The Nucleus **51**, No. 1 (2014) 117-124

The Nucleus
A Quarterly Scientific Journal of Pakistan Atomic Energy Commission
NCLEAM, ISSN 0029-5698

ISP-BASED MPLS VPN: OVERVIEW, TRAFFIC ENGINEERING SERVICES AND SOLUTIONS

*M. J. ARSHAD, H. AHMAD, M. SAMIULLAH and A. BASIT

Department of Computer Science and Engineering, University of Engineering and Technology, Lahore, Pakistan

(Received September 23, 2013 and accepted in revised form February 07, 2014)

In recent years MPLS-Multiprotocol Label Switching enabled VPNs-Virtual Private Network have gained popularity as alternative to private WANs. MPLS-VPNs are more reliable, secure, scalable and cost effective than other candidate solutions. Traffic engineering (TE) is supported over MPLS, which allows network organizations to associate a LSP-Label Switched Path with the physical path they select. In this article, we present an implementation of traffic engineering over an Internet Service Provider (ISP)-based MPLS-VPN. We will start by defining the features, modes and preconditions for traffic engineering. Then we will explain what information needs to be disseminated to all the TE enabled routers and how the underlying routing protocol is modified to send it. Then we will define and configure MPLS TE tunnels. Finally, we will show how to achieve link protection in TE supported MPLS-VPN.

Keywords: Quality of Service, Security, TE, MPLS, RSVP, Backup Tunnels

1. Introduction

In recent years [4, 6, 7, 9, 13] the Internet has grown exponentially which has placed enormous pressure on the networks of service providers. In addition to the increase in the number of users there has been a rapid increase in connection speeds multiform, backbone traffic and emerging new applications. To fulfill the service guarantees, service providers must provide the required data rates and also work on architectures that can provide and guarantee agreed Quality of Service (QoS) levels and optimal performance with a minimum increase in network resources cost.

Multiprotocol Label Switching (MPLS) [6, 13] is an innovative technique for packet forwarding with high performance. It has many applications. One of its most widely used applications is to enable Virtual Private Networks (VPNs). MPLS enabled VPNs [1, 9, 11, 12] are more cost effective, reliable, secure and scalable than the previous VPN solutions. It also provides QoS by enabling traffic prioritization.

TE-Traffic Engineering is a phenomenon of selecting routes through which traffic will travel. It adapts the route for traffic according to dynamically changing networks condition. It has dual objectives: to provide good performance to user and to make efficient use of network resources. Traffic engineering is supported over MPLS [2, 3, 5, 10, 14], which allows network organizations to associate a LSP-Label-Switched Paths with physical paths they select. Constraint-based routing is also supported over MPLS, which makes sure that an LSP can fulfill specific performance requirements. In this research work we present an implementation of traffic engineering over an ISP-based MPLS-VPN. In the following sections, we first introduce traffic engineering and its features and show its effect on an MPLS-VPN. Then the two modes of traffic engineering are discussed. After that the preconditions, for the traffic engineering to work, are listed. Then we explain what information needs to be disseminated to all the TE enabled routers and how the underlying routing protocol is modified to send it. Next section lists the attributes of MPLS TE tunnel and discusses the factors that decide the path for MPLS TE tunnel. After that the advantage of enabling traffic engineering on MPLS is demonstrated by an example. The next section discusses how to configure MPLS TE tunnels. Then we discuss how RSVP labels are used for forwarding of traffic in TE tunnels. Finally, we show how link protection is achieved using backup tunnels and fast reroute.

2. MPLS-VPN Traffic Engineering

Traffic Engineering [5, 10] means to use network optimally and to utilize those links that are underutilized because they are not on the best routes. It shows that traffic engineering provides the option to route the traffic through paths other than best paths in order to utilize all links in the network. Figure 1 shows the impact of traffic engineering on a MPLS-VPN network. As shown in Figure 1, traffic engineering gives us an alternate to the path selected by the IGP. IGP selects the shortest path which is in this case PE1 to Core-C and Core-C to PE2. Traffic engineering gives the path PE1 to Core-A, Core-A to Core-B and Core-B to PE2 which

* Corresponding author : junaidarshad@uet.edu.pk

is not the shortest. This way we can also route the traffic through paths which are not much used by changing the routing protocol's metrics. Following are some features of Traffic Engineering:

- Provides efficient use of links throughout the network avoiding overutilization and underutilization of links.
- Takes the configured bandwidth into account
- Also considers link attributes, like delay and jitter, into routing decisions.
- Adjusts automatically to changing bandwidth and link attributes

2.1 Applying Modes of TE

Traffic Engineering [2] can be enabled in a network in two ways:

- By creating TE tunnels between each pair of edge LSRs
- By enabling TE everywhere in network but no TE tunnels until they are required

In the first method MPLS TE tunnels are created between each pair of edge LSRs in the network. This way all traffic is routed without any congestion in the network. In addition, the traffic can be assigned the characteristics like bandwidth, delay etc. which it needs. A good example of this method is an MPLS-VPN where you can create one tunnel i.e., TE from each router i.e., PE to every other PE router.

In the second method MPLS TE is enabled in the whole network but TE tunnels are not created until they are required. An example of this method is to create TE tunnels to route traffic around a hotspot or overloaded point in the network.

2.2 Overview of Operation of TE

Following are the prerequisites [3] for TE to work:

- Link constraints i.e. how much traffic each link can support and which TE tunnel can use the link
- TE information distribution by MPLS TE enabled link-state routing protocol
- An algorithm (PCALC) to calculate the optimal route as of head to tail end LSR
- A signaling protocol (RSVP) to signal the TE tunnel across the network
- A way to forward traffic on TE tunnel

2.3 Distribution of TE Information

A link state routing protocol [5] is required to flood the constraints of links in the network to all TE enabled routers. The next section will examine what link information the routing protocol needs to flood and how OSPF and IS-IS are modified to carry it.

2.4 Requirements for the IGP

The information of links in the whole network topology is required to be sent to all TE enabled routers in the network. This task [3] can be performed by a link state protocol which sends the status of all links in an area to all routers in that area. As a result each router in the area has the information of every alternate path to the destination. The topology and the link state information of the network must be available at the head end of the TE tunnel so that it knows all the possible routes. The constraint information is the collection of resource information of the links associated with TE. The link state routing protocol must be extended to carry this extra resource information. The TE resources of a link are as follows:

- Metric of Traffic Engineering (TE)
- Maximum Bandwidth of the Link
- Maximum Bandwidth that can be Reserved
- Bandwidth which is Unreserved
- Administrative group

Metric of TE is a parameter used for constructing TE topology which is different from IP topology. So it can be different from the IS-IS metric or OSPF cost of link.

The maximum bandwidth is the total bandwidth of the link whereas the maximum bandwidth that can be reserved is the available bandwidth of the link configured by the network administrator. The unreserved bandwidth is the remaining available bandwidth calculated by subtracting maximum reservable bandwidth from the maximum bandwidth.

The administrative group is a 32-bit field. The network operator can set each of these 32 bits individually and can define semantic of each bit.

2.5 Flooding by the IGP

The link state routing protocol [2] disseminates the TE information in any of the following cases:

- Change in Link Status
- Change in Configuration
- Flooding Timer Expires
- Change in the Reserved Bandwidth
- On failure of tunnel setup

Link state protocols like OSPF and IS-IS [6] floods LSA and LSP respectively when the state of interface changes or when a manual configuration changes the characteristics of the interface. They also flood LSAs

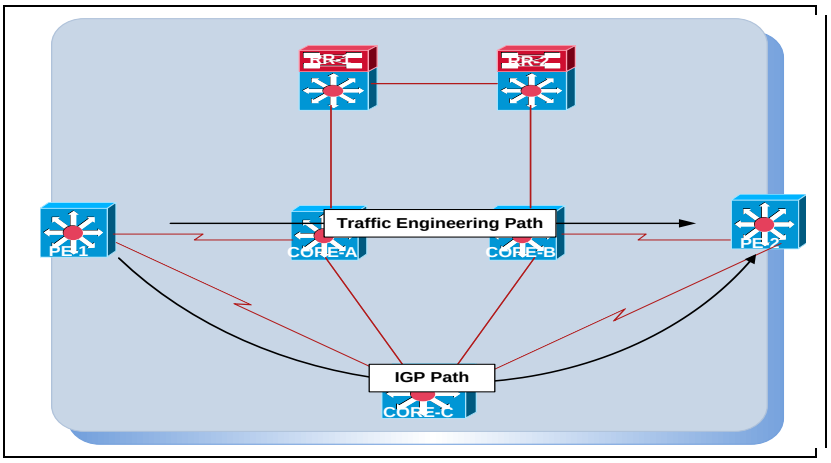

Figure 1. Traffic engineering scenario.

and LSPs on periodic intervals which are different for both of these protocols and can be changed.

Small changes in the bandwidth are not flooded immediately because there are more chances that a tunnel LSP will find enough bandwidth across that link when link has a lot of unreserved bandwidth than when link has less unreserved bandwidth. That is why the triggers in place for flooding the information when bandwidth is reserved on the link are closer to each other at the high end mark than at the low end mark of reserved bandwidth.

2.6 Attributes of MPLS TE Tunnel

MPLS TE tunnel [5, 10] has the following attributes:

- Tunnel Destination
- Desired Bandwidth
- Affinity
- Setup and Holding Priorities
- Reoptimization
- Path Options

The MPLS TE router id of the tail end LSR is the tunnel destination. The tunnel LSP is to be routed to the tunnel destination. The desired bandwidth means bandwidth which is required by the TE tunnel.

2.7. TE Tunnel Path Calculation

The selection of the path for TE tunnel [2] depends on the following factors:

- Path Setup Option
- Setup and Holding Priority
- Attribute Flags and Bits
- Reoptimization

2.7.1 Path Setup Option

Path options can be set on tunnel configuration on the head end router. Tunnel can be configured either explicitly or dynamically.

In the explicit method every router that the TE tunnel is to be routed on, including tail end router, is specified. Intermediate routers can be specified by either specifying the link IP address or TE router id.

In the dynamic method the tunnel head end router determines the best route for the tunnel through the network to the tail end router. In this method only the destination of TE tunnel is needed to be configured. The head end router determines the path for TE tunnel from MPLS TE database acquired from IGP.

2.7.2 Setup and Path holding Priority

MPLS TE tunnels can have different levels of importance in the network [10]. For example a longer tunnel with more hops can be more important than a shorter tunnel. Similarly a tunnel with a requirement of high bandwidth can be more important than a less bandwidth requiring tunnel. So there can be a situation in which an important tunnel cannot be routed optimally. To avoid such scenarios TE tunnels use the priority mechanism to make sure that the more critical tunnels can be routed optimally.

There are two priorities for each tunnel; Setup and Holding. Lower priority value means higher priority. The setup priority tells how important a tunnel is to get ahead of the other tunnels and holding priority shows how much the strength of that tunnel is to hold on to its reserved links.

2.7.3. Re-optimization

Re-optimization [5] is somewhat similar concept to convergence. If a link goes down or becomes available

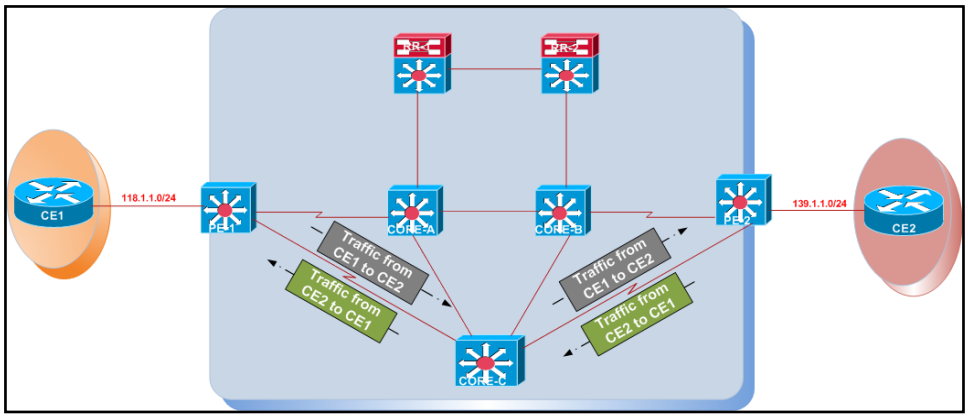

Figure 2. Traffic flow without traffic engineering.

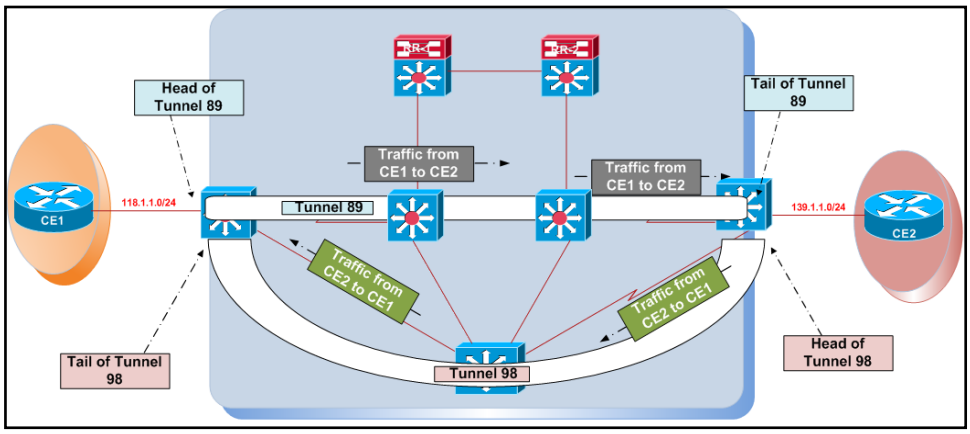

Figure 3. Traffic flow with traffic engineering.

again or some configuration changes occur in the network the routers in the network reruns the algorithms to calculate the best paths for destinations affected by that change. Similarly if a TE tunnel ends up on a path which is no longer an optimal path for it, the Reoptimization mechanism causes the tunnel to be rerouted to other optimal paths on the network. Reoptimization mechanism is triggered by one of the following :

- Periodic Reoptimization
- Event-driven Reoptimization
- Manual Reoptimization

2.7.4. Periodic Reoptimization

This kind of Reoptimization occurs after a specific interval. This interval can be the by default value configured by the vendor or the value configured by the network administrator.

2.7.5. Event-driven Reoptimization

This kind of Reoptimization occurs when a link which was previously down becomes available again due to configuration or due to change in the state of link.

2.7.6. Manual Reoptimization

By typing a command to perform the Reoptimization is known as Manual Reoptimization.

2.8. Effect of Enabling Traffic Engineering over MPLS

The TE-Traffic Engineering [3, 5, 10] is allowed for the efficient utilization of the links which are underutilized. Figure 2 shows an example of the flow of traffic without using traffic engineering. Here the path taken, by traffic from customer CE1 to CE2 and vice versa, is shown.

Figure 2 can elaborate this fact that all the traffic is utilizing the path chosen by the MPLS which is from PE1 to PE2 through Core C. Due to this selection the path through Core A and Core B is underutilized and the burden of whole traffic will be on Core C router. To avoid this scenario traffic engineering can be used.

Figure 3 shows the previous example of the flow of traffic with traffic engineering enabled. Two tunnels 89

and 98 were configured on PE1 and PE2 respectively. The head of tunnel 89 is at PE1 and tail at PE2. And the head of tunnel 98 is at PE2 and tail at PE1. The traffic from CE1 to CE2 adopts the path of tunnel 89, which is from PE1 to PE2 through Core A and Core B routers, which was previously underutilized. And the traffic from CE2 to CE1 is using the path of tunnel 98. So with traffic engineering the burden is reduced on Core C router as it is now processing one way traffic only.

2.9 Configuration of Tunnels

To configure [3] a tunnel following configurations are required on PE routers.

2.9.1 PE1

On PE1 tunnel 89 is configured which carries the traffic from CE1 to CE2. Following configurations were made on PE1.

ISP1-PE1

```
!
interface Tunnel89
 ip unnumbered Loopback0
 mpls traffic-eng tunnels
 tunnel mode mpls traffic-eng
 tunnel destination 9.9.9.9
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng path-option 1 explicit name PE1-CoreA-CoreB-PE2
!
!
!
ip route 9.9.9.9 255.255.255.255 Tunnel89
!
ip explicit-path name PE1-CoreA-CoreB-PE2 enable
 next-address 10.1.58.5
 next-address 10.1.56.6
 next-address 10.1.69.9
!
```

2.9.2 PE2

On PE2 tunnel 98 is configured which carries the traffic from CE2 to CE1. Following configurations were made on PE2.

ISP1-PE2

```
!
interface Tunnel98
 ip unnumbered Loopback0
 mpls traffic-eng tunnels
 tunnel mode mpls traffic-eng
 tunnel destination 8.8.8.8
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng path-option 2 explicit name PE2-CoreC-PE1
!
!
!
ip route 8.8.8.8 255.255.255.255 Tunnel98
!
ip explicit-path name PE2-CoreC-PE1 enable
 next-address 10.1.79.7
 next-address 10.1.78.8
!
```

Following commands are required to be configured on all the participating interfaces of routers other than route reflectors to enable traffic engineering on them. The lower part commands are configured in IGP.

```
!
mpls traffic-eng tunnels
!
interface Ethernet2/3
 mpls traffic-eng tunnels
 ip rsvp bandwidth
!
router isis
 metric-style wide level-2
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng level-2
!
```

To view the interfaces using RSVP and the bandwidth reserved for it the following command is used.

Core A

```
CoreA#sh ip rsvp interface
interface   rsvp    allocated  i/f max   flow max  sub max
Se1/1       ena           0    1158K     1158K     0
Et2/1       ena           0    7500K     7500K     0
Et2/3       ena           0    7500K     7500K     0
CoreA#
```

2.10. RSVP Label Swapping in Traffic Engineering

In traffic engineering, Label Distribution Protocol (LDP) is not used for forwarding the traffic of customers. For forwarding of traffic, in traffic engineering tunnels, RSVP labels are used [2]. Figure 4 shows the swapping of RSVP labels for the normal working of tunnels.

For tunnel 89 which is carrying the traffic from CE1 to CE2, PE1 imposes a label 513 which is the local label of Core-A for tunnel 89. When packet reaches Core-A the RSVP label 513 is swapped with label 612 which is the local label of Core-B for tunnel 89 and Core-B removes the label from traffic as PE2 is the edge LSR. On the other hand PE2 imposes label 704 on traffic from CE2 to CE1 which is the local label of Core-C for tunnel 98. Core-C performs penultimate hop pop and then sends the traffic without any label to PE1.

Following is the result of “traceroute” command issued on PE2 to PE1.

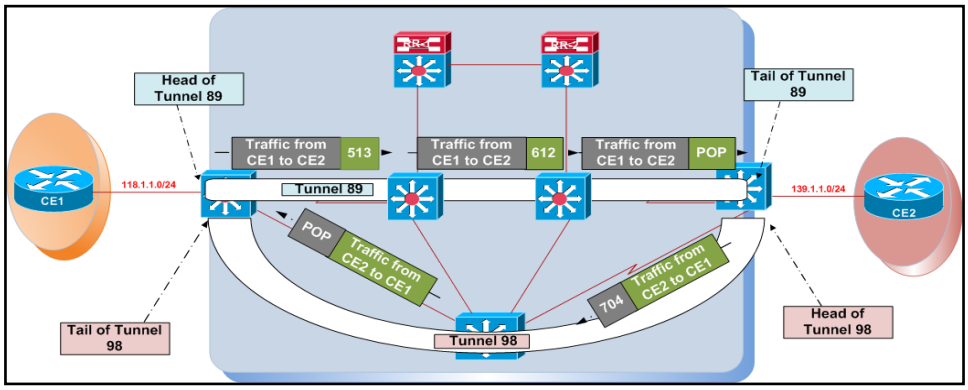

Figure 4. RSVP label swapping in traffic engineering.

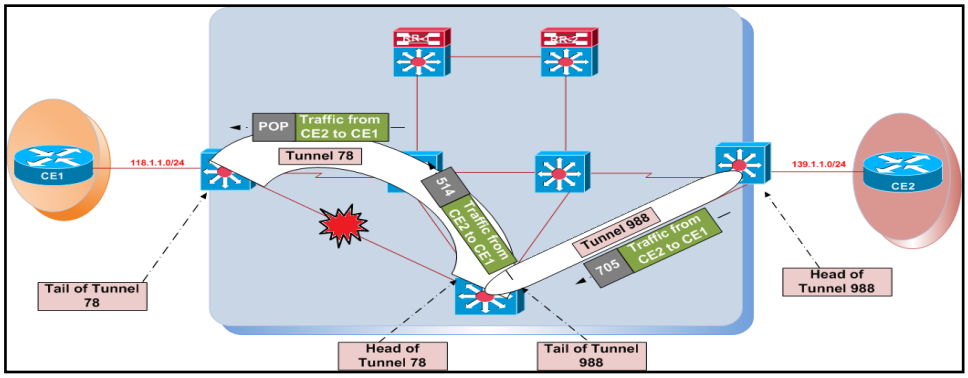

Figure 5. Label swapping in case of tunnel failure.

ISP1-PE2

```
R9#traceroute 8.8.8.8

Type escape sequence to abort.
Tracing the route to 8.8.8.8

  1 10.1.79.7 [MPLS: Label 704 Exp 0] 164 msec 144 msec 88 msec
  2 10.1.78.8 160 msec *  120 msec
R9#
```

The traffic goes from PE2 to Core-C then reaches PE1.

Following is the result of "traceroute" command issued on PE1 to PE2.

ISP1-PE1

```
R8#traceroute 9.9.9.9

Type escape sequence to abort.
Tracing the route to 9.9.9.9

  1 10.1.58.5 [MPLS: Label 513 Exp 0] 148 msec 132 msec 100 msec
  2 10.1.56.6 [MPLS: Label 600 Exp 0] 104 msec 116 msec 92 msec
  3 10.1.69.9 96 msec *  140 msec
R8#
```

The traffic goes from PE1 to Core-A then to Core-B and then reaches PE2.

Another scenario of label swapping is when a tunnel fails and backup tunnel carries the traffic. Figure 5 shows the swapping of RSVP labels when tunnel 98 fails because of the link failure between Core-C and PE1. PE2 router imposes RSVP label 705, on the traffic going from CE2 to CE1, which is the local label of Core-C for tunnel 988. When packet reaches the Core-C the 705 label is swapped with 514 which is the local label of Core-A for tunnel 78. RSVP label is removed when packet reaches Core-A, because it performs the penultimate hop pop.

After the link failure between PE1 and Core-C, the "traceroute" command is issued on PE2 to PE1 and following results are obtained.

ISP1-PE2

```
R9#traceroute 8.8.8.8

Type escape sequence to abort.
Tracing the route to 8.8.8.8

  1 10.1.79.7 [MPLS: Label 705 Exp 0] 200 msec 108 msec 140 msec
  2 10.1.57.5 [MPLS: Label 514 Exp 0] 172 msec 132 msec 160 msec
  3 10.1.58.8 232 msec *  252 msec
R9#
```

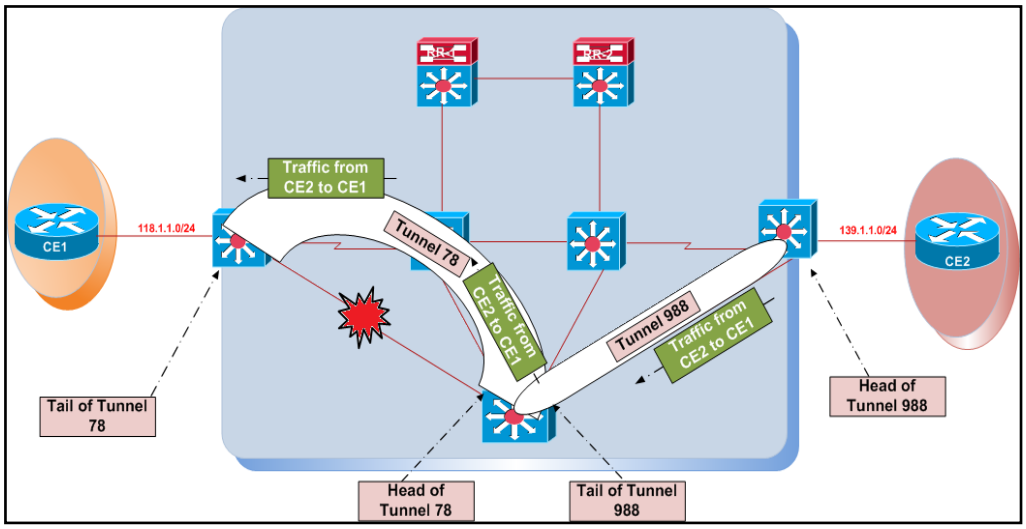

Figure 6. Link protection through backup tunnel.

After the link failure the traffic flows from PE2 to Core-C then to Core-A and then reaches PE1.

2.11 Link Protection using Fast Reroute Through Backup Tunnels

LSPs get link protection using fast reroute. When a link failure occurs, fast reroute redirects, all the traffic on the LSPs that traverse the failed link, around the failed link. The router which has the direct interface with the failed link controls the rerouting decision. Through either IGP or RSVP the link failure is notified to the headend of the tunnel. After being notified the headend tries to establish a new LSP that can bypass the failed link. As an example consider the scenario in Figure 3. If the link of tunnel 98, connecting Core-C router and PE1 router, fails, the traffic flow can be disturbed. So to avoid it we configure another tunnel 988 on PE2 whose head is on PE2 and tail is on Core-C router. Then another tunnel 78 is configured on Core-C router whose head is on Core-C router and tail at PE1 router. The tunnel 78 connects the Core-C with PE1 through Core-A router. Figure 6 shows this scenario. It shows that when link between Core-C and PE1 router fails the traffic from CE2 to CE1 routes through PE2, Core-C, Core-A and PE1.

3. Conclusion

In this paper we emphasized on the benefits of MPLS enabled VPNs and discussed the advantages of traffic engineering. The rest of the paper discussed how to enable traffic engineering over MPLS-VPN. First we introduced traffic engineering and its features and how it can affect an MPLS enabled VPN. Then we discussed the two modes of traffic engineering. Following that the preconditions, for the traffic engineering to work, were established. Next we talked about what information should be disseminated to all the TE enabled routers and how the underlying routing protocol is modified to send it. After that we listed the attributes of MPLS TE tunnel and discussed the factors that decide the path for MPLS TE tunnel. Then we illustrated the advantage we achieve by enabling traffic engineering over MPLS. The next section discussed how to configure MPLS TE tunnels and how RSVP labels are used for forwarding of traffic in TE tunnels. Lastly we discussed how TE tunnels are supported by using backup tunnels and fast route in case of a link failure.

References

[1] B. Alawieh et al., Journal of Security and Communication Networks **1**, No. 4 (2008) 269.

[2] D.O. Awduche, MPLS and Traffic Engineering in IP Networks, IEEE Communication Magazine **37**, No. 12 (1999) 42.

[3] D. Awduche et al., Requirements for Traffic Engineering Over MPLS, RFC-2702, 1999.

[4] R. Callon, A Framework for Layer 3 Provider Provisioned Virtual Private Networks, IETF (draft-ietf-ppvpn-frame-work-06.txt) (2002).

[5] C. Chou, Traffic Engineering for MPLS-Based Virtual Private Networks, Computer Networks **44**, No. 3 (2004) 319.

[6] S.K. Das et al., MPLS-BGP Based LSP Setup Techniques, Proceedings of the 28th Annual IEEE Conference on Local Computer Network (LNC), Singapore (2003) pp. 279-280.

[7] S. Deering and R. Hinden, Internet Protocol Version 6 (IPv6) Specification, RFC-2460 (1998).

[8] P. Ferguson and G. Huston, The Internet Protocol Journal **1**, No. 2 (1998).

[9] H. Lee et al., End-to-End QoS Architecture for VPNs: MPLS VPN Deployment in a Backbone Network, Proceedings of IEEE International Workshop on Parallel Processing, Toronto, Canada (2003) pp. 479-483.

[10] E.D. Osborne and A. Simha, Traffic Engineering with MPLS, Cisco Press (2003).

[11] S. Previdi, Introduction to MPLS-BGP-VPN, Proceeding of MPLS Forum 2000, Cisco, 2000.

[12] E. Rosen and Y. Rekhter, BGP/MPLS VPNs, RFC-2547, IETF (draft-rosen-rfc2547bis-03.txt) (1999).

[13] E. Rosen et al., Multiprotocol Label Switching Architecture, IETF RFC-3031 (2001).

[14] G. Swallow, IEEE Communication Magazine **37**, No. 12 (1999) 54.