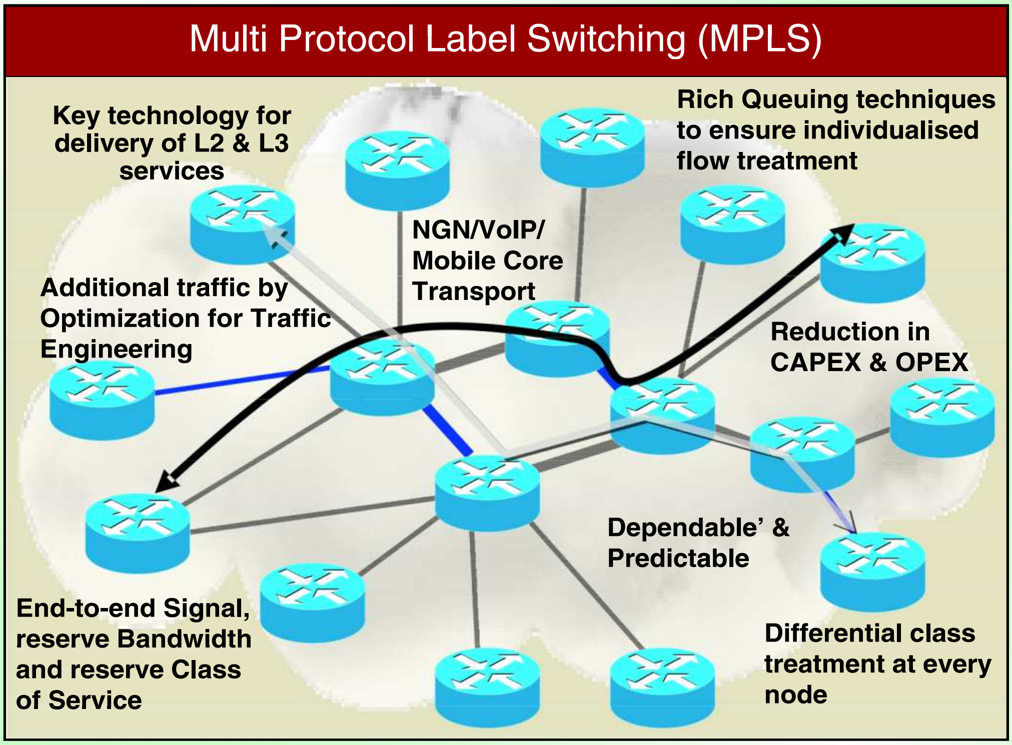
TEC
TELECOMMUNICATION ENGINEERING CENTRE

NEWSLETTER
टी ई सी संचारिका

VOL 11 SEPTEMBER 2007 ISSUE 3



Multi Protocol Label Switching (MPLS)

Key technology for delivery of L2 & L3 services

Rich Queuing techniques to ensure individualised flow treatment

NGN/VoIP/ Mobile Core Transport

Additional traffic by Optimization for Traffic Engineering

Reduction in CAPEX & OPEX

Dependable' & Predictable

End-to-end Signal, reserve Bandwidth and reserve Class of Service

Differential class treatment at every node

IN THIS ISSUE

- Multi Protocol Label Switching (MPLS)

Multi Protocol Label Switching (MPLS)

NGN is evolving into a ubiquitous network and inspiring the development of a variety of new applications and services in business and consumer markets. These new applications demand will augment and guarantee bandwidth in the network. The demands placed on the network by these new applications and services, in terms of speed and bandwidth, require augmentation of the existing network infrastructure.

The exponential growth in the number of users and the volume of traffic adds another dimension to the network problem. Class of Service (CoS) and Quality of Service (QoS) are important issues of NGN as they determine the degree of satisfaction to the user of a service. These are the requirements of network to support wide range of applications and services.

Most of the IP routing protocols deployed today are based on algorithms designed to obtain the shortest path in the network for packet traversal and do not take into account service requirement information contained in the packets. Additional constraints such as delay, jitter, packet loss and traffic congestion further diminish network performance. Traffic engineering is a challenge for network managers.

Multi Protocol Label Switching (MPLS) has emerged as an most appropriate solution to meet the bandwidth management and service requirements for Next Generation Networks. MPLS is a versatile solution to address the problems faced by the present-day networks of speed, scalability, quality-of-service (QoS) management and traffic engineering.

MPLS plays an important role in routing, switching and forwarding of packets through the NGN in order to meet the service demands of the network users.

What is MPLS?

MPLS is a packet forwarding technology which uses labels to make data forwarding decisions. MPLS does not replace IP – but supplements IP so that traffic can be classified, managed, and policed. With the use of MPLS, end-to-end quality of service can be achieved.

MPLS is an Internet Engineering Task Force (IETF) specified framework that provides for the efficient designation, routing, forwarding, and switching of traffic flows through the network. MPLS performs the following functions:

- Specifies mechanisms to manage traffic flows of various granularities such as flows between different hardwares, machines or even flows between different applications
- Provides a means to map IP addresses simple, fixed- length labels used by different packet-forwarding and packet switching technologies
- Interfaces to existing routing protocols such as Resource Reservation Protocol (RSVP) and Open Shortest Path First (OSPF)
- Remains independent of the Layer-2 and Layer-3 protocols
- Supports the IP, ATM and frame-relay Layer-2 protocols

How MPLS works?

In MPLS, data transmission occurs on label switched paths (LSPs). LSPs are a sequence of labels at each and every node along the path from the source to the destination. LSPs are established either prior to data transmission (control-driven) or upon detection of a certain flow of data (data-driven). The labels, which are underlying protocol-specific identifiers, are distributed using Label Distribution Protocol

(LDP) or RSVP or piggybacked on routing protocols like Border Gateway Protocol (BGP) and OSPF. Each data packet encapsulates and carries the labels during their journey from source to destination. High speed switching of data is possible because the fixed-length labels are inserted at the very beginning of the packet or cell and can be used by hardware to switch.

The devices that participate in the MPLS protocol mechanisms can be classified into Label Edge Routers (LERs) and Label Switching Routers (LSRs).

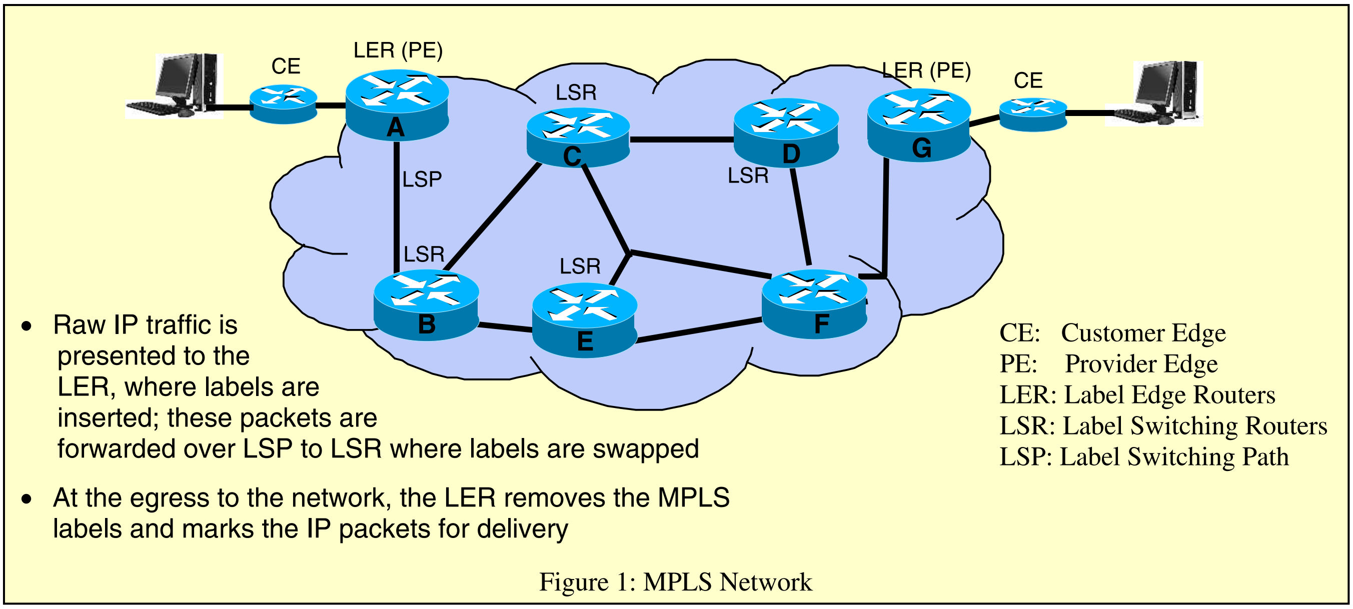
An LSR is a high-speed router device in the LSPs using the appropriate label signaling protocol and high-speed switching of the data traffic based on the established paths.

An LER is a device that operates at the edge of the access network and MPLS core network. LERs support multiple ports connected to dissimilar networks (such as frame relay, ATM, and Ethernet) and forwards this traffic on to the MPLS network after establishing LSPs. Label signaling protocol at the LER plays a very important role in the assignment and removal of labels, as traffic enters or exits an MPLS network.

The Forward Equivalence Class (FEC) is a representation of 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. As opposed to conventional IP forwarding, in MPLS, the assignment of a particular packet to a particular FEC is done just once, as the packet enters the network. FECs are based on service requirements for a given set of packets or simply for an address prefix. Each LSR builds a table to specify how a packet must be forwarded. This table, called a Label Information Base (LIB), is comprised of FEC-to-label bindings.

A label, in its simplest from, identifies the path that a packet traverses. A label is carried or encapsulated in a Layer-2 header along with the packet. The receiving router examines the packet for its label content to determine the next hop. Once a packet has been labelled, the rest of the journey of the packet through the backbone is based on label switching. The label values are of local significance only, meaning that they pertain only to hops between LSRs.

Labels are bound to an FEC as a result of same event or policy that indicates a need for such



- Raw IP traffic is presented to the LER, where labels are inserted; these packets are forwarded over LSP to LSR where labels are swapped
- At the egress to the network, the LER removes the MPLS labels and marks the IP packets for delivery

CE: Customer Edge
PE: Provider Edge
LER: Label Edge Routers
LSR: Label Switching Routers
LSP: Label Switching Path

Figure 1: MPLS Network

binding. These events can be either data-driven bindings or control-driven bindings. The latter is preferable because of its advanced scaling properties that can be used in MPLS.

Label assignment decisions may be based on forwarding criteria such as the following:

- Destination unicast routing
- Traffic engineering
- Quality of Service (QoS)
- Multicast routing
- Virtual Private Network (VPN)

When a labeled packet arrives at a Label Switching Router (LSR), the incoming label will determine the path of this packet within the MPLS network. MPLS label forwarding will then swap this label to the appropriate outgoing label and send packets to the next hop.

This MPLS look up and forwarding system allows explicit control routing, based on destination and source address, allowing easier introduction of new IP services.

The following steps are taken for a data packet to travel through an MPLS domain.

- Label creation and distribution
- Table creation at each router
- Label-switched path creation
- Label insertion/table lookup
- Packet forwarding

MPLS provides two options to set up LSP

Hop-by-hop routing: This methodology is similar to that used in IP networks, where each LSR independently selects the next hop for a given FEC. The LSR uses any available routing protocol, such as OSPF, ATM private network-to-network interface (PNNI), etc.

Explicit Routing (ER): In this methodology, the ingress LSR first specifies the list of nodes through which the ER-LSP traverses. Along the selected path, the resources are reserved to ensure QoS. This eases traffic engineering throughout the network and differentiated services can be provided based on the policies or network management methods

MPLS Traffic Engineering

Traffic Engineering (TE) refers to the process of selecting the paths chosen by data traffic in order to facilitate efficient and reliable network operations while simultaneously optimizing network resource utilization and traffic performance. The goal of TE is to compute path from one given node to another such that the path does not violate any constraints (bandwidth/administrative requirements) and is optimal with respect to some scalar metric.

In an MPLS domain, all the source traffic need not be necessarily transported through the same path. Depending on the traffic characteristics, different LSPs could be created for packets with different CoS requirements.

Traffic Engineering

Traffic engineering is a process that enhances overall network utilization by attempting to create a uniform or differentiated distribution of traffic throughout the network. This process avoids the congestion in any path of the network. It is important to note that traffic engineering does not necessarily select the shortest path between two devices. It may be possible that for two packet data flows, the packets may traverse completely different paths even though their originating node and the final destination node are the same. This process enables the less-exposed or less-used network segments to be used and hence differentiated services can be provided.

In MPLS, traffic engineering is inherently provided using explicitly routed paths. The LSPs are created independently, specifying different paths that are based on user- defined policies. However, this may require extensive operator intervention. RSVP and CR-LDP are two options to manage dynamic traffic engineering and QoS in MPLS.

Constraint-based routing (CR)

Constraint-based routing takes into account parameters such as link characteristics (bandwidth, delay, etc.), hop count and QoS. The established LSPs could be CR-LSPs, where the constraints could be explicit hops or QoS requirements. Explicit hops dictate which path is to be taken. QoS requirements dictate which links and queuing or scheduling mechanisms are to be employed for the flow.

While using CR, it is possible that a longer (in terms of cost) but less loaded path is selected. However, while CR increases network utilization, it adds more complexity to routing calculations, as the path selected must satisfy the QoS requirements of the LSP. CR can be used in conjunction with MPLS to set up LSPs. The IETF has defined a CR-LDP component to facilitate constraint-based routes.

Tunnelling in MPLS

A unique feature of MPLS is that it can control the entire path of a packet without explicitly specifying the intermediate routers. It does this by creating tunnels through the intermediary routers spaning multiple segments.

MPLS Applications

MPLS addresses today's network backbone requirements effectively by providing standards based solution that accomplishes the following:

- Improved packet-forwarding performance in the network thereby increasing network performance
- QoS and CoS for service differentiation by using traffic-engineered path set up thereby achieving service level guarantees.
- Network scalability support
- MPLS is a standards based solution that builds interoperable networks
- MPLS facilitates IP over Synchronous Optical Network (SONET) integration in optical switching.
- MPLS helps build scalable VPNs with traffic engineering capability.

Quality of Service (QoS)

There are two architectures for adding QoS capabilities to IP networks Viz. Integrated Services (IntServ) and Differentiated Services (DiffServ).

Integrated Services maintain an end-to-end QoS for an individual or group of flows with the help of a Resource Reservation Protocol (RSVP).

In DiffServ model, packets entering a DiffServ enabled network are grouped into a small number of classes. Each class has a color or mark associated with it (use of the DiffServ Code Point DSCP bits). This makes packet classification extremely scalable and assures appropriate bandwidth and delay guarantees in the core network. Each node within the core network is applied to different queuing and dropping policies on every packet, based on the marking carried by packet (Per Hop Behavior).

Resiliency

Network reliability is mandatory in high-speed networks. Disruption can occur due to several reasons namely congestion along the LSP, failed link, failed node, administrative change in the LSP. One of the most significant features of MPLS TE is the possibility to provide non disruptive traffic across the LSP. In case of outage, the upper level application will not notice any service disruption.

Security

MPLS can provide a secure service only if the core network is provided in a secure manner. MPLS itself does not provide encryption, integrity, or authentication services. If these features are required, IPSec has to be used over the MPLS infrastructure. To keep control of the encryption, the IPSec should be implemented on another device before the CE router in the network.

IMPORTANT ACTIVITIES OF TEC DURING MAY 2007 TO AUGUST 2007

Following GRs/IRs and Technical documents were issued:

New GRs/IRs

- National Standards for H.248
- National Standards for SIGTRAN
- Radio Network Planning tool for CDMA 2000 1x & 1x EV-DO
- Metal Free Optical Fibre Cable (G-652 D Fibre)

Revised GRs/IRs

- Synthesized Signal Generator (1 GHz-40 GHz) Digital Cable Fault Locator for Copper Cable
- 2 mbps Echo Cancellar
- 55°K Low noise amplifier subsystem in lower C-band and Ext C-band
- Synthesized Signal Generator (1GHz-40 GHz)

GRs/ IRs Amended

- 20 Metre and 30 Metre Narrow Base Light Weight Tower

Approvals issued by TEC during the period May 2007 to August 2007

Interface Approvals..........................	52
Interface Approvals............................	194
Total	**246**

Tests and Field trials

- Testing of V5.2 protocol with EPABX (IRIS IVDX of M/s Coral Telecom)

Manufacturers' Forum conducted for

- Softswitch for Local and Transit Application
- Element Management System
- SIP Application Server
- Service Description for NGN Subscribers
- Session Border Controller
- Line Media Gateway
- Trunk Media Gateway
- Interface Requirement of Digital Exchange with 2048Kbit/s and STM-1 interface
- Centralized Monitoring System (CMS)

Field support/technical advice

- Implementation of "Lo karlo Baat" service in C-DOT exchanges

Technical Presentation

- Software Defined Radio by C-DOT
- Safety Requirement of Telecom products as per IEC Safety Standards
- Centralized Monitoring System (CMS)

Approvals issued by TEC upto 31.08.2007

Interface Approvals..............................	4382
Service Test Certificates......................	2384
Grand Total	**6766**

DISCLAIMER : TEC Newsletter provides general technical information only and it does not reflect the views of DoT, TRAI or any other organisation. TEC/Editor shall not be responsible for any errors, omissions or incompleteness.

टी ई सी संचारिका
सितम्बर 2007
भाग 11
अंक 3

दूरसंचार इंजीनियरी केन्द्र
खुर्शीदलाल भवन
जनपथ
नई दिल्ली-110001

Editor : Vipan Kumar, DDG (S) Phone : 23329354 Fax : 23318724 Email : vkumar.ddg@gmail.com CSN 40

Prabhat Publicity, New Delhi