2 which requests 8Mbps and traverses the southern path.

11) Is the traffic from R1 to R5, load balanced between two TE tunnels “tunnel 1” and “tunnel 2”? Ping 30.0.0.5 from R1 and show which tunnel is used for the “ping request”. Ping 30.0.0.2 from R1 and show which tunnel is used for the “ping request”?

12) Signal another tunnel named “tunnel 3” requesting 20Mbps from R2 back to R1 via the southern path. Is there enough bandwidth available to accommodate this tunnel? At this point you must have the following tunnels up and active! Paste relevant output to prove.

TUNNEL #	SOURCE	DEST	BANDWIDTH(Mbps)	PATH
1	R1	R2	12	SOUTH
2	R1	R2	8	SOUTH
10	R6	R2	13	SOUTH
3	R2	R1	20	SOUTH

13) Ping 30.0.0.5 from R1 and explain the “ping request” and “ping reply” path with labels.

EXTRA CREDITS!!! (3 points)

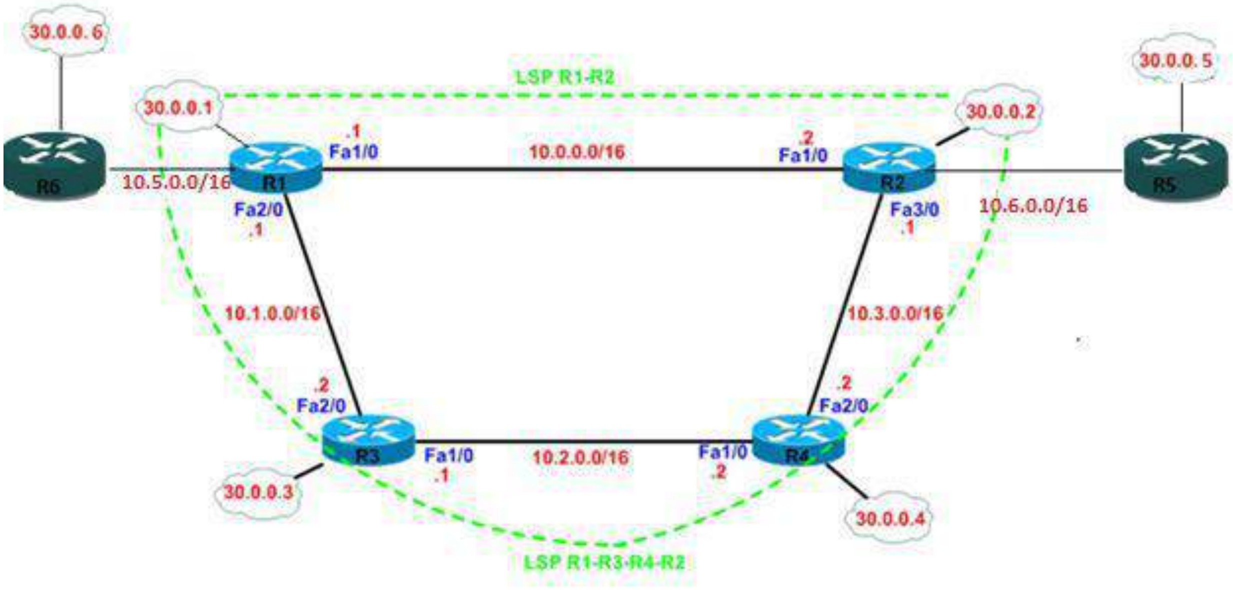
Disable Tunnel 10 and 2. Just enable Tunnel 1 and tunnel 3 in your network.

TUNNEL #	SOURCE	DEST	BANDWIDTH(Mbps)	PATH
1	R1	R2	12	SOUTH
3	R2	R1	20	SOUTH

1) Only bi-directional traffic between R6 and R5's loopback should use the TE tunnel. In other words, traffic destined to 30.0.0.5 from R6 should use TE tunnel 1. The return traffic destined to 30.0.0.6 from R5 should use TE tunnel 3. All the other traffic in your network should use IP routing and not label switching. Show necessary configuration changes and packet captures.

Verification:

a. Traceroute to 30.0.0.5 from R6 should show the labels used by tunnel 1
b. Traceroute to 30.0.0.6 from R5 should show the labels used by tunnel 3.
c. Traceroute to 30.0.0.2, 30.0.0.3 and 30.0.0.4 should not show any labels.
d. Show relevant packet captures!



Reading Materials: http://blinky-lights.org/networking/mpls.pdf

http://www.cisco.com/en/US/tech/tk436/tk428/technologies_q_and_a_item09186a00800949e5.shtml

http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/fsfrr24.html
http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6557/prod_presentation0900aecd80312051.pdf

http://www.ciscopress.com/articles/article.asp?p=680824
http://www.cs.vsb.cz/grygarek/TPS/MPLS/mpls_te.pdf