Original Research Paper Communication

Mpls Vpn Tunneling Using Ipv4 and Ipv6

Parth J. Trivedi Post Graduate Student, Department of Electronics and Communication, Aadishwar College of Technology, Gandhinagar

Prof. Rinkal Shah Professor, Department of Electronics and Communication, Aadishwar College of Technology, Gandhinagar

ABSTRACT

Advancement and innovation in internet networking field is reaching to remarkable milestones rapidly. So far Frame Relay is being used for exchanging information through internet, Frame Relay uses a packet switching methodology for faster delivery of packets but has much more disadvantages such as higher error rate, no guarantee of data delivery, need of special equipment and protocol dependent. Lately MPLS a label switching technology which ensure faster and guaranteed delivery of data with lesser delays has been in internet networks. MPLS is a protocol independent technology which works on label switching for faster routing and switching compared to ATM and Frame Relays providing flexibility of inter-networks without compromising scalability. MPLS provides a carrier grade transport platform, pseudo wires for separate virtual paths and much more. Implementing MPLS in the core network will reduce the overheads at service providers providing load balance reducing traffic congestion at service stations, pseudo wire paths for different kinds of data can be allotted, Traffic engineering and shaping, security, Backup paths are additional features of MPLS. MPLS can be applicable to ISP's, Large Enterprises, huge Railway networks etc.

KEYWORDS : MPLS, RSVP, CBTS, CSPF, Fast reroute, LDP, LSP, LSR, MPLSVPN

INTRODUCTION

Present networks are converged networks as they carry voice, video and normal data by using the same network resources. Since some user data traffics such as voice, video or bank transactions are more important and less tolerant to delay, they are differently treated based on their delivery requirements such as bandwidth and maximum affordable delay[1].

MPLS Traffic Engineering [2] is one of the most important and powerful feature of MPLS which provides network optimization by flexibly utilizing all the available links in the network. MPLS provides an approach to divert network traffic from congested parts of the network to non-congested parts[3].In traditional IP networks [4],links under-utilization was a huge problem where one route was over used for heavy network traffic and the other were unused or less used as a result bandwidth was wasted. To address the problem of link under-utilization, one solution was to force load balancing on the links by using routing protocols. In this method we change the metric of the link and this may potentially change the path of all the packets traversing the link [1]. This solution is scalable in large service provider networks where it is very hard to manage load balancing on hundreds of routers. The most efficient and better way to utilize all the available links in the network is MPLS Traffic Engineering. By using MPLS TE we can conveniently utilize the available network resources to their optimal potential. MPLS TE lets us to engineer the traffic the way we wants not the way routing protocol wants. It was not possible with traditional IP networks. Traditional IP network forwards all the traffic on the shortest path calculated by SPF algorithm [5]; it doesn't consider non-shortest paths for traffic sending regardless the fact that there may be enough bandwidth links.

II MPLS TE KEY ELEMENTS

2.1 Constraint Based Routing

In constraint based routing a shortest path is selected if it satisfies a particular set of constraints. The constraints are minimum bandwidth, link attributes and administrative weight, setup and hold priority values etc. [2] MPLS TE uses constraint shortest path first algorithm to build LSP tunnels. CSPF is an extension of SPF [6] and it looks not only on the cost values but also on the constraints to select the best path according to the resource requirements.

2.2 RSVP Signalling

RSVP [7] is a resource reservation protocol; it allocates bandwidth along the LSP for tunnels to establish. RSVP messages are sent by head end router for resource reservations. A head end router is the starting point of the tunnel whereas tail end is the ending point of it [8]. The actual available bandwidth is configured on the physical interfaces, which is announced by RSVP. The desired bandwidth for the establishment of tunnels is configured on the tunnel interfaces. So before establishing a tunnel desired bandwidth of the tunnel and the available bandwidth announced by RSVP are compared.

2.3 Class Based Tunnel Selection

Class Based Tunnel Selection is a way of forwarding traffic based on Class of Service values. We can create many tunnels on the same head end and tail end devices and assign different data traffic based on CoS values (Head end is the device where tunnel starts and tail end is where tunnel ends).Each tunnel is configured to look for a specific CoS value on the incoming traffic. Traffic is forwarded on a particular tunnel if the CoS of the traffic matches the value configured on tunnel. There are only three 3 bits specified in EXP field of MPLS label which are used for QoS purposes.

2.4 Fast Reroute

Fast Reroute is very important factor of MPLS TE. If a link or a node fails in LSP of MPLS network, FRR automatically reroutes traffic i.e. Switches traffic to the secondary path. For FRR, there are two paths Primary path and Secondary or Backup path. Primary path is the main tunnel used to carry traffic. Secondary path is used to carry traffic if a node or a link fails in primary tunnel. FRR provides protection against two types of failures.

1) Link Failure 2) Node Failure

Rerouting of traffic after link failure is illustrated in the figure 1(a).

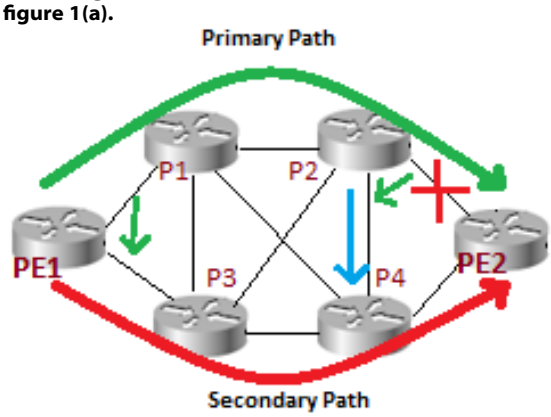

Figure 1(a): FRR with Link Protection

If link between P2 and PE2 fails somehow, P2 will quickly switch the traffic to the P4 through detour i.e. through PE1->P1->P2->P4->PE2. P2 will also signal PE1 about link P2-PE2 failure. As soon as PE1 knows about link P2-PE2 link failure, it diverts traffic to secondary tunnel i.e. To PE1->P3->P4->PE2.

Figure 1(b) shows the rerouting of traffic after a node failure

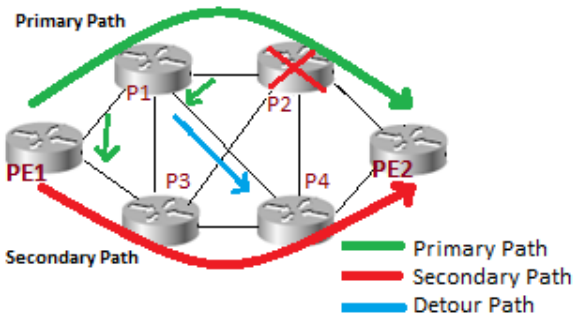

Figure 1(b): FRR with Node Protection

When node P2 fails, P1 quickly switches traffic to P4 through detour path which is PE1->P1->P4->PE2. P2 make a notice of node P2 failure to head end router i.e. PE1 and traffic is then diverted to secondary path which is PE1->P3->P4->PE2.

III. NETWORK IMPLEMENTATION

3.1 Primary Tunnels Implementation

I used GNS 3 simulator to create an MPLS based network used in this research work. Figure 2 shows the logical topology of the network which was used to work on MPLS TE and fast rerouting.

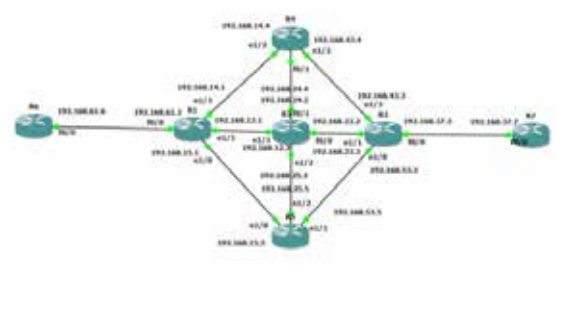

Figure 2: Topology of MPLS based Network

There are 7 Label Switch Routers all together in the MPLS backbone. Two of them (PE1 and PE2) are provider edge LSRs and five of them (P1, P2, P3, P4 and P5) are provider LSRs and they make the core of the MPLS network.PE routers can provide connectivity to the customers whereas P routers know only to forward packets based on the values contained in the labels, they know nothing about the end customers.

Four separate primary tunnels are configured on PE1 to take traffic of voice, video conferencing, mission critical data and best effort data to PE2.These tunnels treat the incoming traffic on preferential basis and take it to PE2 along different LSPs. Since tunnels are unidirectional, four more tunnels need to be configured on PE2 to take the traffic back to PE1.

PE1	Destination	Tunnel	EXP	Setup- Hold Priority	Path Option
Master Tunnel 10	7.7.7.7(PE 2)	Voice	5	3-3	Explicit
		Video Conf.	4	4-4	Explicit
		Critical data	3,2	5-5	Explicit
		BEst Effort		6-6	Dynamic

Table 1: Primary tunnels configured in the MPLS backbone network running from PE1 to PE2

3.2 Tunnel 1

Tunnel 1 is created to take voice traffic from PE1 to PE2. It is created along the path PE1>P1>P2>P3>PE2.

Since voice data can't afford much delay or jitter, EXP value 5 instructs Tunnel 1 to look for the incoming traffic with EXP value 5 to accept. The traffic with EXP value other than 5 is not accepted by the tunnel 1. So using this value tunnel 1 will take only voice data. Setup priority and hold priority are two important values. The lower these values are, the more important the tunnel is going to be. The lower setup priority value will make the tunnel to pre-empt other tunnels and the lower holding value will stop other competing tunnels to pre-empt this tunnel. So tunnel 1 is the most important tunnel in our network, it can pre-empt any other tunnel in the network and no other tunnel can pre-empt it. More than one path options can be configured and each of them can be given a preference number. Lower the number given to the path higher will be its preference. Tunnels can be created dynamically too. Dynamic option makes use of CSPF to calculate best path for the tunnel.

3.3 Tunnel 2

Tunnel 2 is created to carry video conferencing data from PE1 to PE2. It is explicitly established along the LSP PE1>P1>P4>P3>PE2.Tunnel 2 looks for EXP value of 4 in the MPLS label to take traffic of video conferencing. Its setup and priority values are 4-4, so it can pre-empt all the tunnels in the network except tunnel 1 and it can't be pre- empted by any tunnel except tunnel 1.

3.4 Tunnel 3

It carries traffic mission critical data such as important SQL bank transactions. It is also explicitly configured and it is established on the LSP PE1>P1>P5>P3>PE2.Tunnel 3 takes traffic only with EXP value of 3 and 2 in its label. It can pre-empt only tunnel 4 in the network and it can be pre-empted by tunnel 1 and 2 because they are more important than tunnel 3 and they carry important voice and video conferencing data.

3.5 Tunnel 4

It is best effort tunnel. It takes normal data. It is configured with dynamic option so it can take any LSP to carry data from PE1 to PE2.No path is explicitly configured for it. It can't pre-empt any of the tunnels in the network, and it can be pre-empted by any of them because their setup and hold priority values are lower than tunnel 4.Since no path is explicitly configured for dynamic tunnel 4, no FRR mechanism can be configured for it.

3.6 Master Tunnel 1

It contains a group of tunnels having the same head ends and tail ends. Since all 4 tunnels in our network heads from PE1 and ends at PE2,I grouped them in master tunnel 10.

3.7 Fast Reroute Implementation

Two backup tunnels are configured on primary tunnel 1 for link and node protection.

3.8 Backup Tunnel 1

This tunnel is configured on P1 along primary tunnel 1 to provide protection at link between P1 and P2.It is explicitly configured along the path P1>P4>P2.It starts from P1 and ends at P2.In case of link P1-P2 failure, It will divert traffic to LSP P1>P4>P2.

3.9 Backup Tunnel 2

This tunnel is also configured on P1 and provides protection against node P2 failure along primary tunnel 1.In case of failure of node P2, backup tunnel 2 will skip node P2 and divert traffic to LSP P1>P5>P3.RSVP sends hello messages to the neighbour routers to check the link or node failure. RSVP checks node-to-node failure detection, if a node doesn't receive acknowledgment from its neighbour node for a given number of times, it announces it down and hence the primary tunnel is announced down. Now the interfaces facing the protected link or node must have to be configured to switch the traffic to backup tunnels in case of link or node failure along the primary tunnels.

IV. CONFIGURATION OF MPLS TE

Following is the configuration of MPLS entered on the PE router

```
hostname PE1
ip cef
mpls traffic-eng tunnels
mpls label protocol ldp
multilink bundle-name authenticated
interface Loopback0
ip address 6.6.6.6 255.255.255.255

interface Tunnel1
tunnel source 6.6.6.6
 tunnel mode mpls traffic-eng
 tunnel destination 7.7.7.7
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng priority 3 3
 tunnel mpls traffic-eng bandwidth sub-pool 2000
 tunnel mpls traffic-eng path-option 1 explicit name LSP1
 tunnel mpls traffic-eng fast-reroute bw-protect

interface Tunnel2
ip unnumbered Loopback0
tunnel source 6.6.6.6
tunnel mode mpls traffic-eng
tunnel destination 7.7.7.7
tunnel mpls traffic-eng autoroute announce
tunnel mpls traffic-eng priority 4 4
tunnel mpls traffic-eng bandwidth sub-pool 20000
tunnel mpls traffic-eng path-option 1 explicit name LSP2
tunnel mpls traffic-eng fast-reroute bw-protect

interface Tunnel3
ip unnumbered Loopback0
tunnel source 6.6.6.6
tunnel mode mpls traffic-eng
tunnel destination 7.7.7.7
tunnel mpls traffic-eng autoroute announce
tunnel mpls traffic-eng priority 5 5
tunnel mpls traffic-eng bandwidth sub-pool 20000
tunnel mpls traffic-eng path-option 1 explicit name LSP3
tunnel mpls traffic-eng fast-reroute bw-protect

interface Tunnel4
ip unnumbered Loopback0
tunnel source 6.6.6.6
tunnel mode mpls traffic-eng
tunnel destination 7.7.7.7
tunnel mpls traffic-eng autoroute announce
tunnel mpls traffic-eng priority 6 6
tunnel mpls traffic-eng bandwidth sub-pool 20000
tunnel mpls traffic-eng path-option 1 dynamic
tunnel mpls traffic-eng fast-reroute bw-protect

interface Tunnel10
ip unnumbered Loopback0
tunnel source 6.6.6.6
tunnel mode mpls traffic-eng
tunnel destination 7.7.7.7
tunnel mpls traffic-eng autoroute announce
tunnel mpls traffic-eng exp-bundle master
tunnel mpls traffic-eng exp-bundle member Tunnel1
tunnel mpls traffic-eng exp-bundle member Tunnel2

interface FastEthernet0/0
ip address 12.168.61.6 255.255.255.0
speed auto
duplex auto
mpls ip
mpls traffic-eng tunnels
ip rsvp bandwidth 80000 sub-pool 2000

ip explicit-path name LSP1 enable
next-address 192.168.61.1
next-address 192.168.14.4
next-address 192.168.43.3
next-address 192.168.37.7
next-address 7.7.7.7

ip explicit-path name LSP2 enable
next-address 192.168.61.1
next-address 192.168.15.5
next-address 192.168.53.3
next-address 192.168.37.7
next-address 7.7.7.7

ip explicit-path name LSP3 enable
next-address 192.168.61.1
next-address 192.168.12.2
next-address 192.168.23.3
next-address 192.168.37.7
next-address 7.7.7.7
```

Similarly PE2 is configured.

V. EXPERIMENT RESULTS

5.1 Verification of Primary Tunnels

The results obtained from the implemented network verify that 4 primary tunnels are successfully created to take voice, video conferencing and mission critical data on preferential basis and to avoid delay which could distort data traffic.

Figure 3: Primary Tunnels on MPLS Network

Figures 3 shows all the primary tunnels configured in the network. The top 5 tunnels are configured on PE1, and are destined to PE2.So PE1 serves as the head end and PE2 as tail end. The last 4 tunnels are configured on PE2 and are destined to PE1. Thus PE2 is their head end and PE1 is the tail end.

VI. CONCLUSIONS

On large networks, no other technology can engineer traffic as efficiently as MPLS itself MPLS TE very conveniently uses the under-utilized links for carrying traffic and using existing network resources. MPLS TE creates tunnels to carry traffic and path of these tunnels can be explicitly assigned. MPLS facilitates important user's data traffic such as voice, video and bank transactions with dedicated tunnels for them to avoid any unnecessary delay. In case of a link or node failure along the primary tunnel's path, backup tunnels created by FRR can make a recovery from the failure very quickly. To further explore the exciting MPLS technology, it is recommended that the same network be implemented and investigated with IPv6 because IPv6 is inevitable and it will ultimately replace IPv4 in the near future. GMPLS, which makes the use of dense wavelength-division multiplexing for traffic engineering, also, needs to be researched. Similarly, Any Transport over MPLS, MPLS QoS with traffic policing and shaping to limit the user data traffic according to the service level agreement and MPLS VPN with encryption algorithm on customer sites also need to be investigated.

VI. REFERENCES

[1] V. Alwayn, 2002, Advanced MPLS Design & Implementation, pp. 222-224 Publishers: Cisco Press Indianapolis, IN 46290 USA

[2]. Eric Osborne, Ajay Simha, 2002,Traffic Engineering with MPLS,pp. 14-16, 122-126. Publishers: Cisco Press Indianapolis, USA

[3]. Cisco Systems, Inc, 2002, MPLS Traffic Engineering Technology,[Online].Available:http://www.multitech.co.in/MPLS-TE.pdf [Date Accessed: 10 August 2016

[4]. Ravi Ganesh V, M. V. Ramana Murthy, 2012, MPLS Traffic Engineering (An Implementation Framework) [Online].Available:http://www.multitech.co.in/MPLS-TE.pdf [Accessed: 10 August 2016]

[5]. Cisco IOS Release 12.0(5)S, 2012. Multiprotocol Label Switching (MPLS) Traffic Engineering, [Online]. Available: http://www.cs.vsb.cz/grygarek/TPS/MPLS/mpls_te.pdf [Accessed: 10 August 2016]

[6]. Juniper Networks, Inc, 2012. Constrained-Path LSP Computation[Online].Available:http://www.juniper.net/techpubs/en_US/junos10.0/information-products/topic-collections/config-guide-mpls-applications/mpls-lsp-constrained-path-computation.html [Accessed: 10 August 2016]

[7]. Juniper Networks, Inc, 2010. Understanding the RSVP SignalingProtocol.[Online].Available:http://www.juniper.net/techpubs/software/junos-security/junos-security10.2/junos-security-swconfig-mpls/topic-47252.html [Accessed: 17 August 2016]

[8]. Lancy Lobo, Umesh Lakshman, 2005. RSVP with TE Extensions:Signaling.[Online].Available:http://fengnet.com/book/ios_mpls/ch09lev1sec2.html [Accessed: 04 August 2016]