10

Traffic Engineering

Mahesh Kumar Porwal
Shrinathji Institute of Technology & Engineering, Nathdwara (Rajasthan), India

1. Introduction

Multi Protocol Label Switching (MPLS) is today mostly used for traffic engineering therefore we start by describing what traffic engineering is and why traffic engineering is needed.

Traffic engineering and fast reroute are the two major applications of constraint based routing Traffic engineering is the process of controlling how traffic flows through a service provider's network so as to optimize resource utilization and network performance[1]. Traffic engineering is needed in the Internet mainly because the shortest path is used in current intra- domain routing protocols (e.g., OSPF, IS-IS) to forward traffic. The shortest path routing may give rise to two problems.

First, the shortest paths from different sources overlap at some links, resulting in congestion at those links.

Second, at some time, the traffic volume from a source to a destination could exceed the capacity of the shortest path, while a longer path between these two nodes remains under-utilized. The reason why conventional IP routing cannot provide traffic engineering is that it does not take into account the available bandwidth on individual links. For the purpose of traffic engineering, constraint based routing is used to route traffic trunk[2], which is defined as a collection of individual transmission control protocol (TCP), or user datagram protocol (UDP) flows, called "microflows" that share two common properties.

The **first** property is that all microflows are forwarded along the same common path.

The **second** property is that they all share the same class of service. By routing at the granularity of traffic trunks, traffic trunks have better scaling properties than routing at the granularity of individual microflows with respect to the amount of forwarding state and the volume of control traffic.

In a sense, IP networks manage themselves. A host using the Transmission Control Protocol (TCP) adjusts its sending rate according to the available bandwidth on the path to the receiver. If the network topology should change, routers react to changes and calculate new paths to the destination. This has made the TCP/IP [3] Internet a robust communication network. But robustness does not implicate that the network runs efficiently. The interior gateway protocols used today like OSPF and ISIS compute the shortest way to the destination and routers forward traffic according to the routing tables build from those calculations. This means that traffic from different sources passing through a router with the same destination will be

aggregated and sent through the same path. Therefore a link may be congested despite the presence of under-utilized link in the network. And delay sensitive traffic like voice-over-IP calls may travel over a path with high propagation delay because this is the shortest path while a low latency path is available.

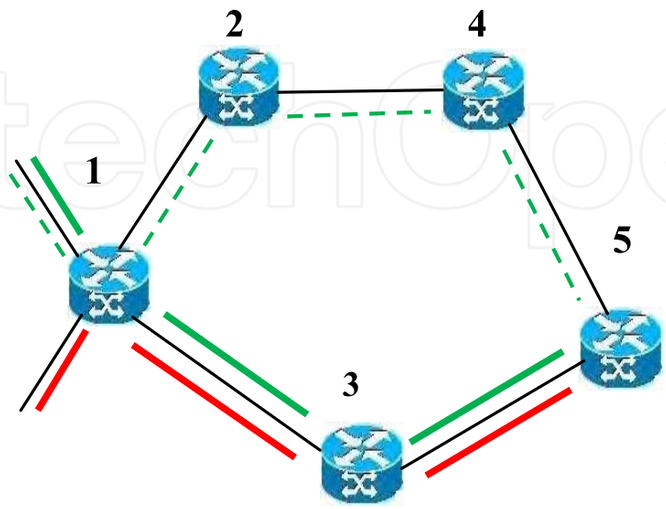


Fig. 1. Traffic Engineering

As illustrated in the above figure 1 the shortest path from router 1 to 5 is the path (1-3-5). All traffic passing through router 1 with destination router 5 (or another router with router 5 in the shortest path) will travel through this shortest path if the shortest path algorithm is used for forwarding in this network. Although there is an alternative path (1-2-4-5) available that could be used to distribute traffic more evenly in the network.

Traffic engineering is the process of controlling how traffic flows through a network to optimize resource utilization and network performance [4]. Traffic engineering is basically concerned with two problems that occur from routing protocols that only use the shortest path as constraint when they construct a routing table.

The shortest paths from different sources overlap at some links, causing congestion on those links. The traffic from a source to a destination exceeds the capacity of the shortest path, while a longer path between these two routers is under-utilized.

MPLS can be used as a traffic engineering tool to direct traffic in a network in a more efficient way then original IP shortest path routing. MPLS can be used to control which paths traffic travels through the network and therefore a more efficient use of the network resources can be achieved. Paths in the network can be reserved for traffic that is sensitive, and links and router that is more secure and not known to fail can be used for this kind of traffic.

2. Traffic engineering's role in next-generation networks

Traditional service provider networks provided Layer 2 point-to-point virtual circuits with contractually predefined bandwidth. Regardless of the technology used to implement the service (X.25, Frame Relay or ATM), the traffic engineering (optimal distribution of load across all available network links) was inherent in the process.

In most cases, the calculation of the optimum routing of virtual circuits was done off-line by a network management platform; advanced networks (offering Frame Relay or ATM switched virtual circuits) also offered real-time on-demand establishment of virtual circuits. However, the process was always the same:

- The free network capacity was examined.
- The end-to-end hop-by-hop path throughout the network that satisfied the contractual requirements (and, if needed, met other criteria) was computed.
- A virtual circuit was established along the computed path.

Internet and most IP-based services, including IP-based virtual private networks (VPNs) implemented with MPLS VPN, IPsec or Layer 2 transport protocol (L2TP), follow a completely different service model:

- The traffic contract specifies ingress and egress bandwidth for each site, not site-to-site traffic requirements.
- Every IP packet is routed through the network independently, and every router in the path makes independent next-hop decisions.
- Once merged, all packets toward the same destination take the same path (whereas multiple virtual circuits toward the same site could traverse different links).

Simplified to the extreme, the two paradigms could be expressed as follows:

- Layer 2 switched networks assume that the bandwidth is expensive and try to optimize its usage, resulting in complex circuit setup mechanisms and expensive switching methods.
- IP networks assume that the bandwidth is "free" and focus on low-cost, high-speed switching of a high volume of traffic.

The significant difference between the cost-per-switched-megabit of Layer 2 network (for example, ATM) and routed (IP) network has forced nearly all service providers to build next-generation networks exclusively on IP. Even in modern fiber-optics networks, however, bandwidth is not totally free, and there are always scenarios where you could use free resources of an underutilized link to ease the pressure on an overloaded path. Effectively, you would need traffic engineering capabilities in routed IP networks, but they are simply not available in the traditional hop-by-hop, destination-only routing model that most IP networks use.

Various approaches (including creative designs, as well as new technologies) have been tried to bring the traffic engineering capabilities to IP-based networks. We can group them roughly into these categories:

- The network core uses Layer 2 switched technology (ATM or Frame Relay) that has inherent traffic engineering capabilities. Virtual circuits are then established between edge routers as needed.
- IP routing tricks are used to modify the operation of IP routing protocols, resulting in adjustments to the path the packets are taking through the network.
- Deployment of IP-based virtual circuit technologies, including IP-over-IP tunnels and MPLS traffic engineering.

The Layer 2 network core design was used extensively when the service providers were introducing IP as an additional service into their WAN networks. Many large service providers have already dropped this approach because it does not result in the cost reduction or increase in switching speed that pure IP-based networks bring

3. Traffic engineering objectives

Traffic Engineering (TE) is concerned with performance optimization of operational networks. More formally speaking, the key traffic engineering objectives are:

1. **Minimizing congestion:** Congestion occurs either when network resources are insufficient or inadequate to accommodate offered load or if traffic streams are inefficiently mapped onto available resources; causing subsets of network resources to become over-utilized while others remain underutilized [5].
2. **Reliable network operations:** Adequate capacity for service restoration must be available keeping in mind multiple failure scenarios, and at the same time, there must be mechanisms to efficiently and speedily reroute traffic through the redundant capacity. On recovering from the faults, re-optimization may be necessary to include the restored capacity.
3. **Quality of Service requirements:** In a multi-class service environment, where traffic streams with different service requirements contend with each other, the role of traffic engineering becomes more decisive. In such scenarios, traffic engineering has to provision resources selectively for various classes of streams, judiciously sharing the network resources, giving preferential treatment to some service classes.
4. **Traffic oriented:** Traffic oriented performance objectives include the aspects that enhance the QoS of traffic streams. In a single class, best effort Internet service model, the key traffic oriented performance objectives include: minimization of packet loss, minimization of delay, maximization of throughput, and enforcement of service level agreements. Under a single class best effort Internet service model, minimization of packet loss is one of the most important traffic oriented performance objectives. Statistically bounded traffic oriented performance objectives (such as peak to peak packet delay variation, loss ratio, and maximum packet transfer delay) might become useful in the forthcoming differentiated services Internet.
5. **Resource oriented:** Resource oriented performance objectives include the aspects pertaining to the optimization of resource utilization. Efficient management of network resources is the vehicle for the attainment of resource oriented performance objectives. In particular, it is generally desirable to ensure that subsets of network resources do not become over utilized and congested while other subsets along alternate feasible paths remain underutilized. Bandwidth is a crucial resource in contemporary networks. Therefore, a central function of Traffic Engineering is to efficiently manage bandwidth resources.

4. Components of traffic engineering

One of the strategies for TE using MPLS involves four functional components [6]:

1. Information distribution
2. Path selection

3. Signaling and path set-up
4. Packet forwarding

Now, discussing each of the components in detail:

1. **Information Distribution:** Traffic engineering requires detailed knowledge about the network topology as well as dynamic information about network loading. This can be implemented by using simple extensions to IGP so that link attributes (such as maximum link bandwidth, current bandwidth usage, current bandwidth reservation) are included as part of routers link-state advertisements. The standard flooding algorithm used by link-state IGP ensures that link attributes are distributed to all routers in ISPs routing domain. Each LSR maintains network link attributes and topology information in a specialized TE database (TED), which is used exclusively for calculating explicit paths for placement of LSPs on physical topology.
2. **Path Selection:** On the basis of the network topology and link attributes in the TED and some administrative attributes obtained from user configuration, each ingress LSR calculates the explicit paths for its LSPs, which may be strict or loose. A strict explicit route is one in which the ingress LSR specifies all the LSRs in the LSP, while only some LSRs are specified in a loose explicit path. LSP calculations may also be done offline for optimal utilization of network resources.
3. **Signaling and Path-Setup:** The path calculated by the path selection component is not known to be workable, until LSP is actually established by the signaling component, because it is calculated on the basis of information present in TED, which may not be up-to-date. The signaling component is responsible for establishing LSP state and label binding and distribution in the path set-up process.
4. **Packet-Forwarding:** Once the path is set-up, packet forwarding process begins at the Label Switch Router (LSR) and is based on the concept of label switching.

5. MPLS and traffic engineering

MPLS is strategically significant for Traffic Engineering because it can potentially provide most of the functionality available from the overlay model, in an integrated manner, and at a lower cost than the currently competing alternatives. Equally importantly, MPLS offers the possibility to automate aspects of the Traffic Engineering function.

The concept of MPLS traffic trunks is used, according to Li and Rekhter [7], a traffic trunk is an aggregation of traffic flows of the same class which are placed inside a Label Switched Path. Essentially, a traffic trunk is an abstract representation of traffic to which specific characteristics can be associated. It is useful to view traffic trunks as objects that can be routed; that is, the path through which a traffic trunk traverses can be changed. In this respect, traffic trunks are similar to virtual circuits in ATM and Frame Relay networks. It is important, however, to emphasize that there is a fundamental distinction between a traffic trunk and the path, and indeed the LSP, through which it traverses. An LSP is a specification of the label switched path through which the traffic traverses. In practice, the terms LSP and traffic trunk are often used synonymously.

The attractiveness of MPLS for Traffic Engineering can be attributed to the following factors:

1. Explicit label switched paths which are not constrained by the destination based forwarding paradigm can be easily created through manual administrative action or through automated action by the underlying protocols.
2. LSPs can potentially be efficiently maintained.
3. Traffic trunks can be instantiated and mapped onto LSPs.
4. A set of attributes can be associated with traffic trunks which modulate their behavioral characteristics.
5. A set of attributes can be associated with resources which constrain the placement of LSPs and traffic trunks across them.
6. MPLS allows for both traffic aggregation and disaggregating whereas classical destination only based IP forwarding permits only aggregation.
7. It is relatively easy to integrate a "constraint-based routing" framework with MPLS.
8. A good implementation of MPLS can offer significantly lower overhead than competing alternatives for Traffic Engineering.

6. The MPLS domain

In [3] the MPLS domain is described as "a contiguous set of nodes which operate using MPLS routing and forwarding". This domain is typically managed and controlled by one administration. The MPLS domain concept is therefore similar to the notion of an AS (autonomous system), as the term is used in conventional IP routing i.e. a set of related routers that are usually under one administrative and management control.

The MPLS domain can be divided into MPLS core and MPLS edge. The core consists of nodes neighboring only to MPLS capable nodes, while the edge consists of nodes neighboring both MPLS capable and incapable nodes. The nodes in the MPLS domain are often called LSRs (Label Switch Routers). The nodes in the core are called transit LSRs and the nodes in the MPLS edge are called LERs (Label Edge Routers). If a LER is the first node in the path for a packet traveling through the MPLS domain this node is called the ingress LER, if it is the last node in a path it's called the egress LER. Note that these terms are applied according to the direction of a flow in the network, one node can therefore be both ingress and egress LER depending on which flow is considered. The terms upstream and downstream routers are also often used to indicate in which order the routers are traversed. If a LSR is upstream from another LSR, traffic is passed through that LSR before the other (downstream). A schematic view of the MPLS domain is illustrated in figure 2.

7. MPLS traffic engineering essentials

Multi-Protocol Label Switching (MPLS) is the end result of the efforts to integrate Layer 3 switching, better known as routing, with Layer 2 WAN backbones, primarily ATM. Even though the IP+ATM paradigm is mostly gone today because of the drastic shift to IP-only networks in the last few years, MPLS retains a number of useful features from Layer 2 technologies. One of the most notable is the ability to send packets across the network through a virtual circuit called Label Switched Path, or LSP, in MPLS terminology.

While the Layer 2 virtual circuits are almost always bidirectional (although the traffic contracts in each direction can be different), the LSPs are always unidirectional. If you need bidirectional connectivity between a pair of routers, you have to establish two LSPs.

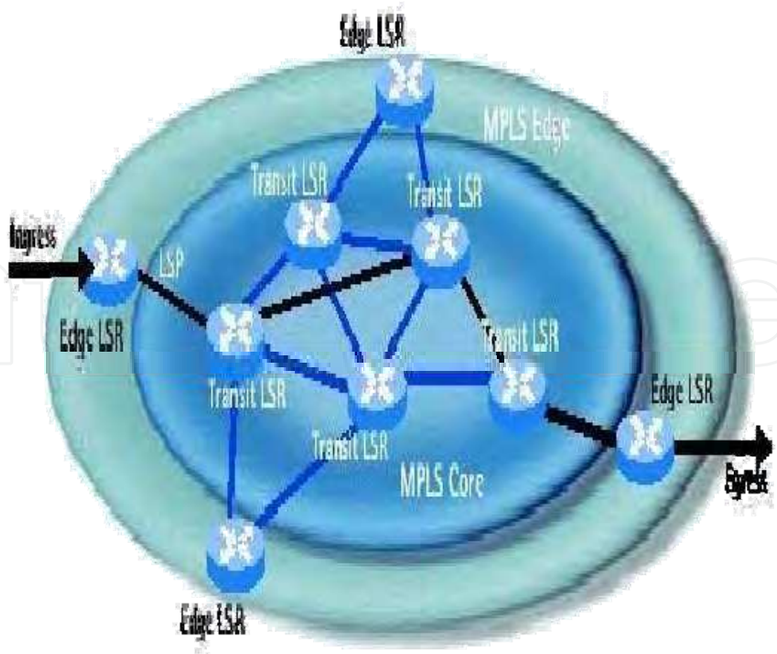


Fig. 2. The MPLS domain

The LSPs in MPLS networks are usually established based on the contents of IP routing tables in core routers. However, there is nothing that would prevent LSPs being established and used through other means, provided that:

1. All the routers along the path agree on a common signaling protocol.
2. The router where the LSP starts (head-end router) and the router where the LSP ends (tail-end router) agree on what's traveling across the LSP.

The other routers along the LSP do not inspect the packets traversing the LSP and are thus oblivious to their content; they just need to understand the signaling protocol that is used to establish the LSP.

With the necessary infrastructure in place, it was only a matter of time before someone would get the idea to use LSPs to implement MPLS-based traffic engineering. The MPLS traffic engineering technology has evolved and matured significantly since then, but the concepts have not changed much since its introduction:

1. The network operator configures an MPLS traffic engineering path on the head-end router. (The configuration mechanism involves a tunnel interface that represents the unidirectional MPLS TE LSP.)
2. The head-end router computes the best hop-by-hop path across the network, based on resource availability advertised by other routers. Extensions to link-state routing protocols (OSPF or IS-IS) are used to advertise resource availability.

NOTE: The first MPLS TE implementations supported only static hop-by-hop definitions. These can still be used in situations where you need a very tight hop-by-hop control over the path the MPLS TE LSP will take or in networks using a routing protocol that does not have MPLS TE extensions.

1. The head-end router requests LSP establishment using a dedicated signaling protocol. As is often the case, two protocols were designed to provide the same functionality as RSVP-TE (RSVP extensions for traffic engineering) and CR-LDP (constraint-based routing using label distribution protocol).
2. The routers along the path accept (or reject) the MPLS TE LSP establishment request and set up the necessary internal MPLS switching infrastructure.
3. When all the routers in the path accept the LSP signaling request, the MPLS TE LSP is operational.
4. The head-end router can use MPLS TE LSP to handle special data (initial implementations only supported static routing into MPLS traffic engineering tunnels) or seamlessly integrate the new path into the link-state routing protocol.

The tight integration of MPLS traffic engineering with the IP routing protocols provides an important advantage over the traditional Layer 2 WAN networks. In the Layer 2 backbones, the operator had to establish all the virtual circuits across the backbone (using a network management platform or by configuring switched virtual circuits on edge devices), whereas the MPLS TE can automatically augment and enhance the mesh of LSPs already established based on network topology discovered by IP routing protocols. You can thus use MPLS traffic engineering as a short-term measure to relieve the temporary network congestion or as a network core optimization tool without involving the edge routers.

In recent years, MPLS traffic engineering technology (and its implementation) has grown well beyond features offered by traditional WAN networks. For example:

1. **Fast reroute** provides temporary bypass of network failure (be it link or node failure) comparable to SONET/SDH reroute capabilities.
2. **Re-optimization** allows the head-end routers to utilize resources that became available after the LSP was established.
3. **Make-before-break** signaling enables the head-end router to provision the optimized LSP before tearing down the already established LSP.
4. **Automatic bandwidth adjustments** measure the actual traffic sent across an MPLS TE LSP and adjust its reservations to match the actual usage.

8. Requirements for traffic engineering model

A TE process model must follow a set of actions to optimize the network performance. This model has the following components:

Measurement: Measurement is an important component of the TE function. The network performance can only be determined through measurement. Traffic measurement is an essential tool to guide the network administrator of large IP networks in detecting and diagnosing performance problems, and evaluating potential control actions. The data measurement is analyzed and a decision based on the analysis is taken for network performance optimization. Measurement is needed to determine the quality of services and to evaluate TE policies.

Modelling, Analysis, and Simulation: Modelling and analysis are important aspects for TE. A network model is an abstract representation of the network that captures the network

features, attributes and characteristics (e.g. link and nodal attributes). A network model can facilitate analysis or simulation, and thus can be useful to predict the network performance.

Network modelling can be classified as structural or behavioural module. Structural modules focus on the organization of the network and its components. Behavioral modules focus on the dynamics of the networks and its traffic workload. Because of the complexity of realistic quantitative analysis of network behavior, certain aspects of network performance studies can only be conducted effectively using simulation.

Optimization: Network performance optimization can be called corrective when a solution to a problem is made, or perfective, where an improvement to the network performance is made, even when there is no problem. Many actions could be taken such as adding additional links, increasing link capacity or adding additional hardware. Planning for future improvement in the network (e.g. network design, network capacity or network architecture) is considered as a part of network optimization.

9. Criteria for selecting the best traffic route

Traditionally, there have been three parameters that describe the quality of a connection: bandwidth, delay, and packet loss. A connection with high bandwidth, low delay, and low packet loss is considered to be better than one with low bandwidth, high delay, and high packet loss. The following parameters can be considered when selecting the best traffic route:

Congestion: Congestion decreases the available bandwidth and increases delay and packet loss. It is important to avoid routes over congested paths.

Distance: Two routes may have different paths. Some networks interconnect only at relatively few locations, so they may have to transport traffic over long distances to get it to its destination. Others have better interconnection, so the traffic does not have to take a detour. There may be reasons not to prefer the more direct route, such as lower bandwidth or congestion, but generally a shorter geographic path is better.

Hops: The number of hops (e.g. routers) that shows up on the path to the destination increases the delay. Each hop potentially adds additional delay, because packets have to wait in a queue before they are transmitted, and the extra equipment in a path means that a failure somewhere along the way is more likely. So, paths with fewer hops are better.

10. Congestion control

Congestion in a packet switching network is a state in which the performance of the network degrades because of the saturation of network resources. Congestion could result in degradation of service quality to users. To avoid congestion, certain mechanisms have to be provided; such mechanisms are usually called congestion control.

10.1 Categories of congestion control

Congestion control policies can be categorized differently based on the objective of the policy, the time period of applying the policy, and the action taken to avoid congestion. In the following we will explain some of these policies.

10.1.1 Response time scale

Response time scale can be categorized as one of the following: long, medium and short. **In the long time scale**, expansion of the network capacity is considered. This expansion is based on estimates of future traffic demands, and traffic distribution. Because the network elements are expensive, upgrades take place in a long time scale between week to month or years. **In the medium time scale**, network control policies are considered (e.g. adjusting the routing protocol parameters to reroute traffic from a congested network node). These policies are mostly based on a measurement, and the actions are applied during a period of minutes to days. **In the short time scale**, packet level processing and buffer management functions in routers are considered (e.g. active queue control schemes in TCP traffic using Random Early Detection (RED)).

10.1.2 Reactive versus preventive

In reactive congestion control, congestion recovery takes place to restore the operation of a network to its normal state after congestion has occurred. Control policies react to existing congestion problems to remove or reduce them. In preventive congestion control, keeping the operation of a network at or near the point of maximum power is the main objective, so congestion will never occur. Control policies applied to prevent congestion are based on estimates and predictions of possible congestion appearance.

10.1.3 Supply side versus demand side

Increasing the capacity in the network is called a supply side congestion control. Supply side control is achieved by increasing the network capacity or balancing the traffic, (e.g. capacity planning to estimate traffic workload). For demand side control, policies are applied to regulate the offered traffic to avoid congestion (e. g. traffic shaping mechanism is used to regulate the offered load).

10.2 Control policies

Different congestion control policies have been proposed to deal with congestion in networks. Generally speaking, these policies differ in the use of control messages. The following will describe some of them.

Source Quench: Source Quench is the current method of congestion control in the Internet. When a network node responds to congestion by dropping packets, it could send an Internet Control Message Protocol Source Quench message (ICMP) to the source**,** informing it of packet drop. The drawback of this policy is that it is a family of varied policies. The major gateway manufacturers have implemented various source quench methods. This variation makes the end-system user, on receiving a Source Quench**,** uncertain of the cause in which the message was issued (e.g. heavy congestion, approaching congestion, burst causing massive overload).

Random Drop: Random Drop is a congestion control policy intended to give feedback to users whose traffic congests the gateway by dropping packets. In this policy, randomly selected packets for a particular user, from incoming traffic, will be dropped. A user generating much traffic will have much more packets drop than the user who generate little

traffic. The selection of packets drop in this policy is completely uniform. Random Drop can be categorized as Congestion recovery or congestion avoidance.

Congestion recovery tries to restore an operating state, when demand has exceeded capacity. Congestion avoidance is preventive in nature. It tries to keep the demand on the network at or near the point of maximum power, so that the congestion never occurs.

Congestion Indication: The so-called Congestion Indication policy uses a similar technique as the Source Quench policy to inform the source gateway of congestion. The information is communicated in a single bit. The Congestion Experienced Bit (CEB) is set in the network header of the packets already being forwarded by a gateway. Based on the value of this bit, the end-system user should make an adjustment to the sending window. The Congestion Indication policy works based upon the total demand on the gateway. For fairness the total number of users causing the congestion is not considered. Only users who are sending more than their fair share (allowed bandwidth) should be asked to reduce their load, while others could attempt to increase their load where possible.

Fair Queuing: Fair queuing is a congestion control policy where separate gateway output queues are maintained for individual end-systems on a source-destination-pair basis. When congestion occurs, packets are dropped from the longest queue. At the gateway, the processing and link resources are distributed to the end-systems on a round-robin basis. Round-robin is an arrangement of choosing all elements in a group equally in a circular. Equal allocations of resources are provided to each source-destination pair.

A Bit-Round Fair Queuing algorithm was an improvement over the fair queuing. It computes the order of service to packets using their lengths, by using a technique that emulates a bit-by-bit round-robin discipline. In this case, long packets do not get an advantage over short packets. Otherwise the round-robin would be unfair.

Stochastic Fairness Queuing (SFQ) is a similar mechanism to Fair Queuing. SFQ looks up the source-destination address pair in the incoming packets and locates the appropriate queue that packet will have to be placed in. It uses a simple hash function to map from the source-destination address pair to a fixed set of queues. The price paid to implement SFQ is that it requires a potentially large number of queues.

11. MPLS, and GMPLS traffic engineering

Network control (NC) can be classified as centralized or distributed. In centralized network control, the route control and route computation commands are implemented and issued from one place. Each node in the network communicates with a central controller and it is the controller's responsibility to perform routing and signaling on behalf of all other nodes. In a distributed network control, each node maintains partial or full information about the network state and existing connections. Each node is responsible to perform routing and signaling. Therefore, coordination between nodes is required to alleviate the problem of contention.

Since its birth, the Internet (IP network) has employed a distributed NC paradigm. The Internet NC consists of many protocols. The functionality of resource discovery and management, topology discovery, and path computation and selection are the responsibility of routing protocols. Multiprotocol label switching (MPLS) has been proposed by IETF, to

enhance classic IP with virtual circuit-switching technology in the form of label switched path (LSP). MPLS is well known for its TE capability and its flexible control plane.

Then, IETF proposed an extension to the MPLS-TE control plane to support the optical layer in optical networks; this extension is called the Multiprotocol Lambda Switching (MPλS) control plane. Another extension to MPLS was proposed to support various types of switching technologies. This extension is called Generalized Multi- Protocol Label Switching (GMPLS). GMPLS has been proposed in the Control and Measurement Plane working group in the IETF as a way to extend MPLS to incorporate circuit switching in the time, frequency and space domains.

11.1 MPLS traffic engineering architecture

Multiprotocol label switching (MPLS) is a hybrid technology that provides very fast forwarding at the cores and conventional routing at the edges. MPLS working mechanism is based on assigning labels to packets based on forwarding equivalent classes

(FEC) as they enter the network. A FEC identifies of a group of packets that share the same requirements for their transport. All packets in such a group are provided the same treatment en route to the destination.

Packets that belong to the same FEC at a given node follow the same path and the same forwarding decision is applied to all packets. Then packets are switched through the MPLS domain using simple label lookup. Each FEC may be given a different type of service. At each hop, the routers and switches use the packet labels to index the forwarding table to determine the next-hop router and a new value for the label. This new label replaces the old one and the packet is forwarded to the next hop. As each packet exits the MPLS domain, the label is stripped off at the egress router, and then the packet is routed using conventional IP routing mechanisms.

The router that uses MPLS is called a label switching router (LSR). A LSR is a high speed router that participates in establishment of LSPs using an appropriate label signaling protocol and high-speed switching of the data traffic based on the established paths.

MPLS-TE has the following components and functionalities, as shown in Figure 2:

1. The routing protocol (e.g. OSPF-TE, IS-IS TE), collects information about the network connectivity (this information is used by each network node to know the whole topology of the network) and carries resource and policy information of the network. The collected information is used to maintain: The so-called Link-state database which provides a topological view of the whole network and the TE database which stores resource and link utilization information. The databases are used by the path control component. A constrained Shortest Path First (CSPF) is used to compute the best path.
2. A signaling protocol (e.g. RSVP-TE or CR-LDP) is used to set up LSP along the selected path through the network. During LSP setup, each node has to check whether the requested bandwidth is available. This is the responsibility of the link admission control that acts as an interface between the routing and signaling protocol. If bandwidth is available, it is allocated. If not, an active LSP might be preempted or the LSP setup fails.

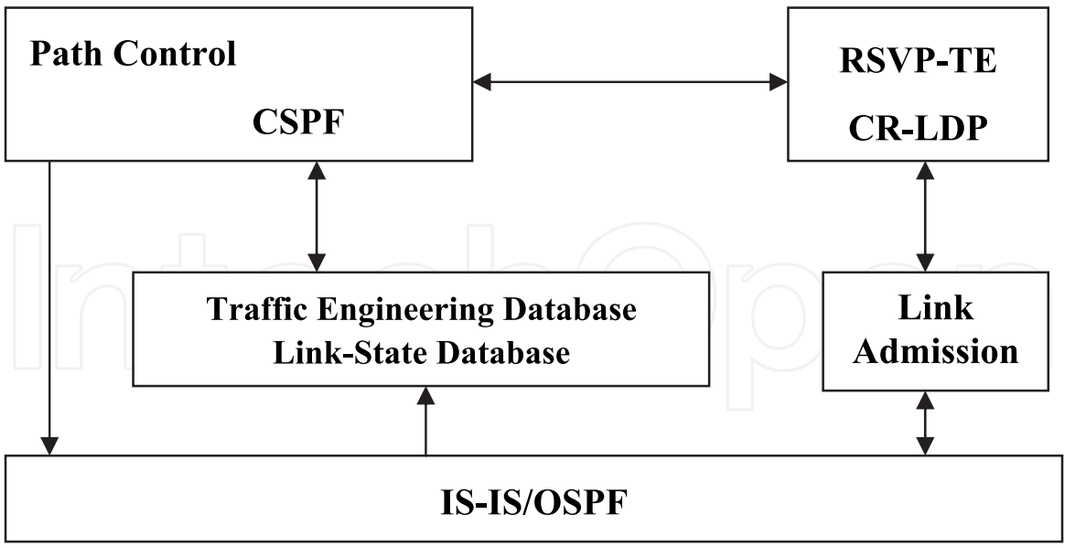


Fig. 3. MPLS-TE functional components.

11.2 MPλS/GMPLS control plane

IETF proposed an extension to the MPLS-TE control plane to support optical layers in optical networks; this extension is called the multiprotocol lambda switching (MPλS) control plane. In an MPLS network, the label-switching router (LSR) uses the label swapping paradigm to transfer a labeled packet from an input port to an output port. In the optical network, the OXC uses switch matrix to switch the data stream (associated with the light path) from an input port to an output port. In both LSR and OXC, a control plane is needed to discover, distribute, and maintain state information and to instantiate and maintain the connections under various TE roles and policies.

The functional building blocks of the MPλS control plane are similar to the standard MPLS-TE control plane. The routing protocol (e.g. OSPF or IS-IS) with optical extensions, is responsible for distributing information about optical network topology, resource availability, and network status. This information is then stored in the TE database. A constrained-based routing function acting as a path selector is used to compute routes for LSPs through mesh network. Signaling protocols (e.g. RSVP-TE or CR-LDP) are then used to set up and maintain the LSPs by consulting the path selector.

Another extension to the MPLS control plane is proposed to support various types of optical and other switching technologies. This extension is called Generalized Multi-Protocol Label Switching (GMPLS). In the GMPLS architecture, labels in the forwarding plane of Label Switched Routers (LSRs) can route the packet headers, cell boundaries, time slots, wavelengths or physical ports. The following switching technologies are being considered, as shown in Figure 3.

Packet switching: The forwarding mechanism is based on packet. The networking gear is an IP router.

Layer 2 switching: The forwarding mechanism is based on cell or frame (Ethernet, ATM, and Frame Relay).

Time-division multiplexing (time slot switching): The forwarding mechanism is based on the time frames with several slots and data is encapsulated into the time slots (e.g. SONET/SDH).

Lambda switching: λ switching is performed by OXCs.

Fiber switching: Here the switching granularity is a fiber. The networkings gears are fiber switch capable OXCs.

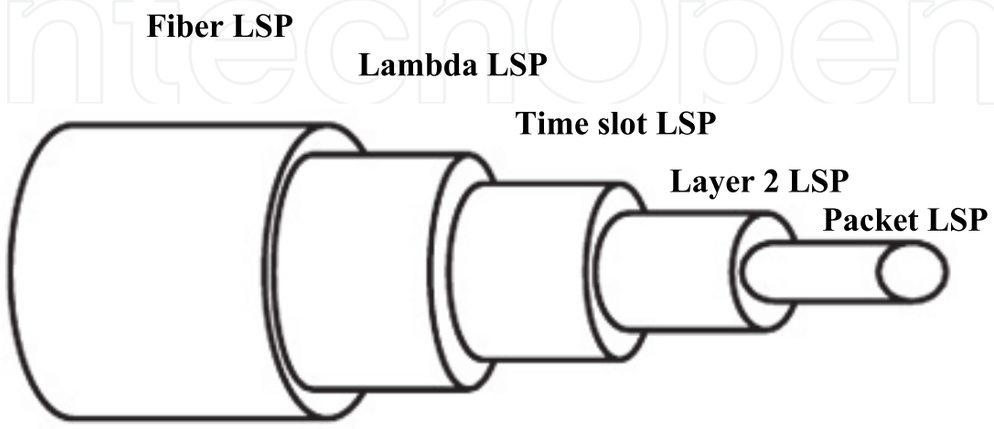


Fig. 4. GMPLS Label – Stacking Hierarchy.

The difference between MPλS and GMPLS is that the MPλS control plane focuses on Lambda switching, while GMPLS includes almost the full range of networking technologies.

12. MPLS traffic engineering features

1. **Explicit routes:** MPLS supports setting up of explicit routes, which can be an important tool for load balancing and satisfying other objectives so as to steer traffic away from particular paths. It is a very powerful technique which potentially can be useful for a variety of purposes. With pure datagram routing the overhead of carrying a complete explicit route with each packet is prohibitive. However, MPLS allows the explicit route to be carried only at the time that the label switched path is set up, and not with each packet. This implies that MPLS makes explicit routing practical. This in turn implies that MPLS can make possible a number of advanced routing features which depend upon explicit routing.
   An explicitly routed LSP is an LSP where, at a given LSR, the LSP next hop is not chosen by each local node, but rather is chosen by a single node (usually the ingress or egress node of the LSP). The sequence of LSRs followed by an explicit routing LSP may be chosen by configuration, or by an algorithm performed by a single node (for example, the egress node may make use of the topological information learned from a link state database in order to compute the entire path for the tree ending at that egress node).
   With MPLS the explicit route needs to be specified at the time that Labels are assigned, but the explicit route does not have to be specified with each L3 packet. This implies that explicit routing with MPLS is relatively efficient (when compared with the efficiency of explicit routing for pure datagram).

Explicit routing may be useful for a number of purposes such as allowing policy routing and/or facilitating traffic engineering.

2. **Path preemption:** Some tunnels are more important than others. Say for example, a VoIP tunnel and data tunnel may compete for same resources, in which case VoIP tunnel is given a higher priority and data tunnel is made to recalculate a path or just drop, if no path is available. Tunnels have 2 priorities: setup priority and hold priority. Each can have a value from 0 to 7 and the higher the priority numbers the lower the tunnels importance. The setup priority is used when setting up a tunnel and is compared with the hold priority of already established ones. If the setup priority is higher than the hold priority of established tunnel, then established tunnel is preempted.
3. **Fast Re-route:** In case of a link failure, interior gateway protocols may take of the order of 10 seconds to converge. Fast reroute involves pre-signaling of backup path along with the primary path. The protection may be path protection (end-to-end) or local protection which may be further differentiated into link protection and node protection.
   Fast reroute is a Multiprotocol Label Switching (MPLS) resiliency technology to provide fast traffic recovery upon link or router failures for mission critical services. Upon any single link or node failures, it could be able to recover impacted traffic flows in the level of 50 ms.

Backup path can be configured for:

1. **Link protection:** a link protection model each link (or subset links) used by an LSP is provided protection by pre-established backup paths.
2. **Node protection:** In a node protection model each node (or subset of nodes) used by an LSP is provided protection by pre-established backup paths.

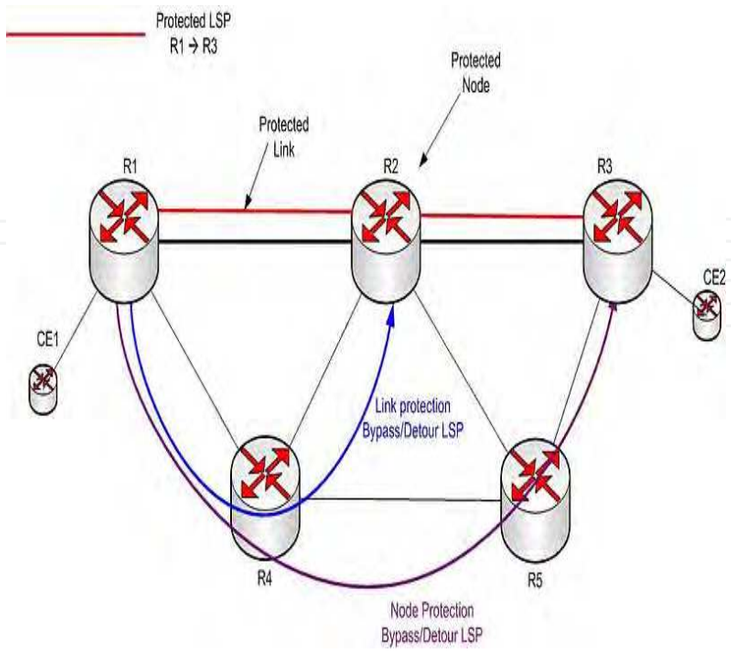
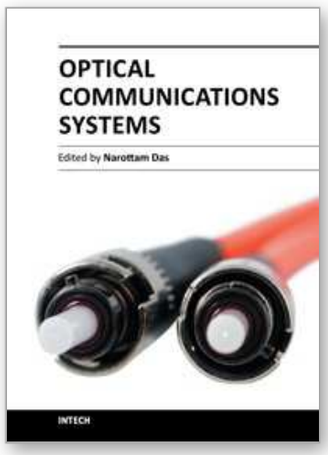


Fig. 5. Link Protection V/s Node Protection

13. References

[1] J. Malcolm, J. Agogbua, M. O'Dell and J. McManus, "Requirements for Traffic Engineering Over MPLS," IETF RFC 2702, September 2004.
[2] T. Li and Y. Rekhter, "A Provider Architecture for Differentiated Services and Traffic Engineering (PASTE)," IETF RFC 2430, October 2006.
[3] M. Allman, V. Paxon, and W. Stevens. TCP congestion control. Request for Comments (Standards Track) RFC 2581 April 1999. URL:http://www.ietf.org/rfc/rfc2581.txt.
[4] D. Awduche, J. Malcolm, J. Agogbua, J. McManus "Requirements for Traffic Engineering over MPLS (RFC 2702)" http://rfc-2702.rfc-list.net/rfc-2702.htm Sept 1999.
[5] V. Alwayn, "Advanced MPLS Design and Implementation"ISBN 1-58705-020-X.
[6] L. Andersson, P. Doolan, N. Feldman, A. Fredette, B. Thomas "LDP Specification (RFC 3036)" http://rfc-3036.rfc-list.net/ January 2001.
[7] Li, T. and Y. Rekhter, "Provider Architecture for Differentiated Services and Traffic Engineering (PASTE)", RFC 2430, October 1998.



Optical Communications Systems

Edited by Dr. Narottam Das

ISBN 978-953-51-0170-3
Hard cover, 262 pages
Publisher InTech
Published online 07, March, 2012
Published in print edition March, 2012

Optical communications systems are very important for all types of telecommunications and networks. They consists of a transmitter that encodes a message into an optical signal, a channel that carries the signal to its destination, and a receiver that reproduces the message from the received optical signal.This book presents up to date results on communication systems, along with the explanations of their relevance, from leading researchers in this field. Its chapters cover general concepts of optical and wireless optical communication systems, optical amplifiers and networks, optical multiplexing and demultiplexing for optical communication systems, and network traffic engineering. Recently, wavelength conversion and other enhanced signal processing functions are also considered in depth for optical communications systems. The researcher has also concentrated on wavelength conversion, switching, demultiplexing in the time domain and other enhanced functions for optical communications systems. This book is targeted at research, development and design engineers from the teams in manufacturing industry; academia and telecommunications service operators/ providers.

InTech Europe
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821

IntechOpen