

IMPLEMENTATION AND REAL TIME PERFORMANCE OF MPLS NETWORK USING RSVP

M Chandra Kala¹, B Ganesh², Ch Narayana Rao³

¹M.Tech Student, ²Associate Professor, ³Assistant Professor
^{1,2}Gokul Institute of Tech & Sciences, ³Raghu Institute of technology

Abstract: *Transferring of the Data from source to destination we have used IP address which is a connectionless and each router has to make independent forwarding decisions based on IP address. It is a huge IP header requires minimum 20 bytes of memory. The routing process in Network layer and it is slower than switching usually designed to obtain shortest path. To minimize this problem The Multi-Protocol Label Switching (MPLS) combines the scalability of the IP protocol and the efficiency of label switching to improve network data circulation. The protection of data flows in the case of link or Node failures is very important, especially for real time services and multimedia applications. In this paper we used MPLS based network for fast recovery both cases of link and node failures. For executing the topology we are using GNS3.*

Keywords: *MPLS (Multi-Protocol Label Switching), RSVP (Resource Reservation Protocol), FEC, LFIBs, GNS3, Label-switched paths (LSPs), Label Switch Router (LSRs), Label Edge Router (LERs).*

I. INTRODUCTION

Now-a-days Data can be transferred over the internet by using IP addresses which is a complexity process which can be reduced data circulation.

Traffic Engineering: Traffic engineering allows a network administrator to make the path deterministic and bypass the normal routed hop-by-hop paths.

An administrator may elect to explicitly define the path between stations to ensure QoS or have the traffic follow a specified path to reduce traffic loading across certain hops. Traffic engineering, then, enables an administrator to define a policy for forwarding frames rather than depending upon dynamic routing protocols.

Traffic engineering is similar to source-routing in that an explicit path is defined for the frame to travel. However, unlike source-routing, the hop-by-hop definition is not carried with every frame. Rather, the hops are configured in the LSRs ahead of time along with the appropriate label values.

Definition of MPLS: Multi-Protocol Label Switching enables ATM switches to act as routers and creates new IP capabilities via flexible classification. "MPLS stands for "Multiprotocol Label Switching". In an MPLS network, incoming packets are assigned a "label" by a "label edge router (LER)". Packets are forwarded along a "label switch path (LSP)" where each "label switch router (LSR)" makes forwarding decisions based solely on the contents of the label. At each hop, the LSR strips off the existing label and

apply a new label which tells the next hop how to forward the packet.

Terminology:

- LSR - Routers that support MPLS are called Label Switch Router
- LER - LSR at the edge of the network is called Label Edge Router (a.k.a Edge LSR)
- Ingress LER is responsible for adding labels to unlabeled IP packets.
- Egress LER is responsible for removing the labels.
- Label Forwarding Information Base (LFIB) – a forwarding table (mapping) between labels to outgoing interfaces.
- Forward Equivalent Class (FEC) – All IP packets follow the same path on the MPLS network and receive the same treatment at each node.

MPLS Benefits:

Comparing MPLS with existing IP core and IP/ATM technologies, MPLS has many advantages and benefits:

- The performance characteristics of layer 2 networks
- The connectivity and network services of layer 3 networks
- Improves the price/performance of network layer routing
- Improved scalability
- Improves the possibilities for traffic engineering
- Supports the delivery of services with QoS guarantees
- Avoids need for coordination of IP and ATM address allocation and routing information

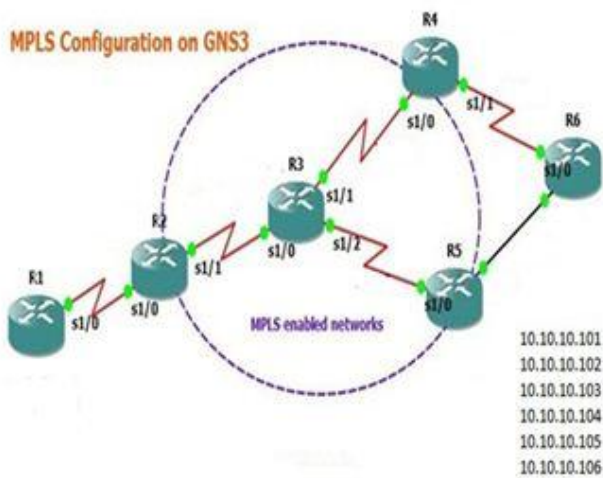
RSVP:

- RSVP is supported by the help of a RSVP object - the tag Object
- The tag object binding information for an RSVP flow is carried in the RSVP "RESV" message
- The RESV message carries the tag object containing the tag given by a TSR and also information about the local resources to be used
- The reservation state is refreshed once the flow is set up using the RESV message

Introduction to Class A 10 Network:

With an IPv4 IP address, there are five classes of available IP ranges: Class A, Class B, Class C, Class D and Class E, while only A, B, and C are commonly used.

Class	Range of Address	Supports
Class A	1.0.0.1 to 126.255.255.254	Supports nearly 16 million hosts
Class B	128.1.0.1 to 191.255.255.254	Supports Nearly 70,0000 hosts
Class C	192.0.1.1 to 223.255.254.254	Supports 254 hosts on each of 2 million networks
Class D	224.0.0.0 to 239.255.255.255	Used for multicast Groups
Class E	240.0.0.0.to 254.255.255.254	Reserved for Future use



II. MPLS TOPOLOGY

Introduction to GNS3:

GNS3 is graphically network simulator which you can use in the absence of physical routers and switches. It is an open source simulator can be installed using synaptic package manager. This describes the software that empowers network professionals.

To allow complete simulations, GNS3 is strongly linked with Dynamips, the core program that allows Cisco IOS simulation. Dynagen, a text based front end for dynamips.

Dependencies: GNS3 depends on several libraries and components. Successfully installing these dependencies is a prerequisite. The important dependencies are

Dynamips: Base of GNS3, a Cisco router simulator

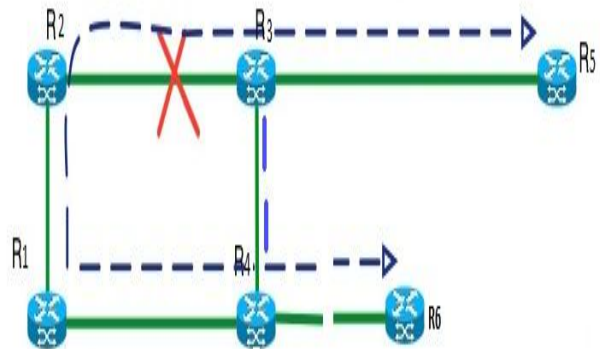
Dynagen: A text bases front-end to Dynamips, which uses the hypervisor mode to communicate with dynamips. It uses a simple configuration files for specifying virtual router configurations, and enables interconnecting of routers and WAN technologies such as ATM, Frame relays and switches. Furtherit provides management CLI for divide functions such as start, stop, suspend, reload, console, connection, etc.

Limitations:

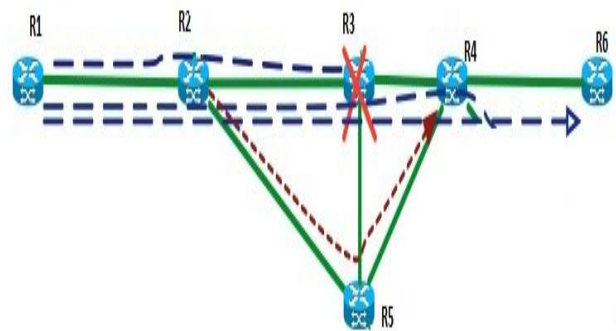
- Certainly Plenty of them.
- Some IOS images won't pass multicast
- Some features in IOU images will configure, but don't actually seem to work (Dynamic ARP

inspection, Private VLANs, etc)

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



Node Failure: FRR provides node protection for LSPs. Backup tunnels that bypass next-hop nodes along LSP paths are called next-next-hop (NNHOP) backup tunnels because they terminate at the node following the next-hop node of the LSP paths, thereby bypassing the next-hop node. They protect LSPs if a node along their path fails by enabling the node upstream of the failure to reroute the LSPs and their traffic around the failed node to the next-next hop. The below figure shows node failure case.



OSPF (Open Shortest Path First):

RSVP uses OSPF hence we are used to define OSPF. OSPF is designated by the Internet Engineering Task Force (IETF) as one of several Interior Gateway Protocols (IGPs) -- that is, protocols aimed at traffic moving around within a larger autonomous system network like a single enterprise's network, which may in turn be made up of many separate local area networks linked through routers. Using OSPF, a router that learns of a change to a routing table or detects a change in the network immediately multicasts the information to all other OSPF hosts in the network so they will all have the same routing table information.

When routes change -- sometimes due to equipment failure --

the time it takes OSPF routers to find a new path between endpoints with no loops (which is called "open") and that minimizes the length of the path is called the convergence time.

OSPF is a link-state routing protocol providing fast convergence and excellent scalability. Like all link-state protocols, OSPF is very efficient in its use of network bandwidth.

RSVP Hello Operation:

RSVP Hello enables RSVP nodes to detect when a neighbouring node is not reachable. This provides node-to-node failure detection. When such a failure is detected, it is handled in a similar manner as a link-layer communication failure.

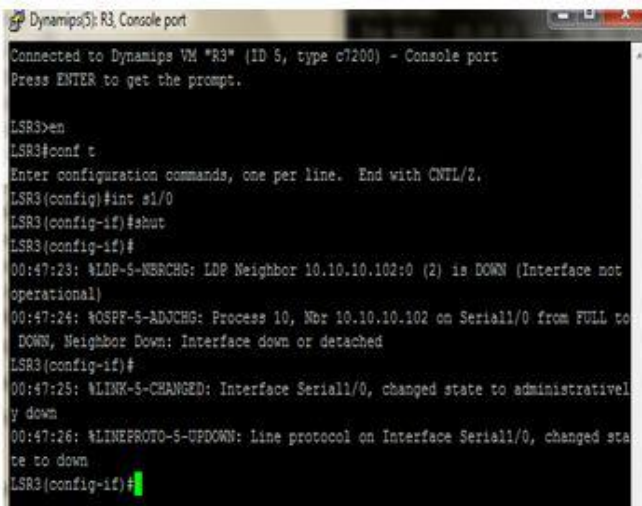
There are two configurable parameters:

Hellointerval--Use

the ip rsvp signalling hello refresh interval command.

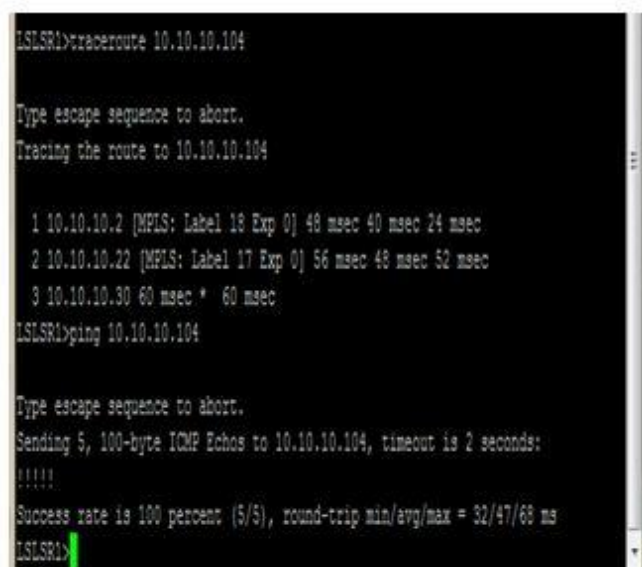
Number of acknowledgment messages that are missed before the sending node declares that the neighbour is down--Use the ip rsvp signalling hello refresh misses command.

Example Screenshots: For finding routes and packets sending we are using a concept called Trace route and ping:



```
Dynamips5: R3, Console port
Connected to Dynamips VM "R3" (ID 5, type c7200) - Console port
Press ENTER to get the prompt.

LSR3>en
LSR3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
LSR3(config)#int s1/0
LSR3(config-if)#shut
LSR3(config-if)#
00:47:23: %LDP-5-NBRCHG: LDP Neighbor 10.10.10.102:0 (2) is DOWN (Interface not operational)
00:47:24: %OSPF-5-ADJCHG: Process 10, Nbr 10.10.10.102 on Serial1/0 from FULL to DOWN, Neighbor Down: Interface down or detached
LSR3(config-if)#
00:47:25: %LINK-5-CHANGED: Interface Serial1/0, changed state to administratively down
00:47:26: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/0, changed state to down
LSR3(config-if)#
```



```
LSR1>traceroute 10.10.10.104

Type escape sequence to abort.
Tracing the route to 10.10.10.104

 0 10.10.10.2 [MPLS: Label 18 Exp 0] 48 msec 40 msec 24 msec
 1 10.10.10.22 [MPLS: Label 17 Exp 0] 56 msec 48 msec 52 msec
 2 10.10.10.30 60 msec * 60 msec
LSR1>ping 10.10.10.104

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.104, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/47/68 ms
LSR1>
```

III. CONCLUSION

MPLS is an efficient Encapsulation mechanism provides an effective design palette of technologies and protocols to solve the most pressing network-design problems. By stripping out legacy Layer 2 elements, it becomes possible to simplify the network and its operation. On one hand, this approach pushes complexity into the provider network, but this is ameliorated by the essential simplicity of MPLS! The big improvement that MPLS brings to the networking arena is the consistency of its models—Layer 2/3 VPNs use two MPLS labels to transport traffic from site to site. The top label is used to get the traffic through the core, and the inner label is used to push the traffic into the destination VPN.

REFERENCES

- [1] V. Alwayn "Advanced MPLS Design and Implementation" ISBN 1-58705-020-X
- [2] G.Swallow "MPLS Advantages for trafficengineering" IEEE Communications Magazine December 1999
- [3] E. Dobranowska "Network ideology, Traffic Engineering, MPLS, Resiliency" Master thesis August 2003
- [4] RFC 3270, "Multi-Protocol Label Switching (MPLS), Support of Differentiated Services", F. Le Faucheur, L. Wu, B.Davie, S. Davari, P. Vaananen, R. Krishnan, P. Cheval, J. Heinanen, May 2002.

Authors:

[1] Mrs. M ChandraKala a Student of Gokul Institute of Tech & Sciences. Currently she is perusing her M.Tech Degree in this College. Her interested areas are networks and Cloud Computing.

Email: chandrakala.marada@gmail.com

Contact No: 7093490518

[2] Mr B Ganesh Associate Professor and he has Rich experience in teaching. Currently he is working in the dept of CSE Gokul Institute of Tech & Sciences. His interested area is networks, image processing and Cloud Computing

Email:laxmisriganesh@yahoo.com

Contact No: 9440165350

[3] Mr. Chokkapu Narayanarao, An Efficient Lecturer, has 2year Experience in teaching. Currently working as an Assistant Professor in the Department of CSE, Raghu Institute of technology (RIT). His areas of interests are Computer Networks, Cloud Computing, Object oriented Programming languages and Image Processing.

Email:narayanarao.chokkapu@gmail.com

Contact No:9014313893